Introducing public sector eIDs

The power of actors’ translations and institutional barriers

Fredrik Söderström

Linköping Studies in Arts and Science No. 701
Faculty of Arts and Sciences
Linköping 2016
At the Faculty of Arts and Sciences at Linköping University, research and doctoral studies are carried out within broad problem areas. Research is organized in interdisciplinary research environments and doctoral studies mainly in graduate schools. Jointly, they publish the series Linköping Studies in arts and Science. This thesis comes from the Information Systems Division at the Department of Management and Engineering.

Distributed by:
Department of Management and Engineering
Linköping University
581 83 Linköping

Fredrik Söderström
Introducing public sector eIDs
The power of actors’ translations and institutional barriers

Edition 1:1
ISSN 0282-9800

©Fredrik Söderström

Picture: Alexander Åkerberg

Department of Management and Engineering 2016
Information Systems Division

Printed by: LiU Tryck
Science, like all creative activity, is exploration, gambling and adventure. It does not lend itself very well to neat blueprints, detailed roadmaps and central planning. Perhaps that’s why it’s fun. (Herbert Simon)
Abstract

The electronic identification (eID) is a digital representation of our analogue identity used for authentication in order to gain access to personalized restricted online content. Despite its limited and clearly defined scope, the eID has a unique role to play in information society as an enabler of public digital services for citizens as well as businesses and a prerequisite for the development of electronic government (eGovernment). This study shows a tendency of treating public sector eIDs like Information and Communications Technology (ICT) artefacts in general. Hence, a narrow focus on technology is often applied thus placing non-technical aspects in the background. Consequently, social and organizational implications are often unproblematized which in turn becomes problematic in the case of the public sector eID.

This study puts forth a need for a broader focus in this area and contributes by focusing on the challenges related to the resistance to introductions of eIDs among affected actors in the public sector. This study assumes that affected actors’ perceptions (translations) of the eID have a potential impact on its introduction on organizational as well as operational level. Research questions focus on the influence of resistance on the introduction and the relationship between resistance and actors’ translations of the eID. The aim is to further develop existing concepts and bring new insights to research as well as practice. The analytical perspectives of sociology and institutionalism aim at developing a tentative analytical framework for investigations of this relationship. Introductions, therefore, become institutional pressures facing resistance as related to affected actors’ translations. The empirical basis consists of two interpretive case studies of eID introductions—a national eID to cover the entire public sector and a professional eID in health care.

The result shows that resistance in the form of institutional barriers develops from actors’ negative translations of the eID and main coordinating actors’ tend to fail in their attempts to negotiate these barriers. This confirms a closer relationship between institutional pressures and barriers and a view of pressures, barriers and eIDs as translated institutions transferred across organizational settings is put forth. To facilitate future research and practice related to public sector eID introductions, three propositions are put forth. (1) The importance of acknowledging pressures to introduce eIDs as closely related to barriers. (2) The institutions involved in this process as all translated by the government, coordinating actors as well as affected actors. (3) The importance of a developed understanding of these institutions, translations and relationships in order to facilitate cooperative efforts shaping future public sector eIDs.
Foreword

Information Systems Development (ISD) is a research discipline within the Faculty of Arts and Sciences at Linköping University (LiU), Linköping Sweden. ISD is a discipline studying human work with developing and changing different kinds of IT systems in organisational and societal settings. The research discipline includes theories, strategies and policies, models, methods, co-working principles and artefacts related to information systems development. Different development/change situations can be studied as planning, analysis, specification, design, implementation, deployment, evaluation, maintenance and redesign of information systems and its interplay with other forms of business development, processes of digitalization and innovation. The discipline also includes the study of prerequisites for and results from information systems development, as e.g. institutional settings, studies of usage and consequences of information systems.

The ISD research at LiU is conducted in collaboration with both private companies and public organizations. Collaboration also includes national and international research partners in the information systems research field. The research has a clear ambition to give distinct theoretical contributions within the information systems research field. Simultaneously, the research aims to contribute with practically needed and useful knowledge.

This work, *Introducing public sector eIDs – the power of actors’ translations and institutional barriers*, is written by Fredrik Söderström, Linköping University. He is also a member of the research group VITS. He presents this work as his PhD dissertation in Information Systems Development, Information Systems Division, Department of Management and Engineering, Linköping University, Sweden.

Linköping, October 2016

Karin Axelsson  Göran Goldkuhl  Ulf Melin
Professor  Professor emeritus  Associate Professor
Doctoral dissertations in information systems development

18. Per Oscarson (2007) Actual and perceived information systems security
22. Ida Lindgren (2013) Public e-Service Stakeholders - On who matters for public e-service development and implementation
23. Malin Granath (2016) The Smart City – how smart can ‘IT’ be? Discourses on digitalisation in policy and planning of urban development
24. Fredrik Söderström (2016) Introducing public sector eIDs – the power of actors’ translations and institutional barriers
Licentiate theses in information systems development

2. Karin Pettersson (1994) Informationssystemstrukturering, ansvarsfördelning och användarinflytande - en komparativ studie med utgångspunkt i två informationssystemstrategier
24. Per Oscarson (2001) Informationssäkerhet i verksamheter - begrepp och modeller som stöd för förståelse av informationssäkerhet och dess hantering i verksamheter
29. Fredrik Ericsson (2003) Information Technology for Learning and Acquiring Work Knowledge among Production Workers
44. Hannes Göbel (2014) IT Service Management – Designprinciper för informationsystemsartefakter
Acknowledgements

It has now been five years since I took my first steps into academia as a PhD candidate and I can honestly say it has been an adventure. Some might say that five years is a considerable time but in my case, the time has really flown by. There have been quite a number of ups and downs along the way, but as time goes by, you come to appreciate them both. It is as the pressures and barriers focused in this PhD - without the downs, you can not appreciate the ups. Since I have been far from alone on this roller-coaster ride, there are quite a few I want to thank for having supported this work. First, my supervisor Ulf Melin and co-supervisor Karin Axelsson. Ulf, your support of this work has been invaluable. No matter how lost I have felt before our meetings and conversations, I have always left with renewed hope. So, that is quite a special power you have there. Combined with your excellent professional expertise, I could never have wished for a better supervisor. Karin, your comments and views on this work along the way have pushed me into new directions, and the opportunity to take advantages of your deep expertise and knowledge has been very valuable.

However, without the funding agency for our project focusing on the future use of eIDs, the Swedish Civil Contingencies Agency, I would most likely not have come in contact with this very interesting research area at all. Without the skilled main authors of papers, I would not have had the opportunity to participate in these very interesting and creative writing processes and without my colleagues at the Information Systems Department, I would most certainly not have endured this process. Dear colleagues, your good advice and comments on seminars as well as in the corridor have been invaluable, and I look forward to our talks in coming ‘fikas’. Without the comments and feedback from participants at my final seminar, I would not have come this far either. I also would like to thank participating respondents as well as ‘the experts’ in the eID field. Without your willingness to participate and share your views, I would never have realized the great potential and vast challenges of this little thing called the eID. In addition, I am sure the cover would have been rather dull without the creative mind of the photographer. Last but not least, without the support and understanding of family and relatives, this could never have happened.

My sincere thanks to you all – you are the best!

Finally, to Anja, Jonathan and Anton: At last and always!

Fredrik Söderström
Linköping, November 2016
Contents

**Part I – Starting points** .............................................................................................................. 1

1. **Introduction** ...................................................................................................................... 3
   1.1 Background and motivation .................................................................................................. 3
   1.2 Research questions ................................................................................................................. 12
   1.3 Aim and contribution ............................................................................................................. 13
   1.4 Knowledge development ....................................................................................................... 15
   1.5 Delimitations ........................................................................................................................... 17
   1.6 Intended audiences .................................................................................................................. 22
   1.7 Dissertation outline ................................................................................................................. 23
   1.8 A reader’s guide ...................................................................................................................... 25

2. **Research perspective and method** .................................................................................. 27
   2.1 Introduction ............................................................................................................................. 27
   2.2 Research perspective ............................................................................................................... 28
   2.3 Research method ..................................................................................................................... 35
   2.4 Selecting cases ........................................................................................................................ 40
   2.5 Data collection ........................................................................................................................ 45
   2.6 Analysis and synthesis ............................................................................................................ 51
   2.7 Quality, relevance and ethical considerations ......................................................................... 55

**Part II – Theoretical and analytical perspectives** ................................................................... 63

3. **Theoretical perspective** ..................................................................................................... 65
   3.1 ISR .......................................................................................................................................... 65
   3.2 Electronic government .............................................................................................................. 68
   3.3 Social and organizational perspectives .................................................................................... 72
   3.4 Electronic identification .......................................................................................................... 85
   3.5 Concluding remarks ................................................................................................................ 96

4. **Analytical perspective** ...................................................................................................... 99
   4.1 Introduction ............................................................................................................................. 99
   4.2 The institutional perspective ................................................................................................. 101
   4.3 The sociological perspective .................................................................................................. 116
   4.4 The socio-institutional framework ........................................................................................ 126
4.5 Concluding remarks ................................................................................................. 132

Part III – Empirical evidence and analysis ................................................................. 133

5. The eGov eID ........................................................................................................... 135
   5.1 The public sector eID ............................................................................................... 135
   5.2 The introduction ..................................................................................................... 150
   5.3 The government perspective .................................................................................. 171
   5.4 Service Providers’ perspective .............................................................................. 175
   5.5 Identity Providers’ perspective .............................................................................. 182
   5.6 Concluding remarks .............................................................................................. 187

6. The eHealth eID ....................................................................................................... 191
   6.1 The Swedish health sector eID .............................................................................. 191
   6.2 The project ............................................................................................................. 196
   6.3 The introduction ..................................................................................................... 201
   6.4 The implications ..................................................................................................... 206
   6.5 Concluding remarks .............................................................................................. 217

7. Translating the eGov eID ....................................................................................... 219
   7.1 Problematization ..................................................................................................... 219
   7.2 Interdefinition of actors ....................................................................................... 220
   7.3 Obligatory Passage Point ...................................................................................... 223
   7.4 Interessement ......................................................................................................... 228
   7.5 Enrolment .............................................................................................................. 236
   7.6 Mobilization .......................................................................................................... 243
   7.7 Closure .................................................................................................................... 245
   7.8 Concluding remarks .............................................................................................. 246

8. Translating the eHealth eID .................................................................................... 251
   8.1 Problematization ..................................................................................................... 251
   8.2 Interdefinition of actors ....................................................................................... 252
   8.3 The Obligatory Passage Point .............................................................................. 253
   8.4 Interessement ......................................................................................................... 257
   8.5 Enrolment .............................................................................................................. 263
   8.6 Mobilization .......................................................................................................... 267
   8.7 Closure .................................................................................................................... 269
Table 17. Challenges and examples of outcomes of the eGov eID introduction ................................ 188
Table 18. Different views of the eHealth eID ..................................................................................... 207
Table 19. Summary of identified challenges and examples of outcomes ........................................... 218
Table 20. Summary of eGov eID translation analysis ......................................................................... 249
Table 21. Summary of eHealth eID translation analysis ..................................................................... 273
Table 22. General characterization of pressures.................................................................................. 284
Table 23. eGov case - factors, dimensions and predicted levels of pressures ..................................... 286
Table 24. eHealth case - factors, dimensions and predicted levels of pressures .................................. 287
Table 25. General characterization of barriers ................................................................................... 291
Table 26. eGov case - factors, dimensions and outcome of pressures ................................................ 293
Table 27. eHealth case - factors, dimensions and outcome of pressures ............................................. 294
Table 28. Legitimacy and efficiency ................................................................................................... 296
Table 29. Multiplicity and dependency ............................................................................................... 298
Table 30. Consistency and constraints ............................................................................................... 299
Table 31. Enforcement and voluntariness ......................................................................................... 300
Table 32. Uncertainty and interconnectedness .................................................................................... 301
Table 33. Implications for research ..................................................................................................... 326
Table 34. Implications for practice ...................................................................................................... 329
Table 35. Addressing principles by Klein & Myers' (1999) ............................................................... 329
Table 36. Result from inductive coding .............................................................................................. 374
Table 37. Result from conceptual refinement ..................................................................................... 376
Table 38. Main incentives for the eGov eID (SOU 2010:104, p. 14) ................................................. 381
Table 39. The four assurance levels (Kantara IAF, 2009, p. 6)........................................................... 386
Table 40. Assessment of identified challenges in (SOU 2010:104).................................................... 390
Part I – Starting points

The first part of this dissertation covers the point of departure for this work with an introductory chapter to provide the background such as central challenges addressed as well as aim and guiding research questions. The second chapter then provides the research perspective and methods applied to carry out this work.
1. Introduction

This introduction provides the background, problem area, motivation and central perspectives applied in this dissertation focusing on the public sector eID as an important enabler of digital authentication. Basic concepts, opportunities and current challenges are described along with a claim for a broader focus on public sector eIDs in research as well as in practice. Guiding research questions are presented together with the aim, contribution and identified theoretical and empirical delimitations. The chapter is concluded with a description of the intended audience, an outline of this work and a reader’s guide for increased accessibility.

1.1 Background and motivation

The electronic identification (eID) has a unique role securing the identity of citizens and customers in public and private digital services (e-services) as well as for employees in organizations. Whenever there is a need for a securely identified user, this can be provided by secure digital authentication provided by the eID. Compared to other methods such as one-time passcodes or simple login procedures where a username and a password is provided, the eID brings a significantly higher level of security and trust regarding the validity of the identification. This is in turn related to the way the eID is issued, implemented and used during the authentication process. For example, it may require two-factor or strong authentication; a process requiring a combination of two different components such as something you have, a certificate on a smart card or mobile phone, and something you know, a password or a passcode. The increasing development and widespread use of digital services requiring users to be authenticated in a more secure way also result in increased development, diffusion and use of eIDs for authentication in external as well as internal services in organizations. Many public authorities, as well as private businesses, are currently completely dependent on this seemingly small and delimited artefact. As citizens and customers, we have also grown very dependent on the eID enabling us to securely access public and private digital services, for declaring our annual income tax, applying for parental and sickness benefits as well as for our online banking services. Our digital identification, as represented by the eID, is overtaking physical identification at a rapid pace in a growing number of service contexts. However, as this dissertation suggests, this increasing dependence on the eID also introduces several new potential challenges in theory as well as in practice. On a general level, this dissertation puts forth the importance of the eID in the public sector and advocates an

---

1 The assessment of the identification representing the identity of the user.
2 In Information Systems Research (ISR), an instantiation (example) of an information system is often referred to as an artefact.
increased awareness of its social and organizational implications. Moreover, since current public sector eID introductions face significant challenges, I argue that this increased contextual focus will facilitate a more reflective and successful handling of the challenges at hand on national as well as organizational levels.

1.1.1 Identity and identification

The concept of using one's identity for the purpose of identification in a particular service context can historically be traced back to local or national population registers, commercial transactions as well as legal matters. For decades, these issues are rather unproblematic and relying on the standardized process of providing the relevant physical documents such an ID card or passport in situations where the individual’s identity needs to be assessed in order for some transaction to take place. In the wake of digitization in the information society, the need for digital identifications and related processes such as authentication and authorization present opportunities as well as challenges regarding the handling of digital identities. In research, the digital identity, as represented by the eID, is often taken for granted and left unproblematized to a great extent (see Section 3.4.1). While there are studies actively trying to analyse the eID concept and relate it to different contexts (e.g. Beynon-Davies, 2006; Whitley et al., 2014), the majority of previous eID studies seem only to spend a sentence or two in the introduction on clarifying this concept. I thereby argue that these over-simplified conceptualizations of digital identity and identification may result in misinterpretations or even misleading results. In applied social sciences, such as the research field of this dissertation (Information System Research, ISR), the surrounding world is the object of study. How this world is translated and interpreted by the human actors existing and acting in different contexts of this world, therefore, needs to be investigated and made transparent. Thus, in an effort to avoid any confusion and misunderstanding regarding the eID concept presented in this work, an analysis is performed inspired by the socio-instrumental pragmatist approach presented by Goldkuhl (2002). The eID is therefore deconstructed into the four sub-concepts of identity, identification, authentication and authorization.

Table 1. Characterization of concepts

<table>
<thead>
<tr>
<th>Concept</th>
<th>Typification</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identity</td>
<td>Unique combination of attributes</td>
<td>Intra-subjective</td>
</tr>
<tr>
<td>Identification</td>
<td>Representation of attributes</td>
<td>Inter-subjective, symbols, artefacts</td>
</tr>
<tr>
<td>Authentication</td>
<td>Assessment of attributes</td>
<td>Interpretive action</td>
</tr>
<tr>
<td>Authorization</td>
<td>Permission based on attributes</td>
<td>Interventionist action</td>
</tr>
</tbody>
</table>
To be able to distinguish and characterize these basic concepts, an ontological approach is applied resulting in the typifications and locations described in Table 1. Identity is defined as a *unique combination of attributes* located in the inner intra-subjective world of an individual while identification is the *representation of attributes* located in the shared knowledge and institutions in the inter-subjective world also represented in the form of symbols and artefacts. The authentication is an *assessment of identity* performed as an interpretive action and *authorization* is granting permission based on attributes and thus performed as an interventionist action. It then becomes clear that the identity is in fact based on attributes unique to the individual while identification, authentication and authorization are related to the process of requesting and acquiring access to something protected from public access. With the addition of the prefix ‘e’ (electronic) and based on the concept analysis above the following definition of the eID emerges.

```
The eID is an identification representing unique attributes used for authentication and authorization in an electronic public or private service context.
```

### 1.1.2 The eID as an eGovernment enabler

Since public sector organizations need to handle sensitive data about individuals as citizens, an increased need to exchange such data in a secure digital way, in turn, creates the need for secure electronic authorization using eIDs (Otjacques et al., 2007). This exchange of data is related to public sector initiatives such as electronic government (eGovernment, eGov) facilitating development of information and communication technology (ICT) (Kraemer & Perry, 1979). Digital services in the public sector, therefore, become important drivers of eGovernment development (e.g. Chan & Pan, 2008; Grönlund & Horan, 2005; UN & ASPA, 2002). There are also internal and external incentives and demands for increased efficiency and improved delivery of public services towards citizens, businesses, employees and agencies as well as an increased citizen participation (Grönlund, 2002). The eID thereby acts as a back as well as front office enabler (Melin et al., 2016) with a potentially positive impact on public administration and democracy. The underlying incentives of eGovernment development can be traced back to targets formulated by the European Council’s Lisbon Strategy in the beginning of 2000 with the aim of improving Europe’s economic performance (UNPAN, 2007). Thus, the eID becomes a very important prerequisite and a key enabler for the public sectors ability to deliver secure digital services (Rössler, 2008); a perspective also shared by the European Commission (EC, 2014a). Since the benefits of the eID are currently being identified and acknowledged on a broader scale such as in national and international initiatives, the research interest in this artefact is steadily increasing. Examples of prior studies focus on several different aspects of the eID such as identity management.
(e.g. Seltsikas & O’Keefe, 2010; Talamo et al., 2014), identity service infrastructures (e.g. Shamah, 2006) and interoperability (e.g. Tauber et al., 2010), the ability of using a common eID in different identity management systems (Halperin & Backhouse, 2008). Significant challenges and opportunities of national eID initiatives are also reported in several studies (e.g. Grönlund, 2010; Hoff & Hoff, 2010). This is a direct consequence of the eID currently rising on national governmental agendas with the identified potential of increased central coordination, standardization, interoperability, and control on national as well as European level where initiatives such as eIDAS3 is currently being launched with a potential of cross-border enabled eIDs acting as a European digital market enabler (EC, 2015). There are currently several national as well as EU level initiatives running in parallel that are all highly dependent on common and secure public sector eID solutions. However, national eID initiatives show a significant fragmentation (EC, 2015) and variance in terms of prerequisites, introduction, and use (Kubicek & Noack, 2010c; Kubicek & Söderström, Submitted). Examples of successful national eIDs such as in Estonia (Martens, 2010) and Sweden (Söderström & Melin, 2012b) are contrasted by the challenges in Finland (Rissanen, 2010), Belgium (Mariën & Van Audenhove, 2010) and the United Kingdom (Beynon-Davies, 2011).

On a national level, to be able to cover the need of eID services across the whole public sector, ongoing efforts to increase the level of coordination, standardization and control have to take a vast number of aspects and needs into consideration. This to be able to gain the acceptance of a large group of affected actors in public as well as the private sector. Therefore, I argue that introductions of such eIDs must be seen as considerable challenges which in turn motivates further research in this area as exemplified by this dissertation. Since the implementation and use of eIDs are spreading across society, the health sector is also an area where the eID has become increasingly important (e.g. Halperin & Backhouse, 2008; Stroetmann et al., 2011). The introduction of Electronic Patients Records (EPR)4 systems and the increased demands of information security in the health sector when digitally storing and sharing sensitive patient data (Halperin & Backhouse, 2008) are strong incentives behind the introduction of eIDs which in turn also allow patients to access their own medical records online. In the private sector, the most successful examples of eIDs are commonly found in areas related to financial services such as online banking (Melin et al., 2013). As a result, in several countries, such as Sweden, actors in the banking sector have become the dominant providers of eID services to be integrated and used in public sector’s digital services (Söderström & Melin, 2012b). With the past development and future potential, it is, therefore, reasonable to assume that if the eID is important today, it will become even more crucial in the near future. This due to its important role as an enabler in the public sector’s strive for

The European Regulation for the electronic identification and trust services for electronic transactions (eIDAS) (EC, 2015)

4 Also referred to as Electronic Health Records (EHR) systems.
an increased coordination, standardization, interconnectedness, interoperability and provision of secure digital services on organizational, national as well as international level.

1.1.3 Current public sector eID challenges

Regardless of the opportunities for public sector eIDs acting as a common way of digital authentication in public as well as private-sector digital services, we are currently witnessing the results of trying to increase the level of coordination and control of eIDs on several levels in the public sector. This, in turn, being a result of the eID rising on national as well as sector specific digital agendas. However, these coordination efforts, in fact, turn out to be particularly challenging in their nature. The first example is the introduction of the national eID in Sweden (Svensk e-legitimation) with the aim of increasing the coordination and control of eID services used in public sector digital services. This introduction, initiated at the beginning of 2011 still, after more than five years, suffers from a lack of support and acceptance of affected actors in the public and private sector. This effort is already described as a high-risk program due to its limited resources and aim to cover the entire public sector (Melin et al., 2013). Moreover, this introduction aims at replacing the current eID solution in turn being a result of a weak central governance model (e.g. Söderström, 2012) and a successful private and public sector market convergence (Kubicek & Söderström, Submitted) with public sector authorities as Service Providers (SPs) and major commercial banks as Identity Providers (IdPs).

The second example covers eIDs for professional use which have long been a way of ensuring proper security levels in public organizations. The health care sector in Sweden, managed by government and tax funded to provide health care to all citizens, therefore is a part of the public sector that has only recently initiated the introduction of eIDs for professional use. These efforts are related to current law and regulations requiring strong authentication for increased security levels to ensure sensitive patient data as well as integrity. This eID solution to be used by medical and administrative staff in their professional role is provided by a dedicated national technical framework. However, in line with the national level, eID introductions in the health sector face similar challenges related to high levels of technological as well as organizational complexity (Hedström et al., 2016) and patient confidentiality (e.g. Anderson, 2006). Health care is a context where the introduction of ICT, in general, creates integrity and privacy concerns (Angst & Agarwal, 2009), hence the introduction of professional eIDs in this context results in anticipated as well as new challenges (Stroetmann et al., 2011). For example, strong professional roles and specific requirements, therefore, result in challenges such as lack of acceptance of the eIDs among medical staff (Hedström et al., 2016) as well as the relation between identities and eIDs affecting the use (Hedström et al., 2015). Therefore, I argue that these two examples of public sector eID challenges share several similarities regarding their incentives as well as implications in practice. For instance, there are clear indications of existing diverging perspectives of the eID being introduced, with on the one hand the actor coordinating the introduction and on the other hand affected
organizations or professionals pressured to accept and use the eID. These examples are also the result of clear external pressures (e.g. DiMaggio & Powell, 1983; Zucker, 1987) being put upon organizations to introduce the eIDs. Hence there are clear potential conflicts between the central government incentives and local requirements and needs in affected organizations. With potential conflicting views and central pressures to accept and use the eIDs, obstacles during these introductions should be imminent. Therefore, I argue that these challenges and obstacles serve as clear indications of eIDs as equally important as challenging to introduce on national as well as on organizational levels in the public sector. As a suggested approach to address these challenges, this dissertation focuses on the described lack of acceptance and particularly the active resistance to these eIDs among affected actors in organizations as well as in different networks and constellations. This is motivated by the potentially negative influence of this resistance on the eID introduction as a whole. Thus, I argue that a public sector eID facing a clear and complex resistance (e.g. Hirschheim & Newman, 1988; Laumer et al., 2016; Oliver, 1991) among affected actors, in turn potentially related to contradictory perspectives and demands (Scott, 1987), will face significant challenges during its introduction.

1.1.4 Need for a broader focus on public sector eIDs

Based on current eID challenges described above, I, therefore, would like to make a claim that there is a significant need for a broader focus of public sector eIDs in research as well as in practice. Historical dominating technical perspectives on eIDs (e.g. Collings, 2008) need to be challenged and revised. These challenges is also a direct consequence of increased complexity in our society including aspects such as identity, identification and ICT (Whitley et al., 2014). Hence, I argue that broader perspectives able to handle these complexities are needed. The problematic nature of the social context of this artefact can be related to research emphasizing the importance of acknowledging social aspects of ICT (e.g. Grint & Woolgar, 1995; Orlikowski, 1992; Walsham, 1993). Moreover, I argue that the eID is no ordinary ICT artefact, such as an information system or digital service with a clear, specific scope and purpose. Instead, the eID is totally dependent on its technical, organizational as well as social context in terms of service context, translations, attitudes, norms, values, actions and assigned meanings. For example, with a lack of a digital service context, the eID becomes completely useless resembling a key to something that does not exist. Accordingly, I argue that this context-dependency makes the eID a unique ICT artefact with vast opportunities as an enabler of secure services but at the same time related to significant challenges in different organizational and social contexts. Depending on the acceptance and use of the actor using it for authentication in a service context (Beynon-Davies, 2006) the eID is, therefore, an artefact with a clear social and technically intertwined character (Orlikowski, 2007). This can also be described as an artefact assigned with an institutional character (Kling & Iacono, 1989) since it also becomes a part of social structures guiding as well as restricting behaviour in organizations (Scott, 2014). The eID becomes embedded in cultural systems in organizations, also referred to as institutions (Avgerou, 2000). However, with a few exceptions, I argue that research focusing on eIDs have up
to this point mainly been of a descriptive or comparative character which in turn moti-
vates further studies aimed at broadening the context of study as related to the eID. In
ISR (see Section 3.1), the problematic relationship between the technical or material
aspects of an artefact, such as the eID, and its social context is no novelty (see Section
3.3), and difficulties to predict the consequences and outcomes of ICT introductions and
use in organizational and social contexts are basic problem areas of this research field
(e.g. Keil, 1995). Given its interdisciplinary character (e.g. Galliers, 2003a), ISR has a
long history of depending on other research disciplines for the appropriate theoretical
perspectives for the study of contemporary ICT related phenomena.

ISR, therefore, provides opportunities to find suitable theoretical perspectives in other
relevant areas, focusing on for example organizational and social behaviour, to be able
to further investigate these contexts of the artefact in focus. Perspectives such as the
ensemble view (Orlikowski & Iacono, 2001) and sociomateriality (e.g. Orlikowski,
2007; Orlikowski & Scott, 2008) are applied in efforts to address the intricate and com-
plex relation between the technical and the social. ISR is therefore very suitable as a
research field to approach current public sector eID challenges but so far, eID research,
as originating from the more technical research area of identity and identification
(Halperin & Backhouse, 2008), has not received much attention. In organizational stud-
ies, traditional perspectives focus on formal structures of organizations (Meyer &
Rowan, 1977) while the institutional perspectives apply a social perspective on collec-
tive behaviour in organizations (e.g. DiMaggio & Powell, 1983; Scott, 2014). Further,
institutionalist perspectives emphasizing the importance of acknowledging institutions
as shared social meanings apply a social constructionist stance (e.g. Berger &
Luckmann, 1967) to the concept of institutions and are often referred to as new institu-
tionalism (Avgerou, 2000) or neo-institutionalism (Scott, 2014).

Institutionalism is commonly applied in ISR to provide insights about social systems of
guidance and control in relation to ICT in organizations (e.g. DeSanctis & Poole, 1994;
Mitchell & Zmud, 1999). Within the eGovernment research field, institutional ap-
proaches are used to address the increased need for better understanding of the complex-
ity of ICT, organizations and institutions during government transformation while em-
powering all affected actors and acknowledging different individual perspectives (Luna-
Reyes & Gil-Garcia, 2014). Studies on eIDs apply this perspective (Kubicek, 2010;
Kubicek & Noack, 2010a) as a basis to investigate of how organizations react and man-
age when subjected to external institutional pressures of conformance and control (e.g.
Oliver, 1991). Accordingly, I argue that if the institutional perspective is applied in a
study of the introduction of public sector eIDs it will present the opportunity to
investigate further how social contexts of organizations in terms of values, norms, be-
liefs, rules and taken for granted assumptions (Barley & Tolbert, 1997). These systems
of social control (Berger & Luckmann, 1967), are affected by and in turn, also affect the
eIDs being introduced. The institutional perspective, therefore, provides a relevant theoretical lens for further investigating the pressure of conformance to introduce eIDs in the public sector as well as exploring the relation between the resistance to the eID and affected actors in organizations and other constellations and networks. In research, resistance to ICT implementations as a factor that needs to be acknowledged is long known (e.g. Keen, 1981; Markus, 1983) and perceiving the resistance as an institutional factor related to ICT is acknowledged (e.g. Davidson & Chismar, 2007; Starr, 1997). For instance, Sharma and Yetton (2003) describe the need of aligning or shaping it to facilitate ICT success as an example of research focusing on resistance as an aspect of ICT related organizational transformation and change (e.g. Cha et al., 2008; Modol et al., 2012). Regarding resistance as related to actions and behaviours, Lapointe and Rivard (2005) focus on how it can be handled from a management perspective. However, as a result of the literature survey (see section 2.3.4), existing studies seem fragmented and focused on for instance how this resistance, as a rather black boxed variable, can be managed and controlled in order to minimize negative consequences on ICT implementation efforts; a view in turn in agreement with (Laumer & Eckhardt, 2010). Nevertheless, there are some notable exceptions such as Janssen et al. (2012) introducing the concept of barriers in the institutional context as negatively affecting ICT adoptions. To avoid perceiving the focused resistance as just a variable to be managed, I argue that it should instead be seen as a process of institutionalization (Barley & Tolbert, 1997). This can be described as actors orienting their actions based on a common set of norms and values or shared systems based on knowledge and belief (Scott, 2014).

By focusing on this process, the creation and re-creation of the resistance to the eID among affected actors, better knowledge can be developed about the factors that cause this kind of resistance and how it influences as well as is influenced by the introduction process. As suggested, the organizational context has a very important role to play regarding how the eID will be perceived and translated by affected actors. These actors, such as organizations or employees, are all acting in a social context where the eID becomes a part of a complex relational context including technical, organizational as well as institutional aspects inherent to the organization as well as social aspects of the individual actor. To improve the understanding of resistance to public sector eIDs, I, therefore, suggest that this organizational level of analysis needs to be supplemented and synthesised with an actor level of analysis to be able to identify a potential relation between the resistance and the translations of actors affected by it. Further, Lamb and Kling (2003) put forth the need of an institutional perspective focusing on actors to be able to better understand the organizational context as related to ICT but this dissertation applies a different approach. The approach suggested in this work is an answer to this call since it includes synthesising an institutional perspective with a sociological actor and network focused perspective as motivated by the potential benefits of linking these perspectives. I argue that to be able to better understand affected actors and how they perceive, translate, influence and act as related to the eID being introduced, this actor
level of analysis must be performed prior to synthesising these findings with the institutional level of analysis. Approaches in sociology are focusing on actors as related to other actors such as actor networks can, therefore, facilitate this level of analysis with one perspective being Actor-Network Theory (ANT) (e.g. Latour, 1991; Law, 1999; Law & Callon, 1988). ANT is developed with the purpose of addressing the problematic relationship between the social and the technical especially in situations where the distinction and separation between these two aspects have been proven difficult (Callon, 1999). ANT is frequently applied in ISR (e.g. Bengtsson & Agerfalk, 2011; Walsham & Sahay, 1999) and Walsham (1997) describes it as a new way of “understanding the socio-technical nature of information systems” (Walsham, 1997, p. 470). Thus, for the actor level analysis, an ANT related framework called ‘the sociology of translation’ (Callon, 1986) seems particularly relevant since it acknowledges social structures and identity as well as emphasizes the importance of actors as perceived from their own perspectives.

This perspective can therefore potentially provide the needed emphasis on the power of actors’ translations as a phenomenon and a central force that influence as well is influenced by the introduction of the eIDs in a public sector context. The institutional perspective on resistance together with the perspective on the sociology of translation can, therefore, facilitate future public sector eID introductions by better knowledge of the influence of institutionalized resistance on the introduction process and a better understanding of its creation and re-creation in the social context of affected actors. What remains is then to identify how these two theoretical perspectives described above can be synthesised to provide the requested broader social and institutional perspective on introductions of eID in the public sector (see Chapter 4). Moreover, the described identified gaps in that will be addressed in this dissertation is the call for a process view on institutional aspects, broadening of the historical, technical view of the eIDs as well as acknowledging the complex context of public sector ICT artefacts. In addition, the merge between these two perspectives will also potentially provide new insights.

With the process view of affected actors’ translations as related to institutional resistance and seeking the appropriate theoretical means for further exploring this relation, this dissertation develops and applies a tentative socio-institutional framework. This framework emphasizes the eID in the social context of actors combined with the institutional contexts of organizations to be able to better understand and address the current problematic public sector eID context. This approach addresses the previously described lack of a broader focus on public sector eIDs. Further, a potential critic might argue that the term socio-institutional becomes a tautology since institutions, in essence, are social. However, I argue that term is still suitable since the prefix, in fact, is an abbreviation for sociological. It emphasizes the synthesis of the two analytical perspectives of sociology
and institutionalism\(^5\). Therefore, the emphasis is not put on the synthesized perspective ‘as a product’ but rather the synthesis ‘as a process’ bringing together these two perspectives. This also being in line with the clear process view on how institutional resistance develops. Nevertheless, I am fully aware of that sociology focuses on social behaviour where institutions are also included hence a certain degree of overlap still remains. However, I argue that this is something positive since it reassures that both these perspectives are related thus sharing similar underlying assumptions which in turn will facilitate a positive synergy between the two.

### 1.2 Research questions

Based on this background and motivation, the research questions guiding this study are described below. Three questions are formulated to facilitate the process of knowledge development ranging from the initial assumption (RQ-1) via identification and analysis (RQ-2) to the contribution of results (RQ-3). Each question addressed below will be highlighted followed by a more elaborate description.

(RQ-1) What influence does the resistance among affected actors have on the introduction of public sector eIDs for use in external and internal digital services?

The first question (RQ-1) focuses on the previously suggested assumption that the resistance to public sector eIDs among affected actors indeed negatively influences the introduction as indicated by current challenges in practice described above. This question seeks to establish the notion of the existence of an institutional resistance among affected actors as shared systems of norms and values or knowledge and belief that opposes the eID. This influence is further investigated with a focus on the eID introduction process, any efforts or neglect to handle it and consequences for the introducing as well as affected actors. The scope of the investigation is described as public sector eIDs for use in external digital services hence aimed at citizens and businesses and internal digital services for professional use in public sector organizations. Thereby, RQ-1 also directly responds to the previously presented claim for a broader perspective expanding the context of public sector eIDs since there is an underlying notion that this resistance exists in the social and institutional context as related to actors’ different translations of public sector eIDs and institutional resistance.

\(^5\) This approach is the result of a merger of two analytical perspectives hence not referring to sociological institutionalism as related to normative institutionalism in political science.
Introduction

(RQ-2) How can this resistance be related to actors’ translations of the eID for further analysis, synthesis and insights?

The second question (RQ-2) further investigates the institutional resistance, as confirmed by a positive answer to RQ-1. The focus here is on how the institutional resistance identified on the organizational level can be related to actors’ translations thus synthesising the institutional and sociological perspective as previously put forth. The aim of this question is, therefore, to locate the relevant existing theoretical and analytical perspectives and bring them together. This to be able to identify, describe and further analyse this relationship to provide new insights on the creation of institutional resistance as related to and a result of actors’ translations. In addition, this will also provide the opportunity to investigate how any efforts to handle the resistance on the organizational/institutional level, in turn, affects actors’ translation.

(RQ-3) How can these insights be structured and conceptualized in order to contribute to research as well as practice for less problematic public sector eID introductions?

The third question (RQ-3), requires RQ-2 to be confirmed and thus is relying on a successful synthesis between the two proposed perspectives of analysis. This question focuses on the potential insights of the identified and analysed relationship between the sociological (actors’ translations) and institutional (resistance) perspectives and how these insights can make a positive contribution to research as well as practice to address current challenges and facilitate future public sector eID introductions. Although this last research question can be seen as covered by the aim and contribution, to be able to provide guidance and transparency to this work it needs to be explicated.

1.3 Aim and contribution

As described, this dissertation rests on the underlying assumption that the public sector eID is to be considered an important enabler for eGovernment development in general and public sector digital services in particular. At the same time, practice currently struggles with an active resistance on national as well as organizational levels during eID introductions. I argue that challenges can be a result of underestimating the complexity of the eID and failing to correctly address important organizational and social aspects
of affected actors. Building on the previously suggested perspectives, this study develops and presents an approach to increase the understanding of how actors’ translations of the eID can be related to the institutional resistance to it on a national as well as organizational level. As derived from the research questions presented above, the general aim of this dissertation is, therefore, to contribute to research as well as practice in the following way:

To identify and describe the resistance to public sector eID introductions and to develop and present a synthesised framework for analysis and new insights.

This contribution also implies the development and application of the previously suggested socio-institutional framework. This to be able to analyse the institutional resistance while also being able to relate and trace this resistance to the social context of affected actors focusing on their individual translations on the eID. Thus, this dissertation focuses on the process of institutionalization of the resistance to an institutionally and socially embedded ICT related artefact (the eID). The dual contribution to research and practice can be described as to provide novel insights from the theorization and synthesis of a sociological and institutional perspective of the eID and facilitate less problematic introductions of public sector eIDs. In detail, contributions to research will be the motivation and insights of applying this socio-institutional framework on public sector eIDs to eGovernment research as well as lessons learned from bringing together the sociological and institutional perspectives to general ISR research. To accomplish this, the institutional resistance must first be identified and described with a focus on its influence on the introduction process as well as management efforts and consequences for affected actors. Actors’ translations will then have to be identified, described and analysed in order to relate these translations to the resistance on the institutional level for further analysis. This provides the synthesis of these perspectives to facilitate new insights on the creation of institutional resistance to public sector eIDs among actors and how these translations influence the creation and re-creation of institutional resistance. Thus, the detailed aim and contribution of this dissertation described above can be summarized as to:
1.4 Knowledge development

Regarding knowledge development, Goldkuhl (2011) puts forth the importance of being aware of the specific type of knowledge to be able to assess it. Based on this classification, the knowledge development taking place in this dissertation can be described as categorical, characterizing, explanatory and prescriptive as summarized in Table 2. As the basic form for of all knowledge development, **categorical knowledge** seeks to conceptualise the world (Goldkuhl, 2011). Hence, this type of knowledge aims at describing the basic concepts and notions of the studied context that form the knowledge base needed for further exploring the most specific aspects of the phenomenon. While, **characterizing knowledge** describes the properties of a categorized phenomenon, the aim of **explanatory knowledge** is to explain the phenomenon by giving causes, grounds, reasons and conditions. Finally, the aim of **prescriptive knowledge** is described as to provide guidance on how one should act in different situations thus this type of knowledge can be provided in the form of rules, prescriptions, advice et cetera (Goldkuhl, 2011).

<table>
<thead>
<tr>
<th>Developed knowledge</th>
<th>Research question(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>-Public sector eIDs</td>
<td>RQ-1, RQ-2</td>
</tr>
<tr>
<td>-Public sector eID introductions</td>
<td></td>
</tr>
<tr>
<td>-Institutional pressures</td>
<td></td>
</tr>
<tr>
<td>-Institutional resistance</td>
<td></td>
</tr>
<tr>
<td>-A'ctors’ translations</td>
<td></td>
</tr>
</tbody>
</table>
To be able to fulfil the aim and purpose of this dissertation, *categorical knowledge* needs to be developed in order to describe and categorize public sector eIDs as well as public sector eID introductions. This knowledge is needed to be able to address the described first research question (RQ-1). Further, categorical knowledge is also required to address the second research question in order to form the basis of the suggested relationship between actors’ translations and resistance to eID introductions. As described, the suggested institutional perspective to be applied on the pressure to introduce eIDs, as well as the resistance thereby, needs the basic concepts of institutional pressures and institutional resistance to be described. In addition, the suggested approach used for analysing actors’ translations also needs to be categorized in a similar way (RQ-2). Next, the development of *characterizing knowledge* is needed by the first as well as the second research question. In addressing the first question, this type of knowledge is needed to be able to describe the properties of the influences of resistance on eID introductions (RQ-1). For the second question, characterizing knowledge is needed to describe the resistance to eIDs in a more detailed way as related to implications in social and organizational contexts of affected actors. Characterizing knowledge is also developed when applying the approach for addressing actors’ translations (RQ-2). *Explanatory knowledge* is sought during the further investigation of the resistance to find out how this can be related to translations of the eID existing among affected actors. A soft social
causality is thereby implied (Goldkuhl, 2011) by applying the above proposed sociological and institutional perspectives for further analysis, synthesis and insights. Hence, this results in the development of knowledge regarding this relation between resistance and actors translations as well as identifying the appropriate approach (the socio-institutional framework) for analysis, synthesis and insights based on different perspectives as referred to in the second research question (RQ-2). The prescriptive knowledge developed focuses on the need of acknowledging the public sector eID as being part of a broader context as embedded in social and institutional contexts. The dissertation seeks to prescribe a needed move away from current narrow perspectives of the public sector eID since this is identified as one plausible cause to current challenges. The emphasis on the importance of acknowledging and a better understanding of resistance to the eID as related to institutional and social contexts of affected actors as well as the benefits of synthesising the institutional and sociological perspectives are also central.

As related to the third research question (RQ-3), the prescriptive knowledge developed is focused on the structuring and conceptualising of these insights as well as the development of propositions to be able to contribute to research as well as practice. Hence, insights facilitate the development of structures, concepts and propositions, in turn, facilitating future research in relevant areas as well as future public sector eID introductions. The knowledge developed is of an action oriented character (Goldkuhl, 2011) with the aim of facilitating research in research fields such as ISR and eGovernment as well as practice focusing on public eID introductions as the prescriptions and desirable goals of the knowledge developed (Goldkuhl, 2011). Although not included in Table 2, the knowledge developed can also be argued as being predictive or prospective (Goldkuhl, 2011) to a certain extent since failing to acknowledge and address social and institutional aspects of the eID in general and the resistance to it, in particular, will most likely result in problematic eID introductions.

1.5 Delimitations

To achieve the purpose, framing the dissertations specific characteristics regarding the applied theoretical and empirical approach become crucial. One aspect of this is to discuss the approach in the light of existing relevant theoretical approaches and focuses as well as empirical considerations and delimitations. Accordingly, these delimitations will be further described and motivated below.

1.5.1 Theoretical

One central character is the phenomenon put in the foreground, the introduction of a new or revised eIDs for internal or external use in public sector organizations. It would, therefore, be obvious to perceive this as an example of organizational change or organizational development and transformation thus relating it to this specific field of research. Organizational change and innovation could therefore be considered as motivated by this area’s interest in different aspects of change such as its nature, key concepts
as well as relevant strategies and approaches (Poole, 2004). This area focuses on aspects such as organizational development and transformation (e.g. Porras & Silvers, 1991), organizational change and barriers to change (e.g. Argyris, 1993), organizational change and development (e.g. Weick & Quinn, 1999) and structural inertia as related to organizational change (Hannan & Freeman, 1984). However, organizational change is an area specifically focused on “[C]hange and innovation and innovation in their own right, seeking to understand them as objects of scientific study, rather than in practical terms.” (Poole, 2004, p. 4). This is the process of seeking to identify processes and factors that shape innovation and change for increased understanding and manageability (Poole, 2004). However, this dissertation delimits itself from this field of research since the featured public sector eID introductions on national and organizational levels will be analysed with a focus on the deeper understandings of the relation between actors’ translations and institutional resistance rather than being examples of organizational change to learn from for increased future manageability. Hence, the process of organizational change as related to ICT is not focused in its own right. Hence the introduction becomes the context where actors’ translations and institutional resistance occur.

Despite the fact that management of resistance will be touched upon, the aim is not focused on an increased and more efficient manageability but rather to fulfil a need for increased understanding. Nevertheless, this increased understanding will in its most optimal form result in a positive contribution and in turn potential positive changes to how this kind of introductions are approached and managed. Furthermore, discourse analysis is a popular approach focusing on the spoken word and its involvement in the shaping of society (Fairclough, 2013) or to put it short - the study of language in use (Gee, 2014). Hence, it can be seen as a relevant approach to consider when analysing ICT related phenomena in an organizational context such as the public sector eID. Discourse analysis is also relational due to its focus on social relations rather than individuals or entities, transdisciplinary since it runs across conventional borders between disciplines and dialectical since it is not possible to clearly define discourse as a separate object (Fairclough, 2013). Discourse analysis can thereby be seen as based on the works of Wittgenstein’s perspective on language and meaning (Klein & Myers, 2001) applied in a wide range of studies in the ISR field (e.g. Avgerou, 2003; Heracleous & Barrett, 2001; Klein & Truex, 1995).

Nevertheless, I have chosen to delimit this dissertation from further analysing these meanings, communication and context as linked to symbols and language and how the semiotics and linguistics of the phenomenon (the eID) link to aspects such as context. Thus, the focus applied in this dissertation is on the institutional aspects and the social context of actors as a whole and not only on the semiotic and linguistic events in detail as focused in discourse analysis. This delimitation is also motivated by existing categorizations of ISR interpretive research based on underlying philosophical and conceptual
Introduction

foundations with one school linking back to the meaning of language (discourse analysis) and one closely linked to hermeneutics and phenomenology (Klein & Myers, 2001). Based on the notion that this dissertation rests on an interpretive and hermeneutic assumptions, the limitation from linguistics and semiotics could be seen as symptomatic. One could also argue that this study focuses on the importance of gaining user acceptance of ICT solutions such as the eID. Thus, proposed frameworks to maximize acceptance should be considered with examples such as the Technology Acceptance Model (TAM) (Davis, 1985; Venkatesh & Davis, 2000) and later developments such as UTAUT\(^6\) (Venkatesh et al., 2003). However, this dissertation clearly delimits from such approaches since the aim is not to maximize user acceptance in any way, but rather on an increased understanding of how actors’ translations can be linked to resistance in an institutional context. Thereby, it also delimits from other maximizing approaches such as best practices (e.g. Szulanski, 1996) and critical success factors (Holland & Light, 1999).

Further, information security is a research field important to relate to when investigating a security solution such as the eID. However, the research interest of information security is described as assuring a balance between information risks and controls (Anderson, 2003) this being the result of development into a more philosophical stance of the field than the historical focus on confidentiality, integrity and availability (Bishop, 2003). Although this dissertation acknowledges the role of the eID as ensuring different aspects of security such as information security, the focus of this work is not on how these risks can be potentially reduced or prevented but rather how these risks are related to different actors’ translations and in turn influences the development of a resistance to the eID. Therefore, at this point, my work on public sector eIDs delimits from the field of information security but nevertheless there are clear future potentials for merging ISR with research approaches focusing on the socio-organizational context of security related ICT artefacts such as the eID (see Section 10.5). This especially with the development of the subfield Information Systems Security (ISS) perceiving information security as related to the social and organizational context (Dhillon & Backhouse, 2001; Siponen, 2001).

This convergence in focus between ISR and ISS should provide opportunities for interesting results. As previously described, this study applies a new institutional perspective (e.g. DiMaggio & Powell, 1983; Scott, 2014) and consequently delimits this study from areas of interest in traditional institutionalism such as economical views and focus on formal structures of organizations (Meyer & Rowan, 1977). Nevertheless, there are clear financial incentives behind the cases of public sector eID introductions presented in this dissertation, for instance the aim of increased levels of efficiency in government. Thus, financial factors driving these introductions are still recognized but left unproblematized since they are not included in the aim and scope of this work. This also automatically

\(^6\) Unified Theory of Acceptance and Use of Technology (Venkatesh et al., 2003)
delimits the present work from prior perspectives emphasising formal and rational organizational processes as put forth in classic institutionalist perspectives by scholars such as Weber, Veblen and Barnard. Further, this work is applied in the ISR field where social and organizational aspects of ICT are emphasized and performed in line with ISR studies applying social theory (see Section 3.3). In addition, a perspective of sociology applied in the field of institutionalism is also applied (see Section 4.2). Accordingly, I argue that the social or sociological perspective becomes so central to this work resulting in need of referring the applied institutional perspective as new or neo-institutionalism as rather superfluous. Therefore, I have delimited from the use of this prefixes (new, neo) throughout this work which in turn I argue has a positive effect on clarity and transparency. The new institutionalist perspective applied in this dissertation will, therefore, be referred to as an institutionalist perspective.

1.5.2 Empirical

In addition to theoretical delimitations, this dissertation is also subject to several empirical delimitations applied during data collection (see section 2.5). However, these also have clear theoretical implications since the including or excluding of empirical perspectives, in turn, guides the identification of relevant literature. The most obvious one being the fact that this study is based on two case studies performed in different public sector contexts. Hence, this delimits it from any private sector organizations. However, this focus is symptomatic with respect to the aims of the focused introductions as well as the position of this work in the eGovernment research field. Nevertheless, private sector actors will still play an important role, especially in the eGov case. This study also puts social and institutional aspects of the eID in the foreground thus leaving the technology or technical infrastructure of the eIDs unproblematised to a large extent. Motivated by the aim and contribution, this is in clear contrast to previous research focused on technological aspects of the eID (e.g. Breward et al., 2009; Hansen et al., 2004; Jøsang, 2013; Tauber et al., 2010).

However, this is fully in line with the above presented call for of a broader perspective expanding studies into organizational and social contexts of the eID to be able to better address current challenges. Further, this study also delimits from further analysing and problematizing the public sector policies governing the focused introductions of eIDs by applying a more consequentialist perspective (Tanner et al., 2008). Hence, the consequences and outcomes of these introductions are focused rather than questioning why and how the governing policies are developed and implemented in the first place. Further, the two empirical cases selected for this study is described in detail in the next chapter (see Section 2.4). However, in the second case focusing on an eID for professional use in health care, there are some clear empirical limitations clearly influencing how this case is approached in this work. Thus, I am fully aware that researchers and skilled practitioners in related fields such as eHealth may argue that this work delimits from several significant and important aspects of the health care sector such as health care organizations as complex professional systems (e.g. Anderson & McDaniel Jr,
Introduction

2000) with a clear relation between organizational aspects and clinical outcomes (Aiken et al., 1997). However, since this study is not positioned in fields such as health care informatics or eHealth, the eID in the health care case will not be analysed and discussed in terms of such organizational characteristics or clinical implications. Hence, findings and insights brought forth, in this case, will focus on the eID in the health care context in a general sense as an artefact providing authentication in an internal digital service context. I am fully aware of clinical implications as a very strong power of influence on ICT in a health care context, and there certainly are such implications behind the views put forth by respondents in this case. However, to facilitate a level of abstraction that will facilitate the supplementary role of this case in this work as a whole, these implications will instead be investigated and analysed in the form of the specific requirements of the eID put forth by affected actors in the organization. Thus, in line with the focus on actors’ translations applied in this work, these requirements are in turn affected actors’ translations of the implications of the eID in their particular operational health care context as being of a clinical or administrative character.

Nevertheless, while a lack of addressing such specific health care aspects can be seen as a shortcoming from a health care perspective, I nevertheless argue that the applied more general view, in turn, can facilitate a potential development of an increased understanding and consensus of eIDs across organizational boundaries and structures in the public sector. There is also a clear delimitation as related to the described focus and emphasis put on introductions of public sector eIDs, hence delimiting this work from any empirical studies of the implementations of public sector eIDs. This is motivated by the focus on introduction as ‘bringing something into use or practice’ (OED, 2016b) thus referring to the verb of ‘to introduce’ and consequently delimiting from implementation as referring to the verb of ‘to implement’ with the meaning of ‘carrying something into effect’ (OED, 2016a). This delimitation seems to be in line with existing research where IS implementations historically have been approached from technical and deterministic perspectives (e.g. Kwon & Zmud, 1987) seeking dependent variables for IS implementation success (DeLone & McLean, 1992; Petter et al., 2008).

Throughout this dissertation, I will refer to the process of bringing of the eID into a public sector practice context as an introduction hence choosing a less deterministic route and instead focusing on social and organizational implications. Applied delimitations also result in the concept of electronic signatures or signing (eSig, eSigning) being placed in the background in favour of the authentication provided by the eID. Often also referred to as digital signatures, eSigning is the digital equivalent of a handwritten signature ensuring the authenticity and non-repudiation of a digital document or message. Although, clearly related since directives and investigations focusing on electronic signatures on national (e.g. SFS 2000:832; SFS 2011:803) as well as EU level (e.g. 1999/93/EC; EC, 2008) have been governing requirements of eIDs in the past. However, there is the tendency of assigning the eID with its own set of directives and regulations
hence acknowledging the different aspects of these two processes related to on the one hand secure authentication and on the other hand signatures to ensure non-repudiation. From a user’s perspective, the concept of eSigning has become increasingly intertwined with the eID since the process of electronically signing is often facilitated by the same technical artefact, e.g. computer software or mobile app, as the authentication. However, from a service provider’s perspective, although associated with the same artefact (the eID), eSigning is significantly different from the eID with a different purpose as well as technical implementation and handling. IdPs also charge SPs using their eID and eSigning services by different tariffs. Although eSigning will be covered to some extent in the case descriptions of the national eID case (see Chapter 5) this aspect of the eID will not be problematized and analysed any further since this dissertation perceives eSigning as another important and significantly different context of use for the eID than the focused process of authentication.

1.6 Intended audiences

This dissertation is presented with a dual contribution to research as well as practice. However, since this is mainly an academic product, the primary intended audience are fellow researchers in areas such as ISR and eGovernment but my intention is also to address skilled practitioners interested in eIDs in general public sector eIDs in particular as a secondary audience. Since this work also focuses on challenges related to an ICT artefact that is highly dependent on its organizational as well as social context it should also interest researchers focusing on the deeper contextual structures, implications and consequences of such artefacts. For skilled and reflective practitioners in the eID area, such as business specialists or architects, policy makers and information security specialists, it also provides examples of two eID introductions that face significant challenges hence it also serves as proof of current implications and handling of such issues. Further, this dissertation is also an example of an interdisciplinary approach applied in ISR which in turn synthesises two different analytical perspectives, the sociological and the institutional, with theoretical perspectives such as ISR, eGovernment, public sector ICT and eID research. It may also inform researchers interested in this type of theory development in the search for novel insights. This work should also serve as evidence of the applicability, and feasibility of applying a social actor and network focused perspective such as the sociology of translation (Callon, 1986), in turn, related to ANT (e.g. Law & Hassard, 1999). Researchers interested in similar actor network approaches may therefore also benefit from these parts of the analysis as well as presented insights and lessons learned.
1.7 Dissertation outline

This dissertation is divided into four central parts each with related chapters as illustrated in Figure 1. Since these parts are clearly dependent and interrelated, relationships between the parts are also illustrated by the arrows.

Part I – Starting points

Chapter 1. Introduction presents the background, central challenges, knowledge gap in research and practice as well as the aim and guiding incentives (research questions). In addition, the intended contribution, knowledge development and delimitations are also brought forth. Chapter 2. Research perspective and methods provide the applied research perspective and methods covering relevant scientific and methodological aspects ranging from underlying assumptions to applied methods such as data collection and analysis. Covering guidance, delimitations and methodological aspects as well as knowledge development, Part I provides the starting points that guides the following theoretical and analytical perspectives (Part II) as well as empirical evidence and analysis (Part III). In addition, Part I also presents the point of departure of the dissertation to be addressed in the final chapter in Part IV.

Part II – Theoretical and analytical perspectives

Chapter 3. Theoretical perspective is presented with the aim of describing the theoretical perspective and hence covers relevant fields of existing research such as Information Systems Research (ISR), eGovernment, different views on social and organizational aspects as related to ICT and of course eID research. Chapter 4. Analytical perspective provides the theoretical basis for the selected analytical approach as grounded in institutionalism and sociology. The proposed framework for analysis is presented to conclude this chapter. These theoretical and analytical perspectives (Part II) provides the analytical approach for translation analysis in Part III as well as the synthesised concluding analysis and discussion (Part IV).

Part III- Empirical evidence and analysis

Chapter 5. eGov eID and Chapter 6. eHealth eID covers the two cases focusing on the national eID (eGov eID) and the professional eID in health care (eHealth eID) with a background followed by different perspectives brought forth by different actors involved in, or affected by this process. Chapter 7. Translating the eGov eID and Chapter 8. Translating the eHealth eID present the analytical findings from the applied sociological perspective in the form of translation analysis performed on the eGov and eHealth cases respectively. Accordingly, Part III, provides the empirical evidence and first stages of analysis thus provides an important input to the final analysis and discussion in Part IV.
Part IV – Discussion and conclusions

Chapter 9. Concluding analysis and discussion presents the synthesised analysis as based on the institutional and sociological perspective where findings are further discussed in the light of theory presented in Chapter 3 and 4. Chapter 10. Conclusions, implications and future research, the final chapter, presents conclusions, implications for research and practice as well as addresses the research questions. A quality assessment and suggestions for future research are also presented. Conclusions and implications in Part IV are also clearly related to the starting points (Part I) particularly regarding the research questions, aim and contribution.
1.8 A reader’s guide

Although this dissertation is written in a straightforward manner with a clear progression from incentives, perspectives, empirical findings, analysis and conclusions, it is fully possible to select separate parts for reading and still get a good picture of these parts. Accordingly, suggested reading is presented with this chapter wise reading in mind. References to relevant prior as well as coming sections are also made throughout this dissertation. Some typical examples of reading interests with suggested chapters are presented in Table 3.

Table 3. A reader’s guide

<table>
<thead>
<tr>
<th>Reading interest</th>
<th>Suggested chapters</th>
</tr>
</thead>
<tbody>
<tr>
<td>Overall motives, aims and contributions</td>
<td>1. Introduction</td>
</tr>
<tr>
<td></td>
<td>10. Conclusions, implications and future research</td>
</tr>
<tr>
<td>Theoretical and analytical perspectives</td>
<td>3. Theoretical perspective</td>
</tr>
<tr>
<td></td>
<td>4. Analytical perspective</td>
</tr>
<tr>
<td>Translation analysis (ANT)</td>
<td>4. Analytical perspectives</td>
</tr>
<tr>
<td></td>
<td>7. Translating the eGov eID</td>
</tr>
<tr>
<td></td>
<td>8. Translating the eHealth eID</td>
</tr>
<tr>
<td>The national eID introduction</td>
<td>5. eGov eID</td>
</tr>
<tr>
<td>An eHealth eID introduction</td>
<td>6. eHealth eID</td>
</tr>
<tr>
<td>Synthesizing translations and institutions</td>
<td>4. Analytical perspectives</td>
</tr>
<tr>
<td></td>
<td>7. Translating the eGov eID</td>
</tr>
<tr>
<td></td>
<td>8. Translating the eHealth eID</td>
</tr>
<tr>
<td></td>
<td>9. Concluding analysis and discussion</td>
</tr>
<tr>
<td>Concluding analysis and discussion, conclusions,</td>
<td>9. Concluding analysis and discussion</td>
</tr>
<tr>
<td>implications and further work</td>
<td>10. Conclusions, implications and future research</td>
</tr>
</tbody>
</table>
2. Research perspective and method

This chapter describes the research perspective and method applied to fulfil the aim and contribution presented in Chapter 1. Underlying research assumptions, perspectives and the role of theory are described and motivated. The applied research method, selection of cases to study and data collection techniques are covered. The applied analytical strategy is described followed by the synthetization of different analytical perspectives. The quality of the approach will be discussed followed by this dissertation’s practical relevance. The chapter is concluded with a presentation of publications as well as relevant ethical considerations.

2.1 Introduction

Since writing a dissertation is a considerable undertaking with respect to time and effort, my personal background in relation to this work becomes highly relevant for my role as a researcher. Before I started as a PhD candidate, I had the opportunity to attend a renowned European Conference in Information Systems Research (ISR)\(^7\), and I especially remember listening in on a very interesting panel discussion. Suddenly a quite provoking question, as interpreted by me, is raised by one of the panel members; a senior researcher in the field. Unable to recollect the exact words but clearly remembering that the question itself quite questioned the existence of entire ISR field. I remember the feeling of being intrigued but at the same time quite concerned about the reasons behind this question. Raised by, from what I understood, an authority in the field, this question is obviously challenging the very existence of the research field at a leading European IS Conference. I remember thinking to myself back then: Should not the ISR field itself be pretty settled, obvious and self-evident in this kind of forum? Is this a sign of a fragmented research field with a clear lack of self-confidence?

Nevertheless, this episode intrigued me and sparked my interest to learn more about this field of research. Later when developing my own view of the research field, I realize that this first episode is merely the consequence of a research field that attracts a strong base of researchers representing a multitude of relevant perspectives. Hence, disputes like the one described above simply indicates that the ISR field is alive, well, constantly changing and questioning itself (see Sections 3.1.1). The interdisciplinary character of this research domain, in turn, creates the flexibility and adaptability of the field that I argue are very important to be able to address the challenges best investigated from a social science perspective. As described, the problems addressed in this dissertation are related to the social and institutional context of public sector eIDs as the featured ICT

artefact, but I argue that these challenges by no means are unique for this particular context. Since the technology of today develops very rapidly, introductions are carried out at the same rate often focused on technology while misjudging or even disregarding social and organizational implications. Having a history of working as an ICT professional, I have also witnessed this evident lack of reflective behaviour and contextual perspectives related to ICT introductions. The potential of ISR to address these non-technical challenges of ICT together with my strong personal drive of to contribute to practice as well as research results in a strong belief in the importance of this work; and also one of the reasons why I started my PhD. Moreover, I first came across the concept of eIDs in fall 2010 during my senior master year. Later, in spring 2011, I am presented with the opportunity to write my master thesis (Söderström, 2011) as part of a research project focusing on the future use of eIDs; a project that also finances part of my dissertation. As it turns out, this also coincides with the Board beginning its mandate to coordinate and introduce the next version of the Swedish public sector eID (see Chapter 5).

My master thesis focuses on the emergence and current status of this national eID aimed at citizens and businesses in a public sector online service context. It concludes that the eID, the current market solution provided by the banks as identity providers, is perceived as a successful solution and a result of positive efforts of strong individual actors and positive relations with identity providers on the market. Hence, the central governance during this emergence is rather weak and mainly focused on updated framework agreements with identity providers. Therefore, the introduction of a new version of the eID as managed by the Board applies a completely different set of incentives aimed at supporting eID services for the entire public sector. Thus, in my master thesis I describe this as a potentially challenging and problematic eID effort (Söderström, 2011). Since this dissertation continues this work and further investigates public sector eID introductions with the national eID as one of two covered cases, I have now the opportunity to come full circle and verify the challenges as predicted by my master thesis which, on a personal level, is a very rewarding step in itself.

2.2 Research perspective

2.2.1 Philosophical assumptions

To be able to understand what guides and influences research, addressing the underlying philosophical assumptions becomes important (Myers & Avison, 2002; Myers, 1997). Moreover, to be able to conduct and evaluate research you must have the knowledge and provide information of what drives it on an underlying philosophical as well as methodological level. Discussing these aspects in research, it is common to speak in

---

8 The Future Use of Secure electronic identification (FUSe) project led by the division of Information Systems at Linköping University and funded by the Swedish Civil Contingencies Agency (MSB) between 2011 and 2015.
terms of epistemology, how knowledge is acquired (Hirschheim, 1985; Hirschheim, 1992) and ontology, how the nature of reality is perceived (Denzin & Lincoln, 1994a). These underlying perspectives are often referred to as research paradigms (e.g. Hirschheim & Klein, 1989) can be seen as basic systems of beliefs guiding the researcher (Guba & Lincoln, 1994). In addition, research paradigms also relate to the validity of research and directly affects what methods should be considered as appropriate (Myers, 2009). Regarding epistemology, since there is no absolute viewpoint or truth, knowledge can be described as the asserted often supported by empirical evidence, which gains acceptance of societal groups where in turn the criteria of acceptance are based on agreed sets of conventions (Hirschheim, 1985).

Accordingly, these agreements in applied fields such as ISR, together with philosophical assumptions and methodological approaches, set the agenda for a study in order for it to be able to gain scientific acceptance. Although ontology is less often referred to in literature, I argue that these underlying assumptions are equally important. The methodology applied is closely related to and influenced by a certain view of the world (Corbin & Strauss, 2008). Therefore I argue that the ontology of this dissertation is relativist or constructionist motivated by the reality in focus being based on social and experiential mental constructions as inherent to individuals or shared among groups of individuals (Guba & Lincoln, 1994). Hence this ontology is related to constructionism\(^9\) by the development of reconstructed understandings that should be trustworthy as well as authentic (Denzin & Lincoln, 1994a). Thus, the guiding social structures of institutional resistance and actors’ translations of public sector eIDs are also social and subjective constructions (Hirschheim, 1992).

This approach is in clear contrast to other ontological perspectives such as external realism based on an independently existing reality (Walsham, 1995b). Accordingly, these intra- and intersubjective constructions become a reality being investigated in this dissertation in the form different actors’ translations as well as institutional resistance to the eIDs being introduced. With respect to its epistemological stance, based on a categorization by Chua (1986), this work can be considered as interpretive since knowledge is obtained in social interaction between the researcher and the respondent during interviews. In order to develop knowledge, I, as a researcher, investigate and interpret and try to make sense of social and intersubjective meanings and actions as assigned or related to the eID (Chua, 1986). Accordingly, interpretive knowledge clearly diverges from positivism with its distinct view of scientific knowledge as based on facts and values (Walsham, 1995b) developed to create a predictive understanding of phenomena.

\(^9\) There seems to be a language confusion here where constructivism (e.g. Guba & Lincoln, 1994) and constructionism (Berger & Luckmann, 1967) are used interchangeably to refer approaches building on social constructions of reality; this also confirmed by e.g. Alvesson and Sköldberg (2008).
(Orlikowski & Baroudi, 1991). Regarding its methodological implications, the described underlying assumptions also motivate this dissertation to be categorized as qualitative with its clear focus on the development of investigating and understanding the resistance to public sector eID introductions as a social phenomenon (Myers, 1997). This as opposed to quantitative approaches based in natural sciences (Myers, 2009) with their aim of observing variables and testing hypotheses (Bacharach, 1989). Accordingly, this dissertation’s ontology and epistemology influence as well as motivate the applied research approach described next. In addition, this dissertation also becomes an answer to previous calls for broadening the philosophical assumptions in ISR (e.g. Orlikowski & Baroudi, 1991).

**Ontology: Relativism/constructionism**
- Perceiving the world as consisting of intra- and intersubjective constructions

**Epistemology: Interpretivism**
- Obtaining knowledge as interpreted from social interaction

### 2.2.2 Interpretive research

The aim of interpretive research in ISR is to develop an understanding of the context of information systems and how these are in turn influencing as well as influenced by their contexts (Walsham, 1993). Hence, this is fully in line with the applied broader contextual focus of public sector eIDs applied in this work. Further, one essential concept of interpretive approaches is the aim to develop an understanding of the subjective meanings of the individuals in the focused domain (Goldkuhl, 2012). In this work, these subjective meanings are exemplified by the focus on actors’ translations of eIDs and the development of an understanding of how these translations turn into an institutional resistance to it. Accordingly, this aim is in clear contrast to positivistic approaches emphasizing internal and external validity, generalizability, reliability and objectivity (Denzin & Lincoln, 1994a). Moreover, this perspective presents the opportunity to develop knowledge through human interpretations and meanings (Myers & Walsham, 1998; Walsham, 1995a) by an increased understanding of the deeper structures of the phenomenon (Orlikowski & Baroudi, 1991). Interpretive research posits that there is no objective reality to be studied but instead puts the focus on inter-subjectivity and knowledge as a social construction of reality. Hence, I argue that this forms a strong link between interpretive research and social constructionism, a theory of knowledge development, which perceives knowledge of the world as socially constructed (Berger & Luckmann, 1967). Thus, due to its strong implications on knowledge development, the interpretive approach is strongly related to the previously described ontological as well
as the epistemological level of this dissertation. However, social constructionist approaches can also be accused of being anti-realist and denying that knowledge can be a direct perception of reality (Andrews, 2012). Nevertheless, I argue that the interpretivist perspective emphasises the epistemological level hence the existence of an independent and objective reality is fully compatible with this view (Andrews, 2012). Further, the type of knowledge developed in interpretive research data is often collected in a qualitative way due to the focus on the interpretations and social contexts of information systems. Accordingly, the interpretive perspective has clear methodological implications on this work described in later sections. Accordingly, this type of research can never be objective since the researcher guides the process as well as interacts with respondents (Schwandt, 1994; Walsham, 1995a). However, I argue that this poses no problem since objectivity is never the aim of these type of research. Dominated by the positivist paradigm in the past (Chen & Hirschheim, 2004), this emphasis on human interpretations and meanings (Walsham, 1995b) has become increasingly important and is by now well established and accepted in the ISR field (Walsham, 2006).

This can be seen as a consequence of previous positivist approaches failing to deliver positive results. Moreover, the interpretive perspective offers aid to increased understanding of human thought and action and presents an opportunity to deepen the insights related to ICT (Klein & Myers, 1999). This is, therefore, the result of the acknowledgement of the importance of social issues related to information systems in ISR and in turn the interpretive perspective (Walsham, 1995b). The interest in interpretive research also results in an increased application of the underlying perspective of hermeneutics (Butler, 1998); as referring to the theory of interpretation and meaning (Bleicher, 1993). Hermeneutics supplies the needed philosophical basis to develop the understanding of phenomena through their assigned meanings (Orlikowski & Baroudi, 1991). This process often referred to as the hermeneutic principle or circle (Butler, 1998). Originating from the classical rhetoric of interpretation of texts, this principle prescribes that the understanding of the whole guides the understanding of its individual parts but the understanding of the whole can only be reached through a cumulative understanding of the individual parts (Gadamer, 1993).

This principle, therefore, allows the researcher to let the interpretations of the inherent parts of a phenomenon guide as well as be guided by the interpretations of the phenomenon as a whole. The hermeneutic principle, operationalizing the epistemology of this dissertation, is related to constructivist hermeneutics where the interpreter enters the interpretive norms of a community (Butler, 1998). Accordingly, this converges with the aim of developing a deeper understanding of how actors’ translations are related to institutional resistance to the eID. To be able to interpret actors’ translations, any pre-interpretations such as related to norms and values in the shared among actors in the organization have to be revealed which in turn is facilitated by the analytic perspective on actors’ translations (see Chapter 7 and 8).
Pre-interpretations and the concept of double hermeneutics should also be taken into account since this concept takes these important pre-interpretations in consideration (Giddens, 1984). Therefore, I argue that it is important that the researcher is aware of interpretations of respondents’ statements as in turn originating from their individual interpretations and pre-interpretations of their own worlds. This dilemma also being described as the interpretation presented by the researcher becoming the construction of the construction of the actors studied (Schwandt, 1994). Although hermeneutics may apply to the general research perspective, it can also be applied to specific methodologies such as literature reviews (Boell & Cecez-Kecmanovic, 2010, 2014). Thereby, I argue that the hermeneutic principle becomes very important and applicable in every situation where the development of an understanding of a complex area is needed, such as a research topic or field or a specific phenomenon such as the public sector eID.

The ontology of this dissertation previously described as relativist/constructionist also forms a strong link to the hermeneutic perspective since interpretations and meanings, in essence, are intra- and inter-subjectively constructed. Regarding critique put forth against ISR in general and interpretive research, in particular, this approach has been faced with the challenge of being perceived as a less legitimate research field due to its applied nature (Hirschheim & Klein, 2003). This creates a risk of scholars choosing academia as main stakeholders since they also control the advancement of researchers (Hirschheim & Klein, 2003). Thus, this potential alienation of research from practice is actively addressed in this work with its described strong emphasis on contributing to research as well as practice (see Section 1.3).

2.2.3 The role of theory

Theory in research is described as “[...] a statement of relationships between units observed or approximated in the empirical world.” (Bacharach, 1989, p. 498). Hence this view of theory focuses on the role of theory to provide insights, clarity and plausible explanations for observations made in the empirical world. Further, theory can also be defined as the sought after the output of research as a result of a systematic accumulation and development of knowledge with the aim of enlightening professional practice (Gregor, 2006). Existing theory is of great importance to research, and it is used in multiple ways to inform and influence research but can also introduce significant limitations that need to be considered. The use of theory in the first stages of research aims at creating an initial theoretical framework or theoretical basis that in turn takes existing research and knowledge into account to act as informants to the empirical work performed (Walsham, 1995b). However, considering theoretical perspectives as an inspiration and guide a priori also introduces a potential risk of introducing bias as well as potentially limiting empirical findings (Eisenhardt, 1989). It also challenges the openness to data as prescribed in interpretive research (Walsham, 1995b) but at the same time bring opportunities of further development and refinement of existing research. Accordingly, several existing theoretical perspectives is actively used to guide the research performed in
Research perspective and method

this dissertation where a need for a broader perspective on public sector eIDs is presented (see Section 1.1.4). Hence, existing research can also be used for the purpose of identifying gaps in existing research that need to be addressed in this work exemplified by the call for a broader perspective on public sector eIDs. Thus, in my opinion, extant theory guides and frames rather than restricts and limits the work presented in this dissertation. The aim is to let this dissertation progress in a direction where it can provide positive insights and contributions to research as well as practice while at the same time eliminating the risk of overlapping and reinventing already existing research (Goldkuhl & Cronholm, 2010). Regarding the risk of existing theory introducing bias and limiting empirical findings, I would rather state that theory in this dissertation is actively used to provide empirical insights in areas in need of further knowledge development. Theory can also be used as part of an iterative process of data collection and analysis. This provides a dynamic use of theory to support this process where theory can be identified, tested against empirical data and possibly be expanded, revised or abandoned (Walsham, 1995b).

Accordingly, existing theory is actively used during the qualitative data analysis in the stage of theoretical matching (Goldkuhl & Cronholm, 2010) where emerging insights and concepts as derived from data analysis are confronted with existing theory further informing the analysis. This also enables the researcher to handle any identified conflicts with existing extant literature as an opportunity by deepening insights (Eisenhardt, 1989). As an example, this dissertation contrasts existing research on institutional pressures and management of such pressures by instead focusing on institutional resistance to such pressures and how these emerge as related to actors’ translations thus potentially presenting deeper insights of the underlying social structures of these concepts (see Section 4.4). In addition, the later described applied iterative analysis approach of continuous empirical testing of the developing theory also introduces an abductive strategy (Patel & Davidson, 2003) to this work where the focus and reasoning constantly shifts from observation, empirical data, to theory and back again (cf. the hermeneutic principle described above). Moreover, theory viewed as the final result or output from research can be defined as concepts, conceptual frameworks, propositions and mid-range theory (Eisenhardt, 1989).

Thus, concepts are ideas with involving generalizations or abstractions of reality hence they become applicable in several contexts sharing similar key characteristics. Conceptual frameworks are specific ways of approaching a field of study, or a set of interrelated assumptions and concepts (Rodman, 1980) and propositions are arguments based on important insights of special interest that contribute to increased understanding of research and practice (Eisenhardt, 1989). Accordingly, this dissertation includes all these aspects of theory development with the use of concepts and constructs, developed during qualitative analysis and the development of a tentative conceptual framework to facili-
tate further analysis of the suggested relationship between actors’ translations and institutional resistance. In addition, based on findings and insights put forth, propositions are also presented in the final chapter. Accordingly, these different types of theoretical results (Eisenhardt, 1989) can be clearly related to the described three research questions. Hence, developed concepts are used to identify and describe the resistance to public sector eID introductions (RQ-1), the conceptual framework enables the analysis of the relationship between actors’ translations and resistance (RQ-2) and emerging concepts and propositions are presented to contribute to research as well as practice (RQ-3) (see Section 1.2). In addition, this work also aims at developing theory in the middle range (mid-range theory), described as a theory of abstract concepts from extant reference theories that are modified to the ISR context to possibly enrich existing mid-range theory (Grover & Lyttinen, 2015). This will be accomplished by synthesising theoretical perspectives of sociology with institutionalism into a conceptual framework in order to identify and investigate the suggested relationship between actors’ translations and institutional resistance hence addressing the described second research question (see Section 1.2). As described, ‘the sociology of translation’ (Callon, 1986) and institutional pressures (Oliver, 1991) are examples of such adapted reference theories each modified to some extent to facilitate new insights to the ISR context regarding public sector eIDs.

Although Eisenhardt (1989) adopts a positivistic view of the developed theory when emphasizing generalizability across contexts and the need of testing, Walsham (1995b) clearly points out that this need does not apply in the interpretive domain of research thus development of theory should still be emphasized and desirable. Accordingly, I argue that generalizability, as translated to the research context of ISR, is still of considerable importance and it will be further elaborated in a later section due to its dependence of the chosen methodology. Further, critique has been put forth against mid-range theory as opposed to grand theories from reference disciplines as associated with a high level of abstraction and generalization unbound in time and space (Bacharach, 1989). This concerns ‘borrowed theories’ not being sufficiently adapted and/or extended into the ISR context resulting in models that are difficult to handle regarding the consolidation of knowledge (Grover & Lyttinen, 2015).

With this in mind, this dissertation strives for a high level of transparency and builds on clearly defined theoretical constructs and concepts of actors translations and institutional pressures with the latter adapted and extended into institutional resistance. Hence, by making the adaptation and modification of concepts in extant theory explicit, I argue that this counteracts the black boxing of theory application and makes transparent the development of mid-range constructs and propositions. My aim of clarifying the contributions as well as potential generalizations will also provide a generative potential for future studies using and further extending the mid-range theory proposals and constructs presented in this dissertation.
2.3 Research method

2.3.1 Interpretive case studies

There seems to be no standard definition of a case study in literature but the following description provides a good explanation of this method for collecting empirical evidence in the context of this dissertation: “A case study examines a phenomenon in its natural setting, employing multiple methods of data collection to gather information from one or a few entities (people, groups, or organizations).” (Benbasat et al., 1987, p. 370). Although I argue that the definition of ‘one or a few entities’ can be challenged as being somewhat imprecise, the case study with its focus on developing a deeper understanding of a phenomenon in its actual real-world context clearly distinguishes it from other methods such as experimental studies trying to control specific variables and observe outcomes. There is a need for case studies when boundaries between the phenomenon and context are not clearly evident (Benbasat et al., 1987; Yin, 2014) and when it is desired to avoid any control or manipulation while collecting qualitative data (Benbasat et al., 1987). The case study provides a holistic view of a particular setting or context to be studied and case studies are often applied in studies aiming at developing an understanding of complex social phenomena (Yin, 2014). Hence, the public sector eID and its social and institutional context where an unforeseen resistance arises is an example of such a complex social phenomena where ‘the context of messy real-life situations’ (Myers, 2009) needs to be approached accordingly to develop understanding.

Based on the research questions previously described, this study clearly requires an approach that is exploratory in nature (Myers, 2009). This since it seeks to investigate the suggested existence and relationship between institutional resistance and actors’ translations as related to the phenomenon (the eID). Accordingly, I argue that it would not be possible perform this work in another way than in the form of an interpretive case study. Case studies are also categorized as being intrinsic, instrumental or collective where the intrinsic case study, as applied in this dissertation, aims at developing a better understanding of a particular case. Hence the case is not selected as showing representative signs of other cases but instead of its uniqueness (Stake, 1994). The two public sector eID cases described below are not selected for their representativeness of others but rather on their uniqueness and potential of bringing new insights provided by this opportunity to study these ongoing eID introduction processes. The introduction of the eIDs will be studied while these are actually being introduced. This uniqueness provides the opportunities for delivering results that are unique or particular in character. However, eIDs are neither unique, nor a novelty to public sector organizations but to be able to study the introduction of such eIDs during its actual introduction while focusing on actors’ translations presents a unique opportunity for a deeper understanding of the social and institutional challenges faced during this process. However, the case study is not a methodological choice made a priori, but rather a choice related to the object to be studied. Hence, it should be the nature of the object of study that dictates the means of
Research perspective and method

how to approach it methodologically (Stake, 1994). The focus on social and institutional aspects of eIDs in a public sector context, in turn, motivates the choice of using case studies as the preferred methodological choice for this dissertation. The purpose of a case study is also to convince the research community of the applicability or inapplicability of a particular theory or proposition with the purpose of contributing to knowledge in a specific field (Myers, 2009). In accordance with the previously described research perspective based on interpretive epistemology, the interpretive field study is a suggested type of empirical method that is a combination of a qualitative and interpretive approach together with methods of case studies well suited for the investigation of information systems (Markus & Lee, 1999). Thus, the selected method of interpretive case studies in this work in well in line with approaches in ISR perceived as being relevant and appropriate for this area of study.

2.3.2 Generalizability

As related to the applied research methodology (Walsham, 1993), the term generalizability refers to “[T]he validity of theory in a setting different from the one where it was empirically tested and confirmed.” (Lee & Baskerville, 2003, p. 221). Thus, generalizability is described as a central challenge for research as well as a prerequisite for research to be perceived as useful (Lee & Baskerville, 2003). With generalizability referring to the ability to gain the same results by applying insights to a repeated number of identical situations, interpretive researchers often refrain from making such generalizations since the conclusions do not have the same high level of plausibility as positivistic approaches, (Hirschheim & Klein, 2003). However, in my opinion, this view implies a clear underlying notion of positivism regarding the potential transferability of results which in turn seems to be related to how generalizability is usually interpreted in interpretive research. Hence, in this work, I will not refrain from generalizations but instead, argue that this concept needs to be interpreted and adapted to the context of interpretive research.

The perspective on generalizations applied in this dissertation is therefore similar to statements such as “Generalization from the setting (usually only one or a handful of field sites) to a population is not sought; rather, the intent is to understand the deeper structure of a phenomenon, which it is believed can then be used to inform other settings.” (Orlikowski & Baroudi, 1991, p. 5). Further, as Walsham (1993) points out, it is also important to understand that generalization, in fact, is more closely related to the research methodology applied rather than the underlying research perspective. Thereby, I argue that to describe ISR and interpretive research as related to this problem, in general, this statement in itself becomes an incorrect generalization. Thus, it should be made clear that generalizability in a statistical sense does not apply here but instead is related to the logical reasoning behind the results and the conclusions drawn from them (Walsham, 1993) and the positive transfer of knowledge between organizational contexts (Walsham, 1995b). As described by the third research question (RQ-3), this dissertation aims at contributing to such a positive transfer of knowledge in order to provide insights for research as well as facilitate more successful public sector eID introductions.
(see Section 1.2). Generalizability is also related to the broader relevance of research (Lee & Baskerville, 2003), and Cresswell (2001) describes an important distinction between ‘relevance to’ and ‘of value to’. Relevancy per se does not include any positive implications of research to a third party since research can be conducted with the sole purpose of developing and advancing knowledge that will make practical contributions become secondary (Cresswell, 2001). Therefore, I argue that it is important to address the relevancy of research being performed with a clear distinction between internal relevancy, aimed at the research field and academia, as well as external relevancy aimed at potential external stakeholders.

The research questions and intended contribution (see Section 1.2 and 1.3) as well as implications for research and practice presented in the conclusions of this dissertation (see Section 10.2) clearly describe how this work will contribute and ‘be of value to’, ISR and other relevant research fields (internal relevancy) as well as different areas of practice (external relevancy). The relevancy with an emphasis on ‘being of interest of’ is put forth when describing the intended audiences of this dissertation (see Section 1.6). Moreover, in this kind of research investigating the social structures and contexts as related to ICT, I argue that the issue of generalization maybe should not be in the hands of the researcher at all. The researcher can only communicate insights and contributions in an appropriate way. Hence the key to a positive transfer of insights and knowledge lay in the hands of actors in relevant research and practice settings potentially making use of them. Therefore, I argue that generalizability from a researcher’s perspective can at best be a qualified estimate of transferability and maybe this is why it is perceived as challenging and problematic.

2.3.3 Triangulation

In research, triangulation\textsuperscript{10} refers to the “[C]ombination of methodologies in the study of the same phenomena.” (Denzin, 1978, p. 291) applied with the aim of strengthening the study (Patton, 2002). Studies only applying one method become vulnerable to potential limitations and problems associated with that particular methodology (Patton, 2002). Hence, triangulation introduces the concept of adding multiplicity or plurality of methods to research as a heuristic tool (Janesick, 1994) for example by the use of multiple methods of data collection or the combination of quantitative and qualitative methods (Myers, 2009). Different types of triangulation are defined as related to data, investigator, theory and methodology (Denzin, 1978). Investigator triangulation applies when several observers or researchers are used in a single study, and the purpose of methodological triangulation is to achieve a multitude of perspectives. Each of these perspectives will then reveal different aspects of the ‘empirical reality’ and in turn result in more valid research propositions (Denzin, 1978). By applying multiple perspectives, the aim is to provide a complete picture of the studied phenomenon (Myers, 2009) but this can

\textsuperscript{10} A term from land surveying where two landmarks and your own position can be used to locate yourself (Patton, 2002)
also be a challenging task especially if these perspectives are based on different research paradigms or assumptions described above. In this dissertation, three types of triangulation are applied according to Denzin’s classification. First, data triangulation is achieved by the variety of data sources used (Janesick, 1994) ranging from primary data collected via interpretive interviews via document studies, fieldwork and observations described in the following section. Hence, this approach allows for the addition of official perspectives in governing documents to the translations of the public sector eIDs thus providing a more complete and realistic picture of public sector eID introductions with all of their inherent challenges and potential contradicting perspectives. Thus, any potential inconsistencies provided by these different perspectives are considered as opportunities for deeper insights (Patton, 2002) about public sector eIDs while not by any means weakening the study’s credibility (Patton, 2002).

As a variation of data triangulation, the specific type of triangulation of subjects (Rubin & Rubin, 2011), a variance in in respondents’ perspectives, is also applied in later described interpretive interviews. Second, investigator triangulation, described in detail later as clearly related to the two cases, is used to a great extent in both case studies and obtained by the use of multiple interviewers (Bechhofer et al., 1984). Third, in this dissertation data is approached with several research questions representing several perspectives as described in the introduction. Hence, since several theoretical perspectives are placed side by side for the assessment of new insights of public sector eIDs this approach can be considered as theory triangulation (Denzin, 1978). Thus, a potential convergence between the sociological and institutionalist perspectives are put forth rather than emphasizing any contradictions. However, I argue that this type of triangulation can be a significant challenge for example when it comes to collecting empirical data on to which different theoretical perspectives can be applied. Since data is collected with the aim of investigating social and organizational implications of the eID, this is fact converges with the social as well as the institutional perspective applied during analysis.

Since the same type of qualitative data analysis is applied to all collected data, methodological triangulation with the aim of strengthening and validating findings is not applied. Janesick (1994) also introduces the concept of interdisciplinary triangulation emphasizing the need of challenging dominant scientific approaches in different research fields for a broadening of the understanding of studied phenomena (see the need for a broader focus on public sector eIDs in Section 1.1.4). Hence, this dissertation can also be seen as applying this type of triangulation when broadening existing technical perspectives of the eID with sociology and institutionalism. However, this is not a conscious approach for increasing its validity as put forth by Flick (2004) but rather the consequence of applying an approach where the development of an understanding of the phenomenon (the eID), addressing the research questions and fulfilling its aim and contribution are put in the foreground. Not confining this study to any pre-established or
dominating approaches or perspectives a priori, but rather letting the focused phenomena dictate the path to be followed. In addition, the interdisciplinary character of this dissertation is also clearly related to its position in the ISR field as a transdisciplinary or interdisciplinary field of research (see Section 3.1). The researcher must also separate empirical findings from the interpretations given them, in addition, resulting in a triangulation of perspectives (Denzin, 1978). Hence, in this dissertation, the interpretations as given by the respondents’ are correctly reported and clearly distinguishable from the interpretations made by me as a researcher. In addition, the calls for increased diversity and pluralism in the ISR field (e.g. Mingers, 2001) can also be seen as calls for an increase in theoretical as well as methodological triangulation to challenge this particular research field’s history of positivistic approaches as described above.

2.3.4 Literature survey

As described, identifying and relating to existing research are important aspects in the process of developing knowledge and the study of published research is one of the most important ways (Boell & Cecez-Kecmanovic, 2014). One potential way to advance the collective understanding in research (Boote & Beile, 2005) is by performing a literature review as a structured process performed with aim of summarize, critically examine, explain results and clarify alternative views of prior research (Rowe, 2014). However, these highly structured or systematic reviews are also contested as being unsuitable for research in social sciences since they require research questions being formulated a priori (Boell & Cecez-Kecmanovic, 2010). As previously described, the process of writing this dissertation is done according to the hermeneutic principle where knowledge and understanding develops during a constant change of focus between the separate parts and the whole. Hence, the dissertation’s basic tenets such as the problem area addressed, research questions, aims and contributions et cetera are continuously formulated and revised during this process as the understanding of the field develops; a progression described as common in social sciences (Boell & Cecez-Kecmanovic, 2010).

This dissertation therefore does not include any systematic literature review, instead the process of identifying prior research is related to its epistemological stance previously described as interpretive and hermeneutic. The process of identifying and assessing of existing literature is therefore referred to as a literature survey with interpretations and emerging knowledge acting as central guides. Nevertheless, some basic guidelines prescribed for formal literature reviews are applied. In addition, due to this dissertation’s interdisciplinary character, the literature survey is not limited to the boundaries of the ISR domain as recommended by Webster and Watson (2002). The structure of the literature survey is clearly what could be defined as concept centric (Webster & Watson, 2002) since central concepts are identified, e.g. ‘electronic identification’, ‘organizational context’ and ‘institutional pressure’, and used to categorise the evolving set of literature considered. In addition, a reference manager software11 is used throughout the

---

11 EndNote by Thomson Reuters.
Research perspective and method

entire process to organize the growing literature base which also facilitates the formulation, revision and management of identified concepts in literature. A specific prerequisite for this literature survey is that it should be clearly categorized as identifying literature serving two specific purposes for the dissertation: literature to be used for framing the research perspective and literature to provide the analytical perspective. The literature forming the analytical perspective is identified during the qualitative data analysis, referred to as theoretical matching (Goldkuhl & Cronholm, 2010). As described in a later section, the survey then becomes part of the abductive and iterative analysis guiding and being guided by emerging concepts and categories.

The theory emerging from qualitative analysis continuously informs the literature survey which I argue in turn provides a high level of relevance and applicability. Thereby, the aim of this literature survey is not to map and structure existing research but rather use it as a source and influence during the development of knowledge about existing research in relevant research fields. This chosen strategy also has clear similarities with the hermeneutic approach to literature reviews describing this process as a hermeneutic development of understanding continuously informed by a developing pre-understanding (Boell & Cecez-Kecmanovic, 2014). Hence, this hermeneutic literature survey is performed as part of the dissertation process until no new information is located and saturation occurs (Combs et al., 2010). Reaching saturation also includes reaching sufficient levels in important categories such as coverage, synthesis, methodology and significance as suggested by Boote and Beile (2005). In addition, my own authored and co-authored publications described in a later section are also considered as existing literature during this literature survey.

2.4 Selecting cases

As mentioned above, this dissertation features two interpretive case studies focusing on public sector eID introductions. The first case, located on a national or inter-organizational level, is referred to as the eGov case due to its aim of introducing an eID serving as a common eID for the entire public sector. The second case, located on an intra-organizational level, is referred to as the eHealth case motivated by the aim of providing eID services for professional use within public health care or eHealth sector. The eIDs being introduced in these two cases are henceforth referred to as the eGov eID and the eHealth eID. An overview of the timeline of these cases is illustrated in Figure 2 (below) with the two different phases of the eGov case, introduction and acceptance, to be described in the next section.
2.4.1 The eGov case

As illustrated in the timeline above, the eGov case is separated into two distinct phases called the introduction phase and acceptance phase. This is done to emphasize that the process itself, as coordinated by the Board, clearly changed in character in late 2013. Between 2011 and 2013 the Board is fully focused on implementing and introducing the regulatory and technical frameworks that will form the basis of the eGov eID solution. Since the eGov eID is simultaneously developed and introduced, there is little room for affected actors to translate it and assess any consequences of it. Hence, the eID is still very much a ‘moving target’ during this period; the case primarily focuses on collecting data via official forums such as hearings, annual conferences and written material and documents. This phase is therefore characterized as the introduction phase. In late 2013, the process of introducing the eGov eID clearly shifts in character when affected actors begin to assess and translate the consequences for instance by actively investigating if they should accept it or not. Thus, during this acceptance phase, the authority coordinating and introducing the eID (the Board) is interviewed and responds positively to the aim of studying this introduction since it has never been done before on a national level.

Discussions about relevant authorities acting as public sector service providers in the case results in three identified organizations. These organizations are thereafter contacted, responds positively and interviews are conducted. Hence, these three authorities, in turn, become embedded cases (Yin, 2014) providing very valuable data in the form of different authorities’ perspectives of the eID to this case study as a whole. Moreover, one authority turns out to be very competent and knowledgeable in the eID field which in turn results in a further in depth study of this particular organization’s perspective of the eID introduction. The extended study of this organization also results in this actor taking place as the service provider in the translation analysis (see Chapter 7). The three selected agencies turn out to provide a significant variance regarding attitudes towards the eGov eID. Regarding the important role of the private sector actors as identity providers of national eIDs, selecting and approaching these organizations turned out to be more problematic. On initial contact, they all turn down the requests for interviews which in turn most likely is due to their very low profile in the eGov eID area at that
time, i.e. during the introduction phase described above. However, during the acceptance phase, I am able to interview relevant representatives of all three leading commercial banks acting as identity providers and hence identified as crucial actors to the introduction of the eGov eID (see Chapter 5). This development is most likely related to the much more open dialogue and climate in the eGov eID area as well as an increasing frustration among identity providers regarding how the introduction progresses over time. To be able to get a correct and more nuanced view of the field, the responsible person at ministry level, as well as a representative of the Swedish Association of Local Authorities and Regions (Sveriges Kommuner och Landsting, SKL), are also selected as respondents.

Table 4. eGov case interviews

<table>
<thead>
<tr>
<th>Date</th>
<th>Organization</th>
<th>Respondent</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>15/10/2013</td>
<td>Agency#1</td>
<td>CIO</td>
<td>FtF</td>
</tr>
<tr>
<td>19/11/2013</td>
<td>Agency#1</td>
<td>Infrastructure Manager</td>
<td>FtF</td>
</tr>
<tr>
<td>19/11/2013</td>
<td>Agency#1</td>
<td>Security Specialist</td>
<td>FtF</td>
</tr>
<tr>
<td>26/11/2013</td>
<td>The Board</td>
<td>Head of Secretariat</td>
<td>FtF</td>
</tr>
<tr>
<td>14/02/2014</td>
<td>Agency#1</td>
<td>IT Security Manager</td>
<td>Phone</td>
</tr>
<tr>
<td>03/03/2014</td>
<td>Agency#1</td>
<td>Area Manager</td>
<td>FtF</td>
</tr>
<tr>
<td>05/06/2014</td>
<td>Agency#1</td>
<td>Head of Digital Channels</td>
<td>FtF</td>
</tr>
<tr>
<td>12/06/2014</td>
<td>Agency#1</td>
<td>Information Security Manager</td>
<td>Phone</td>
</tr>
<tr>
<td>17/03/2015</td>
<td>Agency#2</td>
<td>Business Developer</td>
<td>FtF</td>
</tr>
<tr>
<td>17/03/2015</td>
<td>Agency#2</td>
<td>IT Architect</td>
<td>FtF</td>
</tr>
<tr>
<td>17/03/2015</td>
<td>Bank#1</td>
<td>Product and Process Manager</td>
<td>FtF</td>
</tr>
<tr>
<td>19/03/2015</td>
<td>Agency#3</td>
<td>Information Security Strategist</td>
<td>FtF</td>
</tr>
<tr>
<td>19/03/2015</td>
<td>Agency#3</td>
<td>Security Specialist</td>
<td>FtF</td>
</tr>
<tr>
<td>19/03/2015</td>
<td>Bank#2</td>
<td>Product and Process Manager</td>
<td>FtF</td>
</tr>
<tr>
<td>10/04/2015</td>
<td>Ministry</td>
<td>Head of Section</td>
<td>Phone</td>
</tr>
<tr>
<td>20/04/2015</td>
<td>SKL</td>
<td>Infrastructure &amp; Security Specialist</td>
<td>Phone</td>
</tr>
<tr>
<td>17/06/2015</td>
<td>Bank#3</td>
<td>Product Manager</td>
<td>FtF</td>
</tr>
<tr>
<td>26/06/2015</td>
<td>The Board</td>
<td>Head of Secretariat</td>
<td>FtF</td>
</tr>
</tbody>
</table>

Summary of interviews: 20

12 Due to the author’s hospitalization, this scheduled interview is conducted via email where the respondent answers and comments the questions in the interview guide; these answers are also actively followed up.
A summary of all official respondents in the eGov case is presented in Table 4 where a total of 20 interviews are conducted (13 face-to-face [FtF] on location, 6 via telephone [Phone] and 1 via email) during the data collection process that is initiated in October 2013 and ends in June 2015. In addition, to facilitate my own development of knowledge of the eID field, several contacts are made with eID specialists outside the eGov eID context, not being in a position as directly affected by the solution. Hence, as non-dependent sources of information or key informants (Myers, 2009), these persons acts as a valuable source of input to facilitate my own knowledge development of the field of study. A selection of informants is also used to validate selected parts of this dissertation (expert validation). On ethical grounds, I have chosen not to disclose the identity of these key informants hence these sources of information are not considered as official interviews but is rather performed in the form of informal conversations.

2.4.2 The eHealth case

Regarding the selection of the organization in the eHealth case, contact is made with a county council that my department has collaborated with on several occasions. Hence, this positive relation provides good access, and it also turns out that this organization is just starting to introduce the eHealth eID across the organization. The main reason for selecting a health care organization is related to the fact that these organizations are at the time of the study just starting out to introduce eIDs for professional use. Thus, in this study, the eHealth case mainly brings an example of a public sector organization introducing eIDs with this kind of intra-organizational perspective. Thus, the complex forms of health care management, structure and control, strong professions and hierarchies and other specific characteristics related to health care will not be emphasized in this work. Although this black boxing can be seen as a clear shortcoming, I instead choose to see it as an opportunity and an example of the possibility of crossing such clear organizational boundaries in search for new insights into public sector eID introductions (see also Section 1.5.2).

The initial contact and interviews are made with representatives coordinating the eID introduction at the central IT unit. Very similar to the eGov case, these representatives stay positive to this study being performed since it is the first time this organization introduces an eID solution. Moreover, they report several unanticipated challenges related to actors’ perceptions and translations of the eID (see Chapter 6). Since the aim of this case is to investigate how an eID introduction is translated by affected actors in operational health care, discussions results in the identification of two local health centres and a hospital clinic as suitable locations to study. Moreover, this selection of embedded units (Yin, 2014) provides a positive variance regarding the type of medical care provided. Local health centres providing primary health care to the community is contrasted by the hospital clinic providing highly specialized health care. This will potentially bring forth important differences in the translations of the eID between these two organizational contexts. Next, contact is made with health centre managers at these three locations and interview are performed on a unit by unit basis. To be able to achieve a
positive representation and variance in respondents at each health centre, several additional respondents are selected based on predefined professional roles. Besides the manager, the local IT coordinator provides the local IT skilled perspective while the medical secretary provides an administrative perspective of the eID. In addition, one assistant nurse, as well as one registered nurse or physician, are selected per site providing the perspective of the eID from a medical perspective.

Table 5. eHealth case interviews

<table>
<thead>
<tr>
<th>Date</th>
<th>Organization</th>
<th>Respondent</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>17/09/2012</td>
<td>Central IT</td>
<td>Infrastructure specialist</td>
<td>FtF</td>
</tr>
<tr>
<td>01/10/2012</td>
<td>Central IT</td>
<td>Security specialist</td>
<td>FtF</td>
</tr>
<tr>
<td>08/10/2012</td>
<td>Central IT</td>
<td>Business specialist</td>
<td>FtF</td>
</tr>
<tr>
<td>09/10/2012</td>
<td>Central IT</td>
<td>Technical specialist</td>
<td>FtF</td>
</tr>
<tr>
<td>19/11/2012</td>
<td>Health Centre#2</td>
<td>Manager</td>
<td>FtF</td>
</tr>
<tr>
<td>05/12/2012</td>
<td>Health Centre#1</td>
<td>Manager</td>
<td>FtF</td>
</tr>
<tr>
<td>17/12/2012</td>
<td>Health Centre#1</td>
<td>Physician</td>
<td>FtF</td>
</tr>
<tr>
<td>17/12/2012</td>
<td>Health Centre#1</td>
<td>Assistant nurse</td>
<td>FtF</td>
</tr>
<tr>
<td>17/12/2012</td>
<td>Health Centre#1</td>
<td>Medical secretary</td>
<td>FtF</td>
</tr>
<tr>
<td>14/02/2013</td>
<td>Health Centre#2</td>
<td>ITR</td>
<td>FtF</td>
</tr>
<tr>
<td>14/02/2013</td>
<td>Health Centre#2</td>
<td>Medical secretary</td>
<td>FtF</td>
</tr>
<tr>
<td>13/03/2013</td>
<td>Health Centre#1</td>
<td>ITR</td>
<td>FtF</td>
</tr>
<tr>
<td>07/05/2013</td>
<td>Hospital clinic</td>
<td>Manager</td>
<td>FtF</td>
</tr>
<tr>
<td>07/05/2013</td>
<td>Hospital clinic</td>
<td>ITR</td>
<td>FtF</td>
</tr>
<tr>
<td>07/05/2013</td>
<td>Hospital clinic</td>
<td>Registered nurse</td>
<td>FtF</td>
</tr>
<tr>
<td>07/05/2013</td>
<td>Hospital clinic</td>
<td>Assistant nurse</td>
<td>FtF</td>
</tr>
<tr>
<td>07/05/2013</td>
<td>Hospital clinic</td>
<td>Medical secretary</td>
<td>FtF</td>
</tr>
<tr>
<td>05/06/2013</td>
<td>Health Centre#2</td>
<td>Assistant nurse</td>
<td>FtF</td>
</tr>
<tr>
<td>07/06/2013</td>
<td>Health Centre#2</td>
<td>Registered nurse</td>
<td>FtF</td>
</tr>
</tbody>
</table>

Summary of interviews: 19

A summary of all respondents in the eHealth case is presented in Table 5 where a total of 19 interviews are conducted face-to-face on location during the data collection process that is initiated in September 2012 and ended in June 2013. To validate results in the eHealth case, two meetings are held with staff at the Central IT function with the opportunity to receive feedback on tentative results.
2.4.3 Reflection on the selection process

The selection of organizations and respondents presented above could be described as a type of referral sampling (Biernacki & Waldorf, 1981) where an initial contact or gatekeeper (Miller & Bell, 2002) referred to additional respondents on intra or inter-organizational levels. Thus, this sampling method is also a case of convenience sampling hence can be considered as less rigorous than other techniques since only focused on accessible subjects (Marshall, 1996). Therefore this method can be a factor potentially limiting the findings brought forth by the study. However, being a widely applied approach in qualitative research (Miller & Bell, 2002), I argue that this way of identifying subjects neither negatively affected the study nor limited the results since I never faced the problem of selecting between accessible or relevant and knowledgeable respondents. The selection of organizations and respondents are made in dialogue with the initial gatekeeper, and the aim of the study is kept intact. For instance, in the eGov as well as the eHealth case, at times particular subjects are less accessible, but since the data collection took place over considerable time, all such problems are solved.

Therefore, I would object to any accusations of inherent biases related to the applied sampling techniques since it, not by any means made me deviate from the proposed aim and path of the study. The variance in perspectives of respondents corresponded with the width and depth I am aiming for hence this enabled collection of data based on actors’ perspectives as converging as well as diverging from the proposed eGov eID solution. Triangulation of subjects (Rubin & Rubin, 2011) described above is in the eGov case achieved by selecting respondents based on their actual involvement in eGov eID introduction hence their organizational belonging and actual assignments related to the eID provides a positive variance (Myers, 2009) across selected organizations. In the eHealth case, this triangulation is achieved by the variation in health centres and selected specific organizational roles. Therefore, I also argue that the focuses of these cases as being inter-organizational (eGov case) and intra-organizational (eHealth case) and also situated in two different empirical domains provide the variations and similarities needed in order to address research questions.

2.5 Data collection

2.5.1 Interpretive interviews

In accordance with the interpretive approach described above, in this study data requires being collected while accessing the real world of the studied phenomenon. This will enable the investigation of the public sector eID in its very own context with the opportunities to capture explicit aspects as well as implicit nuances. Although selected techniques for data collection should rest upon prior research choices such as method, topic and availability of data as well as prior experiences in collecting data (Myers, 2009) I strongly agree with suggestions putting forth the phenomenon to be studied as well as the anticipated result as important influences (Stake, 1994). Thus, interpretive
interviews are selected as the primary data collection technique since they allow the researcher to access respondents’ interpretations on different levels such as actions and events as well as aspirations and views (Walsham, 1995b). Rubin and Rubin (2011) state that: “Qualitative interviews let us see that which is not ordinarily on view and examine that which is often looked at but seldom seen.” (Rubin & Rubin, 2011, p. xv). Thus referring to the investigation of the deeper social and organizational context of studied phenomena. During the interview, knowledge is co-constructed by the interaction between the interviewer and the interviewee (Kvale & Brinkmann, 2009). Therefore, data become socially constructed (Berger & Luckmann, 1967) through the interaction between the researcher and the respondent (Klein & Myers, 1999). This presents the opportunity to access the respondents’ assigned meanings as emphasized by interpretive approaches (Orlikowski & Baroudi, 1991).

Using interpretive interviews as the primary data collection technique corresponds very well with the ontological and epistemological stance described above as well as the described aim and purpose of this dissertation. In general, interviews are considered one of the most important methods of data gathering in qualitative research and allow the researcher to gather rich data from people in various roles and situations (Myers, 2009). Moreover, I argue that rich data and the resulting rich findings as interpreted by the researcher, in turn, become a prerequisite for the delivery of rich insights and deeper understandings. Nevertheless, these rich findings may also be dismissed as storytelling but are in fact very important for qualitative research to be able to deliver its depth, thoroughness and credibility in results (Rubin & Rubin, 2011). This is also a prerequisite for the development of an understanding of complex phenomena such as related to ICT (Walsham, 1995b) as exemplified by the eID in a social and organizational context.

There are several different types of interviews that can be applied. Structured interviews bound to a specific setup of pre-formulated questions provide consistency across multiple interviews while unstructured interviews with few if any pre-formulated questions allow the respondent to talk freely about topics considered to be important from the respondent’s perspective (Myers, 2009). Further, semi-structured interviews provide consistency by the use of a set of pre-formulated questions while leaving the flexibility for new questions to arise during the interview (Myers, 2009). In this dissertation, semi-structured interviews are conducted. This is motivated by the need for guidance and continuity needed in collected data for performing the analysis. Two interview guides are developed, one for the eGov case and one for the eHealth case (see Appendix 1). These remain the same during both case studies and allow for structure and guidance during the interviews. Further, the semi-structured approach also allows for additional follow up questions depending on the situational context of each interview. Hence, this type of interview allows for the needed flexibility during the interview and opportunity to get acquainted and hopefully adapt to the cultural context of this situation. As described, since the process of the interview is one of social co-construction, I argue that
it is important for the respondent to be able to actively influence the interview based on this individual’s pre-understanding. In addition, if a similar interview guide is used throughout the case, I argue the researcher can also significantly improve his or hers pre-understanding of the organizational context which in turn also will have a positive effect on interviews. However, this data collection technique also brings significant challenges. Since interpretive interviews put great trust in the researcher being able to access and interpret the interpretations (Giddens, 1984) to be able to transform the rich descriptions, via densifying abstractions and conceptualizations, into positive contributions. These challenges are related to the acts of preparing, conducting and transcribing the interviews and also affected by and related to later research stages such as analysis, conceptualization, and synthesis as well as written record. Therefore, I argue that striving for as high quality as possible during data collection is a prerequisite to being able to provide high quality results in terms of trustworthiness and authenticity (Denzin & Lincoln, 1994a).

2.5.2 Multiple interviewers

Further, in both cases, a significant number of interviews are performed with more than one interviewers hence resulting in the investigator triangulation described above. This allowed for the capture of several perspectives on the dialogue taking place as well as a clear division of tasks between the interviewers. In the eGov case, 13 out of 20 and in the eHealth case, 4 out of 19 face-to-face interviews are conducted by two interviewers. In the eHealth case, two interviews are also conducted by a research colleague, without my participation, due to urgent family matters. During these interviews, one interviewer can be assigned the role of being ‘active’ and hence leads the interview, and the other is the ‘passive’ interviewer assessing the overall interview situation, asks supplementary questions and prepares for when roles are changed (Bechhofer et al., 1984). In the cases covered by this dissertation, the strategy of multiple interviewers is applied differently. In the eHealth case, one interviewer usually takes on the active role during the entire interview while the passive interviewer cover additional aspects and asks follow up questions. In the eGov case, however, these kinds of interviews are mostly performed with two interviewers working in different research contexts hence the synergy of performing interviews with a dual purpose of these two interviewers are applied. During these occasions, the interview is clearly divided in time between the two interviewers. Based on my experiences, this interviewing technique works very well with the main advantage of being less labour intensive. Hence, I argue that performing an interview as a single interviewer can be very exhausting since you have to focus and record all aspects of the interview by yourself. This also being in line with Bechhofer et al. (1984) also putting forth positive sides such as the interview becoming more of a conversation, a reduced risk of being stuck on a topic and the possibility to cross-check data between interviewers afterwards. Thus, I argue that the benefit of using multiple interviewers are only positive.

13 Arrival of new family member in February 2013.
2.5.3 Document studies

In addition to interviews, documents are used as an important data source hence can be seen as adding the concept of data triangulation as described above. Since these documents are treated as data collected via written records, the analysis is performed in the same way as with other data collected such as interview data. The documents used also serve different purposes. First, documents are used to gather background information about the public sector eIDs in the eGov and eHealth contexts since in both cases, the eID being introduced is governed by public policy documents. Accordingly, such documents provide important information about the aim and purpose of the eIDs. Moreover, these documents also provide the translation of the eIDs from the government perspective. Second, public documents on national as well as EU level are also used to inform and validate the process of conducting interpretive interviews by giving the opportunity to compare or triangulate respondents’ interpretations of the focused eID introductions against the public sector policy documents governing them. For instance, since the eHealth eID introduction is focused on increasing the level of patient security, the respondents’ translations of this concept can be assessed as a means of investigating the understanding and dissemination of this central concept and aim of the eHealth eID. Further, the report governing the eGov eID as well as the mandate and activities of the Board are actively used as a reference point for comparing how the eGov eID turns out in practice.

Third, public documents regarding the eHealth and eGov eID are also used for developing an understanding of the past, current and future opportunities and challenges of public sector eIDs in both cases. In the eHealth case examples of such documents are laws and regulations, investigations, directives as well as prior and current national eHealth strategies. In the eGov case, an extensive amount of official documents is studied ranging from historical documents on the emergence of the current eID solution from different authorities, investigations, referrals, assessments, agency reports, laws and regulations, framework agreements, guidance as well as regulations and directives on EU level. Since the eGov eID is actively being developed and introduced in parallel during this study, all documents produced by the introducing authority (the Board) are successively integrated into document studies. When needed, specific public documents are also requested from authorities and responsible ministries, for example, signed agreements and responses to referrals. Table 6 provides an overview of particularly important public documents for each case. All documents used in this study are approached from a critical perspective, and their authenticity, as well as reliability, are assessed prior to considering use (Myers, 2009). Similar to empirical data collected via interviews, document studies involves the researcher actively interpreting these documents (Denzin & Lincoln, 1994b) since these, in essence, are words of individuals thus become interpretations presented in written form. Accordingly, I have to interpret and try to make sense out of these documents to be able to integrate them into the different versions of working...
interpretive documents (Denzin & Lincoln, 1994b) until finally presented in written form in this dissertation.

Table 6. Public documents of interest – an overview

<table>
<thead>
<tr>
<th>Case</th>
<th>Published by</th>
<th>Description</th>
<th>Year</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Ministry of Finance (Dir. 2010:69)</td>
<td>Authority for the cooperation of electronic identification and signing.</td>
<td>2010</td>
</tr>
<tr>
<td></td>
<td>Ministry of Finance (SOU 2010:104)</td>
<td>The eID Board and Swedish electronic identification.</td>
<td>2010</td>
</tr>
<tr>
<td></td>
<td>Swedish Civil Contingencies Agency (MSB, 2014a)</td>
<td>Analysis of the information security of the Swedish eID.</td>
<td>2014</td>
</tr>
<tr>
<td></td>
<td>European Union (EU 910/2014)</td>
<td>eIDAS regulation&lt;sup&gt;14&lt;/sup&gt;</td>
<td>2014</td>
</tr>
<tr>
<td></td>
<td>Center for eHealth Cooperation (CeHis, 2010)</td>
<td>National eHealth – the strategy for available and secure information in health and social care.</td>
<td>2010</td>
</tr>
</tbody>
</table>

2.5.4 Additional data sources

In addition to interviews and documents, several additional data sources are used to provide data for this work mainly in the eGov case by applying methods such as observations, participant observations and the use of key informants described later. There are several advantages of direct observations such as enabling the researcher to better understand the studied context by being discovery oriented and open to nuances in the studied context (Patton, 2002). During the observation, the passive observer observes some kind of social event or meeting with little or none interaction while the participating observer participates in activities as relevant to the situation (Myers, 2009; Spradley, 1980). In this study, observations are used to gain a deeper understanding of the eGov eID context by attending and observing official events such as open hearings and annual eID conferences as described in a later section. In addition, data collection also includes participating in several meetings and seminars as well as presenting tentative results in different contexts in both cases.

For example, presenting tentative results for members of the Board or representatives from the eHealth organization provides very valuable feedback on current work as well as positive reactions to my suggested need of broadening the perspective of public sector eIDs to be able to cope with current challenges. These events and actions are also part of my strategy to strengthen the practical relevance of the research being performed as described in a later section. Further, the participating observer is faced with the opportunity of becoming explicitly aware of nuances commonly being unnoticed or overlooked by the normal participant which in turn also can be a challenge (Spradley, 1980). Thus, attending the first meetings as a participating observer, I feel I am facing a daunting task; to observe and record everything going on during that event as well as participating and taking notes of the reactions all by myself. However, with practice comes experience that makes me more comfortable in this dual role. Hence I am able to move back and forth between selective attention and inattention (Spradley, 1980); a challenge also described as the researcher having to continuously move back and forth between different roles of the self (Denzin, 1978).

An additional challenge of using observations in contrast to interviews is not able to use audio recording on these events. Hence, I rely on taking notes during the meetings, and additional notes and reflections are added directly after when trying to capture the inherent nuances of the empirical context. Concerns about ethics are raised against observations when the subjects are unaware of the role of the researcher (Denzin, 1978). Therefore, in line with the ethical considerations applied in this dissertation described below, I argue that this way of collecting data is ethically justifiable since the aim of the observations and participating observations are to inform the study to be able to develop a deeper understanding of the studied context. Hence, no participating members on these events are disclosed or used as official respondents with the exception of some official
statements and presentations held at the annual eID conferences (see Chapter 5). In addition, when appropriate I also make clear my purpose of attending these events. As described, key informants also provide very useful information to be able to better understand the eID context from different perspectives. These informants are selected due to their positions of being specialists with an extended knowledge (Myers, 2009) of the eID field. The opportunity of to use these informants as providing expert knowledge from organizational and security perspectives are therefore the result of me being active in the eID field for a considerable time, building relations that result in a positive dialogue and mutual trust. These informants are to inform, guide and validate the study they are not used as official respondents in this dissertation. This is a reflective choice based on ethical grounds in order to maintain the established confidence and trust in these relationships. Further, in addition to traditional documents described above, online media such as web sites, blogs\textsuperscript{15} and social media channels\textsuperscript{16}, are actively used throughout the work as an additional source of information.

2.6 Analysis and synthesis

2.6.1 Analytic strategy

Related to this dissertation’s underlying assumptions described as constructionist and interpretive, empirical data need to be further analysed and condensed to be able to provide insights and provide proposals on abstract levels. Thus, qualitative analysis consists of data condensation, data display and conclusion drawing as well as verification (Miles et al., 2013). Data condensation refers to the process of transforming the raw data appearing in the transcript into a stronger form reflecting the analytic choices and emphasis on what to extract and focus on made by the researcher for example during coding and categorization. The purpose of data display is to compress information to allow for further conclusion drawing which in turn refers to the development of conclusions drawn from data along the path of analysis. These conclusions continuously need to be verified against other data or other sources (Miles et al., 2013). Data analysis is also about considering and reflecting about the specificity versus generality in empirical findings to be able to relate to existing research and theory. Data analysis includes several different complex stages and is often referred to as rather elusive or even as a trick of the trade of the researcher (Becker, 1998). Therefore, I search for guidance in this process and identify Grounded Theory (GT) (e.g. Corbin & Strauss, 2008; Glaser & Strauss, 1967) as an approach that provides a structured and systematized way to analyse and abstract empirical data into categories and theoretical constructs (Goldkuhl & Cronholm, 2010). GT offers a significantly different approach than traditional logical deductive methodologies where hypotheses are derived from existing theories which in turn structures the

\textsuperscript{15} A truncation of weblog i.e. an online information site where articles or posts are published in chronological order.

\textsuperscript{16} Twitter
whole research process of data collection and analysis towards verification or refutation (Charmaz, 1990). The development of GT can be traced back to efforts in sociology trying to bridge the gap between pure theorists’ and empiricists’ approaches as a consequence of very abstract conceptual grand theories in the field (Goulding, 1998). These theories are therefore deemed not developed enough to be tested or too abstract (Wells, 1995). However, the inductive approach in GT is contested and results in further developments of this methodology such as Multi-Grounded Theory (MGT) (Goldkuhl & Cronholm, 2010). On a general level, MGT addresses the risks of not considering and building on existing theory by adding theoretical as well as internal grounding to the process (Goldkuhl & Cronholm, 2010). Thus, GT in its original form provides the clear strategy and guidance I am looking for, but this inductive approach diverges from the aim of this work as being theoretically informed during stages of analysis and possibly further develop prior research. Therefore, MGT as grounded in empirical data as well as existing theory and applying a process of internal grounding is considered a better fit for the analytical strategy of this dissertation. This approach allows the researcher to keep an open mind during analysis which in turn corresponds well to the interpretive approach described above. Furthermore, in MGT empirical data as well as external theories influence the research interest during the development of theory as illustrated by the three processes of empirical, theoretical and internal grounding (Goldkuhl & Cronholm, 2010) in Figure 3.

![Figure 3. Three grounding processes of MGT (adapted from Goldkuhl & Cronholm, 2010)](image-url)
In Figure 3, theoretical grounding refers to the process of considering pre-existing theories during the development of theory while internal grounding is a systematic investigation of the evolving theory to provide consistency. Empirical grounding refers to the inductive approach of analysing empirical data as prescribed in GT (Goldkuhl & Cronholm, 2010). MGT consists of a number of stages divided into theory generation, explicit grounding and research interest reflection and revision (Goldkuhl & Cronholm, 2010). However, with large amounts of raw data and rather limited resources, my aim is not to apply the MGT approach in full during this work. Thereby, I am looking for guidance regarding the processes of coding, developing concepts and categories as well as how and when to relate to existing theory during the process of analysis without becoming over influenced or biased and at the same time keeping the possibility of further developing existing theory. For this purpose, the stages of inductive coding, conceptual refinement and theoretical matching are selected from MGT (Goldkuhl & Cronholm, 2010) to form the basis of this dissertation’s primary analytical approach.

This approach of selecting separate parts or stages from an existing analytical model provided the much needed guidance during the analysis without having to apply the complete analytical model. Hence, it is important to note that this work does not apply MGT during data analysis but rather uses particular stages of MGT to provide a structured and methodological approach during qualitative data analysis. In line with the applied hermeneutic principle, the analytic strategy of this dissertation is highly inductive and grounded in empirical data, but at the same time equally grounded in pre-existing theory hence multi-grounded (Goldkuhl & Cronholm, 2010). These selected stages are performed in several iterations until an appropriate level of analytical saturation is achieved, hence when there are no new ideas emerging from data (Corbin & Strauss, 2008) and concepts as well as categories seem sufficiently developed and coherent to move forward and start focusing on the written record. Moreover, this strategy is also in line with the described aim of further development of knowledge and theory in the applied fields of ISR and eGovernment focused on public sector eID introductions previously described as the development of mid-range theory. To further clarify this process, the selected stages of MGT are described in detail each with a selected exemplification from the dissertation in Appendix 2.

2.6.2 Synthesis and development

Regarding the aims and purposes of theory applied in this dissertation, there are two clearly distinct differences. Hence, the theoretical perspective describes and positions the work in relation to existing relevant fields such as ISR, eGovernment and eID research (see Chapter 3) while the analytical perspective covers literature used for analysis, for example, the institutional perspective (see Chapter 4). While the literature base for the research perspective is identified by the hermeneutic literature survey described above, the analytical perspective is directly related to the emerging analysis hence empirically as well as theoretically grounded as described in the stage of theoretical matching. Hence, during analysis two clearly distinguishable and different streams
or areas of literature are identified hence referring to the sociological and institutional perspectives. The previously described needed synthesis between these two perspectives and the development of the synthesized analytic model will be briefly described below in the light of theory development or theorization. To be able to synthesize the previously suggested sociological and institutional perspectives, a conceptual framework called the socio-institutional framework. This framework consists of interrelated assumptions and concepts (Rodman, 1980) to be able to address the second and third research question (see Section 1.2) and is presented in detail in Chapter 4. This framework introduces a ‘four-stage institutional model’ containing the stages of (1) pressure, (2) barrier, (3) negotiation and (4) institutionalization (Figure 4). The concept of institutional barriers is later introduced referring to the previously described institutional resistance (see Section 4.4). This is motivated by how the resistance is perceived and translated by the actor coordinating the introduction. Hence, the resistance becomes a significant barrier obstructing the introduction process on social and organizational (institutional) levels. The relation between this institutional level and the translations on actor level is formed by linking these stages together via actors’ translations as illustrated by the arched arrows linking the four stages in Figure 4.

![Figure 4. The four-stage institutional model](image)

The pressure exerted on the organization in Stage 1 is translated by actors and these translations, in turn, develops into a barrier in their social context in Stage 2 (top arrow). This barrier is, in turn, translated (right arrow), and different strategies are launched during Stage 3 to possibly negotiate it by the central level coordinating actor. However, these strategies, in turn, become translated (lower arrow) and also influence institutionalization of barriers in turn affecting the ongoing exertion of pressures (left arrow). In detail, the barrier in Stage 2 is seen as directly derived from problem areas identified based on the different actors’ perspectives and translations of the eID, hence a result of the translation analysis (see Chapter 7 and 8).
This four-stage model facilitates an overall view of the socio-institutional framework applied in this dissertation and hence addresses the second research question (see Section 1.2). In addition, the development of this framework is also influenced by the conceptual framework presented by Mignerat and Rivard (2009), in turn being a synthesis of different perspectives itself (see Section 4.4). Moreover, as an example of successful theorization in ISR, Walsham (2006) puts forth Orlikowski (1993)’s development of concepts using grounded theory that brought together in a framework for the conceptualization of organizational issues regarding a particular type of IS (case tools). Hence, this dissertation provides a similar contribution to theory development as described by Walsham (2006). As previously described as the development of mid-range theory, this approach is motivated by addressing an identified gap by further development of existing concepts and frameworks hence applying or testing existing frameworks could not be used to address the research questions (Eisenhardt & Graebner, 2007). Regarding the process of theory development, a constant comparison between emerging concepts and extant literature searching for similarities and contradictions as suggested by Eisenhardt (1989) is applied during theoretical matching as well as considering a broad range of literature from different research disciplines. Fully aware that the extensive use of empirical data in theory development could result in overly complex theory (Eisenhardt, 1989). I therefore throughout this process strive for simplicity, transparency and clarity despite the rather complex context brought forth. In line with Eisenhardt (1989)’s guidelines, I also provide evidence of this theory-building process during its progression for transparency and assessment.

2.7 Quality, relevance and ethical considerations

2.7.1 Quality in qualitative research

Rigour is used to assess the quality of research and the means for attaining it are often described in terms of reliability and validity. Since these criteria are clearly related to rationalistic or quantitative research, attaining rigour or quality in qualitative research turns out to be an ongoing challenge (Morse et al., 2002). Different approaches are suggested for the use of similar criteria as quantitative research to scholars advocating that no predetermined criteria for quality should be used (Rolfe, 2006). As later described, this dissertation applies a strategy that can be placed in between such efforts with the use of a framework for quality assessment specifically aimed at interpretive research (Klein & Myers, 1999). Furthermore, an equivalent of rigour in qualitative research is described as trustworthiness (Morse et al., 2002), which I argue in this dissertation positively correlates with the described ontology of constructionism and the aim of developing understandings that are trustworthy and authentic (Denzin & Lincoln, 1994a). I am also in agreement with Corbin and Strauss (2008) describing that quality in qualitative research as related to several positive subjective properties of the reader since it deals and resonates with life experiences. Thus, properties such as delivering insights,
showing sensitivity and presenting enough detail in descriptions become important (Corbin & Strauss, 2008).

2.7.2 *Klein & Myers’ seven principles*

With the described increasing interest in interpretive research, questions are also raised on how to achieve and maintain quality in such research. Accordingly, Klein and Myers (1999) put forth a set of seven principles\(^{17}\) to ensure quality in interpretive case studies, and this approach is selected as the way of assuring quality throughout this dissertation. This framework is based on the fact that it is adapted to the interpretive perspective in ISR hence to be considered as a specific assessment tool rather than generic (Rolfe, 2006). It focuses on important areas and aspects to facilitate the development of the understanding of the parts as well as the whole in turn corresponding with the described applied hermeneutic principle. These seven principles themselves constitute a hermeneutic circle to ensure positive handling of the most central parts of an interpretive research process. These principles, briefly described in the following sections will then form the basis of a quality assessment presented in the final chapter ensuring transparency and clarity (see Chapter 10).

1. **The fundamental principle of the hermeneutic circle**

The first principle is important to all interpretive work and is, in fact, a meta-principle to be further expanded by the following six principles. The basic idea of this circle is that it is our preconceptions and interrelationships of the meanings are the parts that shape our understanding of the whole. After a number of iterations with focus shifts, a more complex whole of shared meanings will emerge (Klein & Myers, 1999). Hence, this first principle corresponds well with the underlying assumptions and perspective applied in this dissertation being of a clearly interpretive and hermeneutic character as previously described and motivated.

2. **The principle of contextualization**

The second principle is based on the notion that there is an inevitable difference in understanding between the author of a text and the interpreter created by for example the historical distance. Therefore, an important task in interpretive research is to seek the meaning in the surrounding context (Klein & Myers, 1999). For this dissertation, this principle implies the importance of actively developing a contextual understanding based on interpretations that are consistent with interpretations put forth by respondents.

3. **The principle of interaction between researcher and the subjects**

The third principle focuses on interpretive research as a result of the interaction between the researcher and the participants. This principle is aimed to handle that interpretive researchers also have to recognize the participants who in turn, like the researcher,

\(^{17}\) A set of principles for conducting and evaluating interpretive field studies in information studies (Klein & Myers, 1999)
should be seen as interpreters and analysts. Therefore, without interacting with the participants, there is a potential risk that these important aspects are overlooked (Klein & Myers, 1999). As previously described, during interviews the social interaction taking place and the development of mutual understanding is emphasized hence the interaction between me and the respondents become a very important aspect in order to be able to collect high quality empirical data. In addition, there are several other opportunities for interaction with subjects relevant for this study in the form of meetings, seminars and presentations described later.

4. **The principle of abstraction and generalization**

Principle number four addresses abstraction and generalization in interpretive field studies. As described, generalization in interpretive studies does not mean that theory is tested in a positivist way. Hence, it becomes important that theoretical abstractions and generalizations are related to field study details and described as they are experienced and collected by the researcher. This improves transparency and the theoretical insights presented by the researcher can be better understood (Klein & Myers, 1999). Accordingly, this dissertation strives for a high level of transparency and clarity throughout the process of analysing empirical data thus enabling the assessment of abstractions as well as generalizations of the developed knowledge.

5. **The principle of dialogical reasoning**

Principle five addresses the preconceptions guiding the research and requires the researcher to confront the preconceptions with the data emerging from the research process. The most important point is to make the fundamental intellectual basis of the research (i.e. philosophical assumptions) as transparent as possible relating to both their strengths and weaknesses. This is the lens through which the collected data are analysed, documented and organized. However, since hermeneutics consider the preconceptions, or prejudice/prejudice, as a necessary starting point of our understanding, the research findings may challenge the preconceptions which in turn might need to be modified or even abandoned (Klein & Myers, 1999). Hence, for this dissertation this principle implies the description of underlying research assumptions as well as a conscious dialogue as my preunderstanding or preconceptions of the studied phenomenon affects and are affected by the ongoing process of knowledge development.

6. **The principle of multiple interpretations**

This principle means that the researcher has to investigate the multiple viewpoints and reasons behind the actions under study. This may also lead to the confrontation potential contradictions and may, in turn, result in a revision of understanding. Revisions like these are similar to the ones described in principle five (dialogical reasoning), but the confrontation is between conflicting interpretations in the studied field and not between the researcher and the field (Klein & Myers, 1999). Considering multiple interpretations become very important for this dissertations with its emphasis on actors’ translations of
the eID. Hence it becomes important to actively seek a deeper understanding of any identified conflicting translations or similar translations existing in parallel.

7. The principle of suspicion
Finally, in principle seven, the principle of suspicion from Ricoeur (1976) is adapted arguing that sometimes consciousness can be seen as false consciousness where the idea is to reveal the effects of distortions and delusions. However, this principle seems to be the one least developed in the ISR field since it requires the researcher to go beyond just the understanding of the data and understand the social world behind the actor’s words (Klein & Myers, 1999). Although limited to the time of the interview, this means that I will work very actively in trying to understand the translations and meanings put forth by respondents. In addition, the applied sociology of translation (Callon, 1986) facilitates the actors participating in the network coming to speak on their own terms which I argue in turn minimizes any distortions.

2.7.3 Practical relevance
The Swedish Law of Higher Education\(^{18}\) clearly describes that universities have an important mission apart from providing education and performing research. This mission often referred to as science outreach or practical relevance is where universities should facilitate the development of knowledge in the surrounding community by working across the border of academia and the society and its practices (Brulin, 1998). In its latest amendment, the law clearly states that Swedish universities are governed by law to cooperate with the surrounding society in order to inform about their activities as well as research being performed in order to make research results available to practice (SFS 2009:45).

Thus, science outreach can be seen as efforts to bridge the existing gap between academia and practice; a well-known challenge that has been addressed by several scholars (e.g. Rynes et al., 2001; Van de Ven, 2007). This gap is also a consequence of the type of research being performed as exemplified by the rather high levels of abstraction in applied social sciences fields such as ISR. The challenge at hand is to perform research with the dual aim of knowledge development, for science as well as practice, and the main reason for this challenge being the problematic aspects of knowledge transfer between these domains (Van de Ven, 2007). Moreover, I argue that active measures to ensure science outreach is clearly related to research quality in interpretive research of ISR described above since this will ensure relevance, authenticity as well as trustworthiness in turn relating to underlying philosophical assumptions (Denzin & Lincoln, 1994a). To ensure the practical relevance an overview of the activities during this work are shown in Table 7. In this dissertation, these outreach activities are assigned with the dual purpose of actively communicating with practice as well as collecting empirical data. In addition, some activities also serve the purpose of providing quality assurance

\(^{18}\) Sv. Högskolelagen
such as the described expert validation in the eGov case and tentative results in the eHealth case is also presented for representatives on two occasions. During this work, I am very eager to keep close contact with eID practice in order to develop my own knowledge of this area in general and learn more about different organizational perspectives of the eID in particular.

Table 7. Types of science outreach activities – a selection

<table>
<thead>
<tr>
<th>Case</th>
<th>Practice context</th>
<th>Activity</th>
<th>Role(s)</th>
<th>Month/year</th>
</tr>
</thead>
<tbody>
<tr>
<td>eGov</td>
<td>eID special interest group</td>
<td>National eID network meetings</td>
<td>Participant, Presenter</td>
<td>2012-2013</td>
</tr>
<tr>
<td>eID Board</td>
<td>Presentation of tentative research (quality assurance)</td>
<td>Presenter</td>
<td>February 2012</td>
<td></td>
</tr>
<tr>
<td>Annual eID Day Seminar</td>
<td>Several participations on the annual eID day (conference)</td>
<td>Participant</td>
<td>2012, 2014</td>
<td></td>
</tr>
<tr>
<td>Open hearing</td>
<td>Attending an open hearing on the eGov eID as an observer</td>
<td>Observer</td>
<td>August 2012</td>
<td></td>
</tr>
<tr>
<td>Responsible ministry</td>
<td>Active dialogue with responsible officer and investigators</td>
<td>Interviewer, Informant</td>
<td>Spring 2015</td>
<td></td>
</tr>
<tr>
<td>eID Board</td>
<td>National IT media covering the eID</td>
<td>Cited source</td>
<td>Spring 2015</td>
<td></td>
</tr>
<tr>
<td>Central IT department</td>
<td>Feedback on tentative research (quality assurance)</td>
<td>Presenter</td>
<td>November 2012, March 2013</td>
<td></td>
</tr>
<tr>
<td>National eHealth Organization</td>
<td>Presentation of tentative research (quality assurance)</td>
<td>Presenter</td>
<td>August 2013</td>
<td></td>
</tr>
</tbody>
</table>

Summary of types of activities: 9

2.7.4 Scientific publications

In addition to practical relevance, measures are also taken to ensure relevance and quality of this dissertation in an academic setting, described as practical relevance in a research context. Throughout the work with this dissertation, I am active in several different constellations of authors resulting in a number of research papers and journal articles as summarized in Table 8.
<table>
<thead>
<tr>
<th>Publication</th>
<th>Type</th>
<th>Status</th>
</tr>
</thead>
</table>

19 Also available via AIS Electronic Library (AISeL), ECIS Proceedings, ECIS 2013 Completed Research (AISeL, 2013)
This results in nine publications of which seven have been peer reviewed between 2012 and 2016. This approach of working actively with research papers in parallel with the dissertation also provides the opportunity to evaluate and discuss different aspects and specific parts of the dissertation in an academic setting.

2.7.5 Ethical considerations

A researcher will always face many choices and potential conflicting values (Spradley, 1980) hence some kind of ethical guidance is required. In ISR there is a reported lack of specific ethical guidelines when conducting empirical work (Walsham, 2006). Consequently, research ethics refers to the moral standards applied to decisions during the processes of planning, conducting and reporting results of research (McNabb, 2002).

Four ethical principles have been put forth as being particularly important when conducting research in public administration and government studies such as this dissertation. While the principle of truthfulness will prevent the researcher from lying or engaging in any kind of fraud, thoroughness refers to the applied method being thorough and systematic. The principle of objectivity refers to the idea of research being free of any personal feelings or beliefs and free of any bias. The final principle of relevance means that research should always be conducted with a relevant purpose (Mitchell, 1998). So, referring this dissertation to these principles, truthfulness and thoroughness are clearly applied throughout the process. However, I argue that objectivity in its purest form does not apply to studies like this one applying a research perspective as based on interpretations and assigned meanings (Bleicher, 1993). Further, as described above, the continuous development of the researcher’s preunderstanding of the studied phenomenon is a basic tenet of the hermeneutic principle as the focus shifts between the individual parts of the study to the whole. Therefore I would like to interpret the objectivity applied in this dissertation in the way that this study is not by any means manipulated or controlled towards any predetermined results and propositions but instead guided by the knowledge development process of seeking and developing in depth understandings of the studied phenomenon of public sector eIDs.
Research perspective and method
Part II – Theoretical and analytical perspectives

The second part presents the relevant theoretical and analytical perspectives. Chapter 3 (The theoretical perspective) covers the research areas of Information Systems Research and eGovernment as well as different views of social and organizational implications of ICT and eIDs. Chapter 4 (The analytical perspective) presents the applied perspectives as grounded in institutionalism and sociology. Throughout these chapters, a certain level of evaluation has also been applied.
3. Theoretical perspective

This chapter covers the theoretical perspective with central research propositions and concepts as well as challenges and opportunities. The current research domain of ISR is described followed by the applied subdomain of electronic government. Relevant research focusing on social and organizational perspectives as well as electronic identification are presented followed by concluding remarks. A reflective tone is applied throughout the chapter, and informed choices are motivated. This chapter is related to the first (RQ-1), and third (RQ-3) research question since it provides the theoretical perspective needed in order to relate empirical findings to existing research and this perspective is later merged with findings from applying the analytical perspective in Chapter 4 for further analysis and discussion in Chapter 9.

3.1 ISR

3.1.1 ISR - an overview

Börje Langefors, often regarded as the founder of the Information Systems Research (ISR) discipline in Scandinavia, states: “In any organization, there is likely to be a lack of knowledge regarding what information systems can do, how one can make them do it, and what will be the effects.” (Langefors, 1993, p. 55). I argue this is a good description of one of the main challenges related to the implementation of ICT in different kinds of social, organizational settings and based on the described aim and purpose of this dissertation addressing social and organisational challenges related to public sector eID introductions (see Section 1.3) it also provides an appropriate point of departure for this work. Since its introduction, Information Technology (IT) and later Information and Communications Technology (ICT), has over time become a very strong force transforming and influencing organizations (Crowston & Myers, 2004). However, ICT related organizational challenges seem persistent over time and attract a significant interest of research focusing on aspects such as project risks (e.g. Lefley, 2015; Schmidt et al., 2001; Sherer & Alter, 2004; Vitale, 1986) and why such a high rate of projects continue to fail completely (e.g Keil, 1995; Nawi et al., 2011). Hence, this confirms the complexity and difficulties in predicting the effects of ICT in an organizational setting. This view is also in line with this dissertation since current public sector eID introductions are facing very similar problems when struggling to overcome

---

20 In the 1990s, this research field is often referred to as Information Systems. However, I choose to strictly refer to the field with its contemporary name of Information Systems Research (ISR). This also avoids potential confusion with the information system (IS) as an artefact.

21 Throughout this dissertation the term ICT will be used to refer to IT as well as ICT related efforts and perspectives.
unforeseen technical as well as organizational and social challenges (see Section 1.1.3). In efforts to develop a better understanding and more successful management of ICT projects, identified challenges have also been related to factors such as overconfidence in technology (Shalev et al., 2014). Best practices as well as critical factors to consider have also been put forth to facilitate ICT project success (e.g. Holland & Light, 1999; Rockart, 1982). These persistent challenges can be seen as the result of the inherent gap between technology and the organization hence this suggests the importance of a positive match between these two contexts to possibly avoid these problems (Leifer, 1988); a perspective also referred to as the organizational validity (e.g. Markus & Robey, 1983) or organizational fit (e.g. Hong & Kim, 2002; Iivari, 1992) of the system. However, I argue that such approaches easily become reactive without any deeper knowledge and understanding of the underlying causes behind these problems. Therefore, this seemingly persistent phenomenon in modern organizations of successfully introducing ICT (Davis, 1991) should, in turn, require a bridging of this gap with a suggested synthesis between technical as well as social perspectives (Dahlbom, 1996).

Investigating these challenges that emerge when the technological and social system of organizations interact (Lee, 2001) have grown to be one of the main focuses in the ISR field. As a social science, studies in ISR usually apply organizational and behavioural perspectives (Davis, 1991) and are mainly focused on one specific instantiation of ICT; the Information System (IS) with the assigned purpose of providing the information needed in an organization (Langefors, 1970). Placed at the intersection of other fields such as computer science and sociology (Davis, 1991), ISR develops into a transdisciplinary or interdisciplinary field of research (e.g. Landry & Banville, 1992; Robey, 1996). This allows scholars with a history in extant research fields to bring theories and methods to ISR (Avison & Elliot, 2006) and ISR scholars to approach other disciplines in search of appropriate theories and explanation models to address the challenges at hand. This interdisciplinary character of the field is also the subject of extensive debates over the years regarding if diversity should be considered a strength or a weakness of the field as opposed to so called reference disciplines (e.g. Benbasat & Weber, 1996; Robey, 1996).

There has also been what is referred to as an ‘identity crisis’, hence suggesting a more unified core of ISR for example as solely focused on the ICT artefact (Benbasat & Zmud, 2003). However, directly addressing this concern, Galliers (2003b) puts forth the argument that ISR must choose a specific path to follow and argues that the field needs to become even more transdisciplinary stating that it is “[Q]uintessentially trans-disciplinary in nature” (Galliers, 2003b, p. 337). Referring to the described interdisciplinary character perceived as a strength rather than a weakness. This is in line with my own view of the trans-disciplinary character as one of the strengths of the ISR field. To be able to address the ever changing implications of technology, researchers in IRS must have a multitude of perspectives and approaches at our hands to be able to address them.
This also seems to be in agreement with scholars in the field showing a great trust in the potential of ISR in the digital society arguing that the field should, in fact, be more relevant than ever. This due to the ever increasing speed of different technical innovations and therefore should become even more agile and focus on new emerging sociotechnical phenomena (Sørensen & Landau, 2015). Looking past the most obvious signs of multilevel diversity such as theoretical and methodological (Iivari & Lyttinen, 1998), several aspects of unity can be found in studies performed in subsets of the ISR field for instance related to the later described Scandinavian school (Iivari & Lyttinen, 1999). This dissertation is, therefore, to be considered as a typical example of such ISR studies since it applies a clear, structured and motivated transdisciplinary approach and in my opinion this research field is very suitable to investigate the social and organizational challenges at hand when it comes to ICT introductions in general and public sector eID introductions in particular (see Section 1.1.3).

3.1.2 The Scandinavian school

The Scandinavian tradition or school of ISR is described as having an “[U]n-proportional significance in the evolution of information systems (IS) as an academic discipline” (Iivari & Lyttinen, 1998, p. 135). As described, within this field different research traditions exist in parallel (Bansler, 1989) and traditions are governed by their knowledge interest, metaphysical (underlying) assumptions, basic notations and practical results (Bansler, 1990). The background of the Scandinavian school in ISR is described as related to the history of having a highly unionized labour market which in turn make the influence of unions very strong. This influence is on how employees are affected for example during the introduction of new technologies in the workplace hence managers have a history of cooperating with the unions to avoid any conflicts or disputes. Further, in Scandinavia, there is historically a greater interest in social and psychological implications of technology such as ICT in the workplace than in other countries (Bansler, 1989). Scandinavian ISR is therefore considered of being performed more on an operational or grass root level when compared to other countries such as the predominant management perspective in the MIS tradition in the United States (Iivari & Lyttinen, 1998). Further, different schools of research have in turn laid a strong foundation for a pluralistic view of ISR in the area. In accordance with the Scandinavian tradition of strong unions and typical research areas for the Scandinavian school of ISR are for example user participation and democracy (e.g. Bjerknes & Bratteteig, 1995), analysis of usability work (e.g. Iivari, 2006) and participatory design in systems development (e.g. Iversen et al., 2010). Accordingly, this Scandinavian perspective on ICT is applied throughout this dissertation with the aim of providing a fair and realistic view of social and organizational implications as caused by public sector eID introductions. However, the aim here is not to critique but rather reveal how potential shortcomings or underestimations affect these processes.
3.2 Electronic government

3.2.1 From public sector computing

In the wake of computers being increasingly diffused and used in businesses and organizations, significant benefits are estimated from these developments in local government by efficiency gains resulting from the replacement of labour with technology (Kraemer & Perry, 1979). With these benefits starting to realize in the public sector, this area receives an increased interest. With an increase in computing also follows an increase in awareness of the inherent organizational consequences and challenges. This, in turn, creates an interest in several relevant research areas such as management information systems (MIS), ISR and public administration studies. The potential of computing at the time, is widely acknowledged but at the same time an awareness about its organizational and social effects starts to grow; “A technology with such appeal and power undoubtedly affects individuals and organizations that use it.” (Kraemer & King, 1986, p. 488). As Kraemer & King put forth important effects of computing in public organizations, but several benefits are yet to be realized (Kraemer & King, 1986). The challenge for research as well as practice is therefore described as to focus on the experiences and lessons learned from the use of computing while seeking out appropriate and emerging management theories in the private and public sector. Hence, research wise, the main challenge is described as focused on empirical research of inherent management problems related to computing (Kraemer & King, 1986).

Later research and studies are focused on for instance public sector computing and innovation (Kraemer & Perry, 1989), how computing might affect the constitution and change power relationships in society (Kraemer & King, 1987), the lack of public sector theory and prescription in the MIS field (Bozeman & Bretschneider, 1986) and the lack of design and implementation of public sector specific information systems (Rubin, 1986). A decade later, Kraemer & King describe this area as still being problematic stating: “The rapid evolution of computing and communications technology offers unprecedented opportunities for the public sector, but also presents vexing challenges for the management of computing in public organizations.” (Kraemer & Dedrick, 1996, p. 3). They find that the research on public sector computing is not developing in the way they anticipated and the focus moves from impacts and management to various forms of use of computing in public sector; preferably by applying a technical perspective. Therefore, Kraemer and Dedrick (1996) argue that this area of research should be more focused on the most specific aspects of computing in the public administration context.

3.2.2 To electronic government

According to Grönlund and Horan (2005), the term electronic government (eGovernment, eGov) emerges when governments start to realize the use of Internet technology for public sector process improvements (UN & ASPA, 2002). Since the term is related to the general use of ICT in the public sector, it can traced back to the described field of public sector computing. In a broad sense, eGovernment is the use of ICT in order to
facilitate the governmental business (e.g. Chan & Pan, 2008) as well as governmental efforts to use the Internet to provide public digital services to citizens (Layne & Lee, 2001). These services are often also referred to as public electronic services (e-services). Hence, this provides a more broad description than just relating eGovernment to service provision via the Internet (e.g. Signore et al., 2005). However, the rapid development of the Internet in the late 1990s and 2000s significantly sparks the development of the eGovernment area (Grönlund & Horan, 2005). Moreover, I argue that this apparent dissonance about the meaning of the term is symptomatic and a sign of how specific technologies affect research fields. Hence the prefix of ‘e’ is added to show that this is a new approach to meet the challenges in the government sector. The broad view of eGovernment is in line with Grönlund (2002) describing it to cover the processes from strategic management to daily operations in government but the author at the same time puts a special emphasis on more efficient operations, better quality of services and better quality of citizen participation (Grönlund, 2002). Thus, this implies a clear relation with the improvement of government services on all levels ranging from internal to external. Further, Carter and Bélanger (2005) describe the area as: “E-government is the use of information technology to enable and improve the efficiency with which government services are provided to citizens, employees, businesses and agencies.” (Carter & Bélanger, 2005, p. 5).

Thus, this emphasizes the aspect of the eID as an enabler improving efficiency that applies to the supply of back-office services, as well as front-office demands of government authorities (Melin et al., 2016). To be able to grasp the rather complex concept, I argue that it can be simply explained by stating that eGovernment is about internal efficiency as well as external availability thus emphasising that there are two important sides of this coin. This definition also being in line with studies describing the dual benefits of eGovernment such as bringing increased agency efficiency and citizens’ benefits (e.g. Axelsson et al., 2013). Hence, eGovernment has therefore come to be used quite ambiguously describing current ICT related efforts as well as future aims of ICT in government (Relyea, 2002). Since eGovernment efforts, just like the described efforts in general, are related to the utilization of ICT in different governmental contexts, there is a multitude of obstacles and challenges ahead (e.g. Irani et al., 2007). There are several efforts to try to measure success and pinpoint specific factors (e.g. Holland & Light, 1999, 2001; Petter et al., 2008), such as critical success factors and stage models that would improve the probability of reaching success in eGovernment development efforts (e.g. Gil-García & Pardo, 2005; Layne & Lee, 2001). This is also in line with general ICT related perspectives aiming at successful outcomes by appropriate management efforts. One widely cited model is the four stage eGovernment model presented by Layne and Lee (2001) where these efforts are described as an evolutionary phenomenon, in turn, motivating this model to be divided into a four stage growth model for governments to follow. These stages range from cataloguing and transaction to vertical and horizontal
integration (Layne & Lee, 2001). Although being an example of a contested development model with a clear potential for further development (e.g. Andersen & Henriksen, 2006; Goldkuhl & Persson, 2006), I argue that this model nevertheless aligns with the described historical development of ICT in public administration. Hence, including an initial internal perspective on benefits realization later followed by inter-organizational synergies across organizational boundaries. As will be described, the national eID in the eGov case is no exception since the benefits of secure digital services as facilitated by the eID first realizing at specific authorities followed by centrally formulated strategies to push this development horizontally across the entire public sector (see Chapter 5).

In the eHealth case, the introduction of the eID is driven in a significantly different way since being clearly related to specific laws and regulations (see Chapter 6). Thereby, I argue that keeping this described broad view of eGovernment in mind, any clearly prescribed path to eGovernment success should, therefore, seem rather limited and not sufficiently problematized this development, in fact, covers public sector business development, cooperation and coordination in general. A simplified view the path to eGovernment success can, in fact, be related to a certain amount of technological determinism not sufficiently emphasizing the organizational and social context to be described. However, since these shortcuts to success inevitably draw attention, scholars also argue that these quick fixes may, in fact, impose several risks such as the described overconfidence of technology, as a reinforcement of an inherent bias towards technology (Andersen & Henriksen, 2006). Since eGovernment comes with a great potential of benefits ranging from an increased internal governmental efficiency to democratization and increased participation, the potential benefits of ICT delivering its potential in the public sector are described as enormous (Warkentin et al., 2002).

Despite its great potential, eGovernment development faces a great number of challenges (e.g. Irani et al., 2007; Ke & Wei, 2004) which I argue in turn is clearly related to the challenges related to ICT in general. For example, Ke and Wei (2004) describe government funding and support, common infrastructures, the digital divide and cross agency services as important aspects to address. Further, Strejcek and Theil (2002) find that government ICT projects tend to fail due to agencies acting too independently. Hence, poor coordination is described as a serious problem in inter-organizational and international eGovernment efforts are also a new kind of cooperation is introduced (Kubicek & Hagen, 2000). In line with my described notion of eGovernment efforts as in fact related to a more general public sector perspectives, Hazlett and Hill (2003) argue that these challenges, in fact, is a result of eGovernment posing some radical changes and significantly complex undertakings in the public sector.
3.2.3 eGovernment research

The research field of eGovernment is described as rapidly growing with underlying approaches and perspectives ranging from good practice via narrow to poor practice (Heeks & Bailur, 2007). Examples of good practice being described as the use of input from other research domains, such as public administration, and political science, acknowledging contextual factors as well as using primary data and different methods of research. These approaches are contrasted with examples of narrow practice described as related to the hype, lack of balance and over-optimism, positivist and a-theoretical approaches as well as the lack of empirical grounding. Finally, studies of poor practice are described as lacking in underlying perspectives, methods and data collection as well as the lack of rigour during collection, analysis and generalization. Further, a clear lack of theory is identified; applied as well as generated (Heeks & Bailur, 2007). However, although these examples are clear, I argue that they, in essence, are not specifically related to eGovernment research but instead can refer to the quality of any qualitative research efforts. Further, I argue that these are examples of trying to assess the current status and identity of the eGovernment field very much resembling the described historical path or ISR hence this fields legitimacy is also challenged (e.g. Scholl, 2006) as well as suggestions of how to ‘save’ the research field by moving into a specific direction (Lenk & Traunmüller, 2002).

Although Scholl (2007) acknowledges a move away from a historical, technological bias in order to address the complex reality of eGovernment efforts, the field is also described as “[A] conglomeration of partially intersecting and mostly juxtaposed studies from various disciplines.” (Scholl, 2007, p. 68). The following six variables are put forth to play a vital role in the forming of eGovernment research questions in order to minimize the risks of the field becoming too mono-disciplinary: (1) information use, (2) technology use, (3) public policy, (4) government operations, (5) government services and (6) citizen engagement (Scholl, 2007). Hence, this can be seen as an effort to try and operationalize the aim of eGovernment research on a slightly more detailed level than described above. However, at the same time, I argue that efforts like this are also examples of attempts of driving the development of a research field in a particular direction. In addition, more holistic approaches is suggested to balance technology and the often “complex socio-technical work reality” (Lenk & Traunmüller, 1999; cited in Lenk & Traunmüller, 2002) thus I interpret this as a call for research emphasizing the importance of acknowledging the social and organizational contexts as described in a later section. Furthermore, Bannister and Connolly (2015) put forth another challenge when describing the concerns about a lack of theory in the eGovernment field during the last decade. This also being in line with other scholars (e.g. Heeks & Bailur, 2007) and also described as an underrepresentation of theory generation in eGovernment research (Grönlund, 2004).
If eGovernment, is placed at the intersection of research fields as public administration and ISR (Bannister & Connolly, 2015) this should come as no surprise since both fields have faced similar challenges in the past (e.g. Harmon & Mayer, 1986; Swanson & Ramiller, 1993). Other possible explanations to the reported low level of theory generation in eGovernment research include perspectives on interdisciplinary fields as unsuitable of the generation of substantive theory due to a broad focus and funding of research indirectly influencing the type of research being performed (Bannister & Connolly, 2015). In addition, the limitations and challenges of the eGovernment field are as also described as related to: (1) the lack of a clear definition of the eGovernment concept, (2) underestimating complex institutional an political contexts surrounding eGovernment development and (3) a lack of process oriented eGovernment development studies as opposed to ones focused on the outcome (Yildiz, 2007). Moreover, this work addresses several of the concerns put forth in the context of eGovernment research. First, motivated by the described underlying perspectives as well as applied method (see Chapter 2) this dissertation should qualify as an example of good eGovernment research in accordance with Heeks and Bailur (2007).

Second, it focuses on the two variables of government operations and government services put forth as important (Scholl, 2007). Thus, government operations are exemplified by the covered eID introductions, and government services are related to the role of the eID as a public sector digital service enabler described below. Third, the suggested need for a broader focus on public sector eIDs (see Section 1.1.4) hence implying the inclusion of contexts such as social and organizational provides the needed holistic perspective (Lenk & Traunmüller, 1999; cited in Lenk & Traunmüller, 2002). Fourth, although this dissertation does not aim at generating theory of neither a substantive exclusively empirically grounded nor a formal highly generalizable type (Gregor, 2006), the aim of providing theoretical development in the mid-range (see Section 2.2.3) should nevertheless be seen as an active effort to potentially enrich and further develop existing theoretical constructs and concepts in relevant research fields. Finally, several challenges of the eGovernment field (Yildiz, 2007) are addressed such as acknowledging complex institutional contexts as well as applying a clear process perspective on the studied phenomenon of eID introductions in the public sector (see Chapter 4).

### 3.3 Social and organizational perspectives

In line with this dissertation’s emphasis on social and organizational implications of public sector eID implications (see Section 1.1), existing research focusing on these perspectives becomes very important to consider. However, these perspectives will not be used as a basis for any deeper analysis, in turn, is covered by the analytical perspective presented in Chapter 4, but as the theoretical lens through which empirical and analytical findings will be further discussed in Chapter 9.

---

22 Theory developed for a specific area based on the analysis of observations (Gregor, 2006).
3.3.1 The organizational perspective

Mason & Mitroff oppose the strong role of MIS designers and argue in favour of becoming more informed about the effects of such systems in an organizational setting. Thus, they put forth a list of key variables including organizational context and state: "There are large, if not infinite, number of ways that one can discuss the influence of organizational structure on the design of MIS." (Mason & Mitroff, 1973, p. 483). Mason & Mitroff also describe that the relation between organizational structure and IS design is neglected and conclude that “We must seek to become better informed about the effects of the key variables which comprise a management information system.” (Mason & Mitroff, 1973, p. 485). Later elaborated by Ein-Dor & Segev, the importance this organizational perspective is described as highly related to structure and people, as an aspect in need of further investigation (Ein-Dor & Segev, 1978). However, since these studies are performed within the described MIS tradition, they try to identify variables for management and seeks out how this aspect directly or indirectly affects the success of the MIS. Thus, I argue that this perspective results in the construction of over-simplified causal relationships between the organization and the IS. Nevertheless, these early studies make an important point stating that the organizational context is one of the key aspects to consider in order to gain IS success in organizations. Later, Leifer describes the match or fit between IS and organizational design as a highly underappreciated aspect affecting IS success (Leifer, 1988) and an ill fit of this kind could, in turn, be the result of not fully assessing the IS organizational context.

This positive match between the organization and IS, is also described as organizational validity hence it is the “[T]he ‘fit’ between an information system and its organizational context of use” (Markus & Robey, 1983, p. 203). Hence, despite the early efforts described above, scholars argue that the dominant focus on technology in MIS research tradition is non-sufficient (Markus & Robey, 1983). This is also building on previous research confirming a positive fit as a key enabler for successful implementations and use of ISs (Robey, 1981). Further, it is concluded that “[C]hanging organizational structure to bring the CBIS [Computer Based Information System; author’s note] and organization into a more natural fit is a strategic necessity for many organizations.” (Leifer, 1988, p. 71). Hence, these are recommendations that the IS determine the rules that the organization has to comply and follow. Iivari describes that the fit, match or congruence between the organizational context and information systems will be increasingly important as systems will become increasingly integrated into organizations (Iivari, 1992). However, this perspective is still reported as being ‘largely neglected’ in ISR (Iivari, 1992). Hence, using the concept of ‘fit’ in contingency theory as a basis and applying it in the organizational science domain, forms the underlying assumption that the structure and context of an organization must fit together in order for the organization to be successful (e.g. Drazin & Van de Ven, 1985; Van de Ven & Drazin, 1984). Thus, a similar
framework to be applied in the ISR field is suggested hence also implying contingency theory to be applied in areas such as IS impacts and adoption (Iivari, 1992). With an increasingly changing environment, organizations tend to change their strategies regarding IS developments. There is an increasing trend of implementing commercially pre-packaged application software rather than developing their own systems in-house (Hong & Kim, 2002). This strategy being motivated as a way to potentially minimize negative consequences of in-house development that I argue can be related to resources, maintainability and dependency. In addition, the increased use of this type of standardized systems also put the systems into the hand of users more quickly (Gremillion & Pyburn, 1983). During this period, different models trying to identify and manage critical factors for IS success maintain their strength as exemplified by the DeLone and McLean model being one of the most cited (DeLone & McLean, 1992). However, I argue that efforts maintaining focus on the management of critical factors to facilitate success still present a rather deterministic view of the IS as inevitably related to a social and organizational context. To balance the focus on technology, there is also a shift towards research investigating the user perspective of the IS and how perceived usefulness and usability affect IS success (e.g. Franz & Robey, 1986; Thong & Yap, 1996; Torkzadeh & Doll, 1999). Nevertheless, the match between IS and organization is still an elusive challenge to manage and in the 2000s resulting in research under different labels such as IS strategic alignment (e.g. Preston & Karahanna, 2009). Thus implying an increased strategic alignment between top management and ICT management to facilitate increases in IS success.

Hence, I argue that efforts like this can be seen as attempts to close the gap between organization and technology on higher strategical levels which in turn can give rise to new concerns if these challenges are perceived from a lower level organizational or social perspective. In addition to the organizational context, organizational change and its relation to ICT is also a popular research focus in ISR in order to gain more knowledge about the implications of ICT in an organizational setting (e.g. Armenakis & Bedeian, 1999; Avgerou, 2001; Keen, 1981; Markus, 2004; Orlikowski, 1993, 1996). Myers and Young describe the important focus on social, organizational and political aspects of IS development and a basic notion is put forth stating that development of IS is to be considered a political activity hence referring potential hidden agendas in efforts such as user participation and user involvement (Myers & Young, 1997). In addition, political forces are put forth as potentially influencing IS efforts along with “taken for granted aspects of social reality such as managerial assumptions” (Myers & Young, 1997, p. 238). Although not explicitly relating to the concept of institutionalism, I argue that this is an example of an early effort in ISR trying to develop an understanding of the underlying social ‘steering mechanisms’ affecting IS development with references to the concept of the institution (Myers & Young, 1997). Therefore, I argue that the step towards acknowledging institutionalism as an appropriate approach and applying a sociological view on organizations is not far (see Section 4.2). Further studies acknowledging this
perspective are for example Klein and Hirschheim (1991) focusing on IS rationality concepts by applying Jurgen Habermas’ critical social theory, a theoretical approach also applied by scholars such as Ngwenyama (1991), Lyytinen and Klein (1985) and Broadbent et al. (1991). This focus, applying a clear critical perspective on politics and power in relation to information systems, can thus in turn clearly be related to the Scandinavian tradition of critical ISR described above. Hence, in the areas of public sector computing and later eGovernment, government level policies and agendas become very important factors of influence. The described approach of Myers and Young (1997), also build on Habermasian social theory as adapted by Broadbent et al. (1991) and describes this approach as a modern society consisting of lifeworlds, systems and steering media. Lifeworlds guide behaviour, attitudes and action and are formed communicatively based on experiences and beliefs. Further systems are expressions or instantiations of lifeworlds as functionally defined in organizations and thereby guided to follow the concerns of the respective lifeworld. Steering media, finally, are the means by which these systems are held together in forms such as power and money and the media become represented through different forms of societal institutions. Thus, government, professional and financial institutions could be characterized as societal steering media being institutions that use their own steering mechanisms to guide the behaviour of societal systems (Myers & Young, 1997). The relations between societal steering media, steering mechanisms and societal systems are shown in Figure 5 below where the steering media steers the societal systems via its range of steering mechanisms.

Figure 5. Societal steering media and systems (adapted from Broadbent et al., 1991, p. 8)

Thus, steering media steer societal systems in accordance with lifeworld demands but it is also possible for steering media to try and steer societal systems in ways that are in opposition or conflict with their own lifeworld demands; a process called “internal of the lifeworld” (Myers & Young, 1997). Put shortly; this could happen when there are contradictions between the lifeworld of the societal steering media and the lifeworld of the societal system. This is illustrated by Broadbent et al. (1991) with a case where government is trying to introduce a new market based model in the entire public sector; a model that in turn a National Health Service (NHS) objected to since it is not in line with the aims and goals, the lifeworld, of that particular organization (Myers & Young, 1997). The government is actively trying to colonize the lifeworld of the NHS via its administrative and legislative means as steering mechanisms. Accordingly, I argue that
The relationship described in the figure above between societal steering media and societal systems via a range of steering mechanisms very much resembles the institutional perspective described in Chapter 4. The societal steering media can potentially correspond to the concept of institutional pressures for conformity, steering mechanisms can be related to strategic responses to such pressures and the implications in societal systems to institutional effects (see Section 4.2). The relationship described in these models is based on a force in the external social context put onto organizations via social mechanisms such as law and regulations or normative rules and values with the aim of influencing the organization in a certain direction. Thus, I argue that the concept of ‘colonizing the lifeworld’ of an organization (Broadbent et al., 1991) is equivalent to the concept of institutionalization in institutionalism (see Section 4.2.1) however formulated with a slightly more negative emphasis. Based the described approaches in research emphasizing the organizational perspective there seems to be a move towards an emphasis on the social context and structures resembling institutions, which brings us further to research focusing on the complex relationship the social and the technical.

3.3.2 The social and the technical

There are studies that focus either on the technical or the social aspects, but there are also a large number of approaches that are trying to bring them together for a deeper understanding of these challenges. An example of such views is the perspective of Socio-Technical Systems arguing that the organization is a work system containing two interrelated subsystems, the social and the technical. Accordingly, the technical system covers technology, tasks and processes and the social system is concerned with people and their relations, skills and attributes et cetera. Hence, the output of these systems is the result of their interaction (e.g. Bostrom & Heinen, 1977). Another example is Science and Technology Studies (STS), an interdisciplinary research field with underlying notions such as science and technology as socially embedded enterprises and technology as socially constructed (Bijker et al., 1987). Thus perceiving technical innovations as a result of merging sociotechnical relations with inherent social, scientific and technological views (e.g. Roth et al., 1996). On a general level, STS is described as consisting of two streams of research focused on science and technology, with one focusing on reception, appropriation and institutionalization, and one focused on the production of science and technology (Roosth & Silbey, 2009). As an example of perspectives related to ICT, the ensemble view suggests suggesting that the technical artefact is only one part of the ensemble required to apply it to socio-economic activity (Orlikowski & Iacono, 2001). Clearly distinguishing between two different fields of theorization within this proposed view with a perspective on how technology is formed with reference to Latour (1987) and a perspective on how technology is used with reference to Kling and Scacchi (1982). Hence, on the one hand, Kling & Scacchi applies a much broader perspective on technology than traditional approaches, for example, taking staff and organizational arrangements into consideration to facilitate effective use of new technology. While, on the other hand, Latour addresses the tendency to black-box technology in social science (Orlikowski & Iacono, 2001). These perspectives, therefore, converge since there is a
Theoretical perspective

general consensus that one research field alone seems to be insufficient to tackle the challenges ahead in these efforts aiming at an increased understanding of technology in an organizational setting. On a general level, this work can be seen as applying an ensemble view of public sector eIDs since it emphasizes the need to acknowledge the broader context of eIDs. However, as later developments in this field show, there are also different perspectives on how technology is perceived and approached. In addition, the concept of ‘the social’ is approached from two different perspectives (sociological and institutional) hence I argue that any characterization of this approach needs to be done in a more nuanced way. Orlikowski and Scott later present the concept of sociomateriality (e.g. Orlikowski, 2007; Orlikowski & Scott, 2008) and although published in the research field of management and organization studies, this perspective has a significant impact and is frequently applied in ISR (e.g. Doolin & McLeod, 2012; Monteiro & Rolland, 2012; Svahn et al., 2009; Wagner et al., 2010). This perspective is categorized as being one of a relational ontology as opposed to the historically dominating substantialist ontology in ISR and management research. While substantialism perceives the social and the material as separate entities engaged in different kinds of interactions, relationalism assumes that these parts are inseparable and only exist in relations (Cecez-Kecmanovic et al., 2014).

The introduction of the sociomaterial perspective also causes a debate in the ISR field resulting in several counterviews (Cecez-Kecmanovic et al., 2014). For instance, shortcomings regarding how technology is handled and an evident neglect of social structures are put forth, resulting in the neglect of systems’ specificity and an inability to handle practice in a broader context (Mutch, 2013). However, in response to Mutch, the authors reply that sociomateriality cannot be judged by the way it is applied since it is still in its infancy. They perceive the critique put forth as an unjustified ontological critique by someone who has not fully understood the concepts of this approach (Scott & Orlikowski, 2013). In short, sociomateriality marks a departure from the view of seeing objects and actors as self-contained entities that influence each other via interactions or impacts. Instead, the focus is on the influence of technology on humans and how materiality has become an inherent part of our everyday relations and activities (Orlikowski & Scott, 2008).

Further, Actor Network Theory (ANT), developed by sociologists such as Callon (1986) and Latour (1987), is referred to as an important influence which in turn is an approached that focuses on relations and networks between human and non-human entities and treats them as equals. Bruno Latour describes this as: “Contrary to the claims of those who want to hold either the state of technology or that of society constant, it is possible to consider a path of an innovation in which all the actors coevolve.” (Latour, 1991, p. 117). This perspective seems to be a path of ISR research that attempts to seek the answers to ICT related issues by incorporating sociological approaches, hence these approaches can be considered as attempts to move further away from a pure focus on the
ICT artefact as such but rather consider it as a part of an entangled view of organization and social life. Thus, sociomateriality is the enactment of a set of activities where materiality is amalgamated in social aspects such as norms and institutions (Leonardi, 2012). What these different approaches have in common is the notion of bringing the technical and social together and not reverting to a separated perspective of dualism or as Orlikowski states: “Instead, the social and the material are considered to be inextricably related — there is no social that is not also material, and no material that is not also social.” (Orlikowski, 2007, p. 1437). To position this dissertation in the field of research focusing on the social and the technical is therefore not an easy task since I have a priori not reflected on which schools or streams of research that are actually applied this study. To further complicate things, several perspectives are integrated into the analytic perspective (see Chapter 4).

However, using Orlikowski and Scott (2008)’s overview and categorization of research in this field, I conclude that the sociological perspective applied in this work (see Section 4.4.3) clearly can be positioned as applying a sociomaterial perspective since a framework related to Actor-Network Theory (ANT) is applied to investigate perspectives and relations between different actors arranged in networks (see Section 4.3.4). These actors are created based on their individual perspectives, aims and goals as well as their relations within this network. Thus, referring to these actors as material or human (social) in fact becomes obsolete. This analytic approach, therefore, embraces the sociomaterial notion of dissolving any boundaries of the social and material. In addition, ANT is suggested being in line with the sociomaterial perspective (Orlikowski & Scott, 2008) which I argue further strengthens this suggested position. Further, the institutional perspective applied in the analysis (see Section 4.4.2) applies a clear process perspective on how institutional resistance is formed as related to the sociological perspective.

According to Orlikowski and Scott (2008), this perspective can, therefore, be characterized as acknowledging mutual dependent ensembles with a focus on the interplay between elements of organizational life, in this case, institutions, and aspects of technology. However, in the upcoming analysis, these ‘aspects of technology’ are in fact facilitated by the outcome of the translation analysis as related to ANT. Thus, in a sociomaterial sense, there are no boundaries of technology but rather only translations of technology. Further, Orlikowski and Scott (2008) also confirms this position by describing the recent application of institutional theory in this stream of research. Hence, in summary, the rather complex task of trying to position this dissertation based on its theoretical and analytical stance within the social and organizational research perspective results in the following position:
3.3.3 Social theory in ISR

Since the perspectives described above are examples of research perspectives applied in ISR as clearly influenced by social theory, I consider it relevant to further describe how this discipline have been applied and inspired studies in ISR. Social theory and its application in the ISR field goes back for instance to the Marxist theories describing the role of technology in social change (e.g. Braverman, 1974, see Hanseth et al., 2004). Further, since the effects of technology are seen as far too deterministic by researchers in ISR, more constructivist approaches emerge (Hanseth et al., 2004) and as a consequence, other theories based on sociology are approached. For instance, Structuration Theory (ST) (e.g. Giddens, 1984) offers a clear example and is applied by scholars such as Orlikowski (1992) and Walsham and Sahay (1999). ST itself is founded by the British sociologist Anthony Giddens and the theory can be seen as an attempt to create a synthesized and integrated approach by bringing together different traditions in sociology with the two central concepts of structure referring to the structure of social systems and agency as related to human agents and human action (Walsham & Han, 1990).

Since, ISR has problems finding a relevant theory to describe social and organizational aspects of technical artefacts in the past (Walsham & Han, 1990), turning to sociology is seen as one possible strategy to solve these problems. Over time, ST is successfully applied by several scholars (e.g. Barley, 1986; Orlikowski, 2000; Orlikowski & Gash, 1994; Orlikowski & Robey, 1991; van Veenstra et al., 2014; Walsham, 1993) and its diffusion and use in ISR is also investigated (e.g. Jones & Karsten, 2008; Poole & DeSanctis, 2004; Walsham & Han, 1990). On a general level, the strength of ST is to counteract against either technical or social determinism (Markus & Robey, 1988), advocating that structures are continuously formed and re-formed through practice (Orlikowski, 2000) as well as the consideration of social processes (Jones & Karsten, 2008). However, the application of ST in ISR is also a subject of critique and for instance Jones and Karsten (2008) argue that it is a general theory which aims to explain the social aspects of organizations and hence lacks an inherent link to the ISR field.

Rose (1998) describes ST as a meta-theory and quite far from the concepts and issues of IS practice. Hanseth et al. (2004) go even further and argue that studies applying ST go equally bad based on the fact that this theory lacks the ability to address the role of technology in a proper way and this is due to the fact that ST in itself totally ignores technology. However, several studies apply ST in ISR and thus acknowledge technology as a structure which enables and/or constrains human action (e.g. DeSanctis & Poole,
1994; Orlikowski, 1992; Walsham, 1993). Thus, I argue that this critique can be a result of ICT becoming increasingly entangled into deeper social structures hence perceiving technology as a separate structure becomes problematic. Nevertheless, Hanseth et al. (2004) describe that viewing technology as structure, as in ST, enabling and/or constraining social structures is a poor conception of technology and this is a problematic idea that contradicts Giddens’ original concept, i.e. that structures are only traces of mind with no material existence. Orlikowski (2000) responds to this critique with the dual concept of technology, the concept of the artefact and technology-in-practice, and argues that the distinction is a purely analytical one. Further, the author describes that the perspective of artefacts-in-practice is “an especially useful one in both empirical research and everyday usage” (Orlikowski, 2000, p. 425).

Therefore Grint and Woolgar (1995)’s notion that “[T]echnology exists only in and through our descriptions and practices, and hence it is never available in a raw, untainted state.” (Orlikowski, 2000, p. 289) is also accepted. However, Hanseth et al. (2004) disagree with this description and claim that it is the relationship between the artefact and technology-practice that needs to be addressed in order to understand technology in a social context. Actor-Network Theory (ANT) is suggested as an appropriate means for addressing this relationship and in turn increase the described need for increased theorization of the artefact (Hanseth et al., 2004). Hence, this dissertation is an example of such relational views of the focused artefact (eID) and by applying an ANT-related perspective to further investigate the relationships between the actors in the defined network (see Section 4.3.4).

3.3.4 Resistance to ICT

In an ICT related context, resistance is often described as related to resistance to related to organizational change facilitated by ICT (Hirschheim & Newman, 1988). Although this work delimits from the perspective of organizational change (see Section 1.5.1), this specific subtopic offers relevant theoretical insights to be able to describe and discuss the type of resistance addressed in this dissertation. Historically, there is a myth of resistance as inevitable when ICT is introduced on a large scale thus explicit or overt resistance is seen as dysfunctional behaviour that should be eliminated (Hirschheim & Newman, 1991); as faults that need to be suppressed or ignored (Keen, 1981). It is even described as a plague: “User resistance to information systems development and use has plagued the computing community for decades.” (Hirschheim & Newman, 1988, p. 398). This perspective of technology as flawless is therefore in line with the history of technical determinism. However, over time more realistic and nuanced perspectives emerge that actively tries to develop an increased understanding of how and why this resistance occur. Thus, explanations of resistance are indeed important since they can improve management as well as the development and implementation of systems (Markus, 1983). However, resistance is still seen as one of the primary reasons behind the high rate of IS/ICT project failure (Hirschheim & Newman, 1988). Since resistance to ICT can take many forms ranging from covert manoeuvring to outright sabotage, it
can be obvious almost at an instant or lay dormant for a considerable time (Hirschheim & Newman, 1988). To manage covert resistance, management literature proposes a number of well-established proactive measures that potentially minimizes resistance such as a focus on people affected, assessing readiness, training, redesign of organizational structures, new ways of management and increased involvement (Markus, 2004). However, rather little is said of how ICT affects organizational resistance (Marakas & Hornik, 1996; Markus, 2004) since ICT related research such as ISR instead tend to focus on user acceptance (Klaus & Blanton, 2010). Nevertheless, resistance to ICT continues to be a clearly under researched area (Lapointe & Rivard, 2005; Laumer & Eckhardt, 2010). Thus, I argue that since the act of sabotaging ICT related efforts being rather uncommon, at least to my knowledge, it is especially the covert resistance laying dormant and staying unnoticed for a considerable time that poses significant threats to ICT efforts such as eID introduction.

This speaks against the idiom of ‘no news is good news’ in this context, where in fact ‘no news’ can be very bad news just waiting to surface. This focus is also needed to contrast existing theoretical perspectives of resistance often assuming resistance to be an observable type hence not to any larger extent acknowledging covert behaviour as active resistance (Marakas & Hornik, 1996). Further, non-use of ICT can also be seen as related to passive resistance and normally related to sanctions in a mandatory context of system use (Marakas & Hornik, 1996). However, there are also different types of non-use also including different types of non-conformance to prescribed use of artefacts. Thus this type of resistance related to the absence of prescribed behaviour must also be taken very seriously since it, for example with underlying conflicts, can result in a total rejection of ICT (Newman & Robey, 1992). Further, as Markus (2004) point out, resistance can turn out too difficult to handle and overcome thus cancelling a project might be the only solution, however, this can also have a negative effect on future similar efforts.

Hence, this is an example of negative effects on the legitimacy of such efforts; an aspect that will be further described in Chapter 4. Nevertheless, it is also important to keep in mind that resistance to ICT, in fact, can have positive effects such as identifying inherent flaws or shortcomings of technology. It can, in fact, result in the future avoidance of undesirable change (Hirschheim & Newman, 1988). Moreover, resistance can also be seen as a signal from the system that there are costs of ICT that needs to be weighed against benefits (Keen, 1981). If costs outrun benefits by far, efforts may have to be reconsidered. Further, this work is based on the existing challenges of addressing and handling resistance to public sector eIDs, but the occurrence of these challenges should come as no surprise since this phenomenon is very complex. Causes of resistance are described as many and varied and occur in complex states hence it is the interaction of these states that results in a particular resistance thus resistance is described as very
difficult to describe by causal relationships thus causes as well as manifestations of resistance show a considerable variance (Hirschheim & Newman, 1988). Since overt resistance also is proven to be associated with unresolved conflicts (Robey et al., 1989), resistance in some cases can also be seen as a secondary side-effect which I argue in turn motivates further investigations and development of increased understanding. There are several efforts trying to categorize and describe resistance in research with for example Markus (1983) describing three perspectives on resistance to ICT as associated with (1) people, (2) system and (3) interaction. First, people or groups may resist systems due to internal factors and second, factors inherent to the technology of the system may cause resistance. Third, the interaction of the system may cause negative consequences resulting in resistance such as centralized control over decentralized authorities or negative implications on the context where systems are used. Further, Markus (1983) also describes familiar causes about resistance as related to (1) lack of top management support and user involvement, (2) systems with technical problems, (3) systems with poor usability, (4) change by default and (5) systems’ costs outweighing benefits. In a slightly more detailed effort to cover plausible causes of resistance, Hirschheim and Newman (1988) describe it as related to the causes summarized in Table 9.

Table 9. Causes of resistance (adapted from Hirschheim & Newman, 1988)

<table>
<thead>
<tr>
<th>Cause</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Innate conservatism</td>
<td>A general resistance to change.</td>
</tr>
<tr>
<td>Lack of felt need</td>
<td>A lack of perceived benefits.</td>
</tr>
<tr>
<td>Uncertainty</td>
<td>Resistance as a result of fearing uncertainty in terms of work duties, skills needed, prestige and status.</td>
</tr>
<tr>
<td>Lack of involvement</td>
<td>Exclusion from decisions or participation associated with change.</td>
</tr>
<tr>
<td>Redistribution of resources</td>
<td>The introduction of an IS may result in resources being redistributed associated with negative implications.</td>
</tr>
<tr>
<td>Organizational invalidity</td>
<td>A divergence between IS features and characteristics of the organization.</td>
</tr>
</tbody>
</table>
Theoretical perspective

<table>
<thead>
<tr>
<th>Cause</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lack of management support</td>
<td>Management support as crucial for acceptance.</td>
</tr>
<tr>
<td>Poor technical quality</td>
<td>Negative aspects of IS related to poor technical quality.</td>
</tr>
<tr>
<td>Designer characteristics</td>
<td>IS designers are focusing on technology while neglecting users' perspectives.</td>
</tr>
<tr>
<td>Other causes</td>
<td>Lack of training, lack of knowledge, cognitive dissonance i.e. presentation is not matching the cognitive style of users.</td>
</tr>
</tbody>
</table>

Such efforts of categorization and identification of causes can be used as a first step when trying to address these issues. Further, despite the fact that resistance in this work will be described on actor level but further synthesised and discussed on an institutional level (see Section 4.4), the described perspective of resistance to ICT although provides important concepts and categories in order to relate and discuss this phenomenon. There are views put forth, for example, relating resistance with aspects and relationships in the social context (Lawrence, 1969 cited in Hirschheim & Newman, 1988). Hence, this is in line with the perspective of focusing on the relationship between actor level translations and institutional resistance. This work will therefore also provide a link between existing research on ICT resistance and pressures on the institutional level of organizations for new insights. Thus, based on descriptions above, this work defines resistance as ‘the overt or covert social expression of affected actors resisting the introduction of the eID in the particular organizational context’.

3.3.5 Path dependency

Apart from resistance as related to affected actors’ perspectives on ICT efforts, I argue that there also are underlying incentives in affected organizations that can be related to the described challenges of introducing eIDs in the public sector. One such incentive or factor being the previous experiences of working with eIDs as in the eGov case (see Chapter 5) or the absence of eIDs in the workplace (see Chapter 6). This means that the eID being introduced will potentially converge or diverge with an organization’s previous historical path in this area which in turn brings us to the perspective of path dependency. In political science, path dependency is described as a state when “actors are hemmed in by existing institutions and structures that channel them along established

---

24 Although the theoretical field of legacy systems could also apply here, I have delimited this work from this perspective since I interpret it as primarily focused on the internal technical infrastructure or backbone of organizations (e.g. Bisbal et al., 1999).
policy paths.” (Wilsford, 1994, p. 251). Hence this notion of perceiving the historical path as an institution aligns very well the later applied institutional perspective (see Section 4.2). When transferred to ISR, path dependency is described as an organization’s previous experience with a technology influencing its adoption of new technology in the same field (Zhu et al., 2006). Hence, it is a matter of the described potential divergence between historical experiences and future development; a matter of competing technologies and a possible lock-in due to an organization’s historical events (Arthur, 1989). Originating from the field of economics (David, 1985), nowadays path dependency on a very general level emphasizes the role of historical events when handling challenges in the present. A slightly more detailed description of this concept states that “path dependence means that current and future states, actions, or decisions depend on the path of previous states, actions, or decisions” (Page, 2006, p. 88). Research describes four causes of path dependency as increasing returns, self-reinforcement, positive feedbacks and lock-in (Page, 2006) as summarized in Table 10.

Table 10. Causes of path dependence (adapted from Page, 2006)

<table>
<thead>
<tr>
<th>Cause</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Increasing returns</td>
<td>Over time, returns and benefits of similar actions and decisions increase.</td>
</tr>
<tr>
<td>Self-reinforcement</td>
<td>Repeated actions and decisions are reinforced via institutions.</td>
</tr>
<tr>
<td>Positive feedbacks</td>
<td>Added bonus to actors that are making similar decisions.</td>
</tr>
<tr>
<td>Lock-in</td>
<td>If made a sufficient number of times, actions or choices become better than any other.</td>
</tr>
</tbody>
</table>

Although these causes are summarized with an applied perspective of political science, I argue that increasing returns, self-reinforcement as well as lock-in can easily be transferred into an ICT context. Hence, increasing returns related to similar actions and decisions being repeated over time can be related to increased efficiency thus allocating resources as a positive outcome. In business agreements for example covering delivery of ICT services between actors, a development of trust over time will also work in favour of this arrangement. In addition, as Page (2006) denotes, institutions can have an important role regarding self-reinforcement as over time there is a clear tendency of actions as well as decisions to develop into social norms and values shared among actors or groups of actors (see Section 4.2.1). Despite not being easily transferred into an ICT
context, I argue that positive feedbacks can be related to systems use and user compliance or non-compliance. Hence, positive feedback for example in the form of lack of sanctions can potentially result in the act of non-compliance being shared among actors if it brings significant benefits. Lock-in finally, although normally related to the concept of technological lock-in (Arthur, 1989) to refer to challenges such as related to changes in technological paths of development as a result of for example intra- och inter-organizational dependencies developed over time. However, it is still important to acknowledge the potential lock-in of actions and decisions as well. Thus, I argue that such lock-ins also can be related to the cause of self-reinforcement since institutionalized actions and decisions also create a certain level of lock-in due to the absence of reflective behaviour in favour of behaviour as based on socially shared taken for granted norms and values. Based on this very brief overview of the concept of path dependence, I argue that this aspect is important to consider when introducing eIDs since these efforts inevitably challenge the history of decisions and events in affected organizations. In existing research, path dependency has also been confirmed as an important aspect to consider when analysing national eID efforts described below (e.g. Kubicek & Noack, 2010a, 2010c; Melin et al., 2016). In addition, path dependence can also be considered as a potential cause of resistance hence there is a potential relationship between these two perspectives of challenges in ICT efforts.

3.4 Electronic identification

With a described call for a broader focus on public sector eIDs in research (see Section 1.1.4), it is important to deeper investigate the relevance of this claim in the light of existing eID research. This will also facilitate the use of existing research as a common point of departure for further investigations as well as learning from previous research regarding important challenges and aspects to consider. In addition, this kind of overview also provides the opportunity of a clear positioning of this work in relation to prior research efforts.

3.4.1 On identity, identification and authentication

In the introduction, I described my own interpretation of basic concepts relating to eIDs such as identity and identification (see Section 1.1.1). Therefore, it becomes important to first investigate how such concepts, as central to the eID area, are described in existing research. Clarke states that “An identity is a presentation or role of some underlying entity.” (Clarke, 2008, p. 222) where an entity, in turn, is a thing existing in the real world. Moreover, identities can be associated with different attributes, and an entity can, in turn, be associated with more than one identity a relationship (Clarke, 2008). This relationship is illustrated in Figure 6. In an IS context, entities and their related identities are represented with different sets of data which in turn corresponds to the related entities and attributes in the real world (Clarke, 2008). In modern digital society, organisations have come to commonly deal with data records representing people rather that dealing with the people themselves and the data represented in a particular record is only
a very limited model of the identity and its underlying entity. However, the data representing an entity needs to be distinguishable from other entities or instances of the very same category. Thus there is a need of an identifier with common examples being usernames or unique personal identifiers.

Figure 6. The entity, identity and attribute relationship (based on Clarke, 2008)

The identifier is related to the identity or role rather than directly to the entity (Clarke, 2008). Thus, this perspective is fully in line with my own presented view of the identity as the core of this concept and the common name of eID as related to the digital or electronic representation of attributes. However, there is a slight difference here in how Clarke perceives identity as a representation separate from attributes. Hence, it is important to notice that my previous description of the concept of identity as consisting of a ‘unique combination of attributes’ (see Section 1.1.1) referred to the inherent parts of for example a unique personal identifier. Thus, the attributes as referred to by Clarke (2008) above are the properties assigned to an entity as identified by its identity. Hence, the digital identity of an entity is a set of digital attributes assigned to or characterizing the entity (Jøsang, 2015). As a result of the described increased development of the eID as an enabler of secure digital services (see Section 1.1.2), a rather complex interplay between identity, identification and information systems is today a reality (Whitley et al., 2014).

Since the eID is becoming increasingly important in organizations (Smith & McKeen, 2011) as well as in society at large as implied by its described role as an eGovernment enabler. Therefore, I argue that this complex interplay or relationship needs to be further problematized to avoid any risks since the eID inevitably is related to our digital integrity and privacy. Hence, for example, if the security of a digital service handling sensitive personal data gets compromised and/or data is extracted, the risks of negative consequences of personal integrity are imminent. As described, the term electronic identification is a term often used in the context of eIDs, but this use can be misleading and
confusing (see Section 1.1.1). According to Oxford English Dictionary, identification means “The action or process of identifying someone or something or the fact of being identified” and “A means of proving a person’s identity, especially in the form of official papers: ‘Do you have any identification?’” (OED, 2015). Therefore, identification is associated with the process of identifying someone and says little or nothing about the result of this assessment and the context in which it takes place. Therefore, as previously stated, in relation to eIDs the term of authentication is a better use since it is related to “The process or action of proving or showing something to be true, genuine or valid.” (OED, 2015). It is the authentication that provides the required certainty about an identity between interacting parties during for example online transactions (Jøsang, 2015). Further, Whitley & Hosein describe the distinction between these two concepts as identification related to the revealing of an identity while authentication is a process of accepting someone as authorized to a certain context (Whitley & Hosein, 2009). The use of authentication in relation to eIDs is also related to different organizations’ requirements of non-repudiation regarding their online transactions. That the authenticity of an identity or signature can not be denied and ultimately hold up in court. In addition, in the information society, the protection of personalized data is of great concern and tightly linked to basic human rights, personal privacy, integrity concerns as well as different aspects of security. Moreover, the registration process, when the physical identity of the individual requiring the eID, is often described as a very crucial security parameter (Kubicek, 2010; Kubicek & Noack, 2010b). So, in order for a user’s identity to be authenticated for access to a particular (physical or digital) service context, the user (1) presents an identification, the artefact, which shape or form varies depending on the context, physical or digital. This identification is then (2) authenticated, and if valid and true, access to the service context is authorized (granted) (Figure 7).

Figure 7. The three-step authentication model

In an attempt to describe personal identity, Beynon-Davies (2006) presents a model consisting of the inter-related processes of identification, authentication and enrolment (Figure 8). In this model, the identifier is a referent of a digital identity that an actor has in the digital world. However, the identification is in turn dependent on the previous successful outcome of the authentication as a prerequisite for the actor to be able to take part and benefit from digital services (enrolment). What I find particularly interesting about this model is the process named enrolment. This term adapted from Actor-Network Theory (ANT) (e.g. Callon, 1986; Latour, 1991; Law, 1999; Law & Callon, 1988) is motivated by the need to acknowledge that the individual must join or be enrolled in
some kind of ‘human activity system’ where a group of actors perform activities with a shared sense of meaning a common goal (Beynon-Davies, 2006). This coinciding with the enrolment as an important step in the upcoming translation analysis based on a framework related to ANT (Callon, 1986) (see Section 4.3.4).

Figure 8. Identification, authentication and enrolment (adapted from Beynon-Davies, 2006)

3.4.2 eID research

As described, the current development of digital services has pushed forth an increased problematization of digital or electronic identities. This is related to the development of increasingly complex and sophisticated digital services as part of eGovernment efforts, in turn being dependent on personal information. Thus, obstacles and problems related to electronic identities facilitate the emergence of the research field focusing on eIDs or digital identities (Halperin & Backhouse, 2008). Similar to the field of ISR, the constant development in the surrounding contexts of digital identity such as technological, commercial and political, constantly presents new challenges (Halperin & Backhouse, 2008). Hence, the more we use our eIDs, the more entangled they become in our social life as well as society at large. Therefore, research on digital identities focuses on an increasing number of key issues such as security and privacy, interoperability as well as convenience and intrusiveness (Halperin & Backhouse, 2008). For instance, Cavoukian (2008) describes implications of the Internet on digital identity and privacy and Hansen et al. (2004) show how privacy enhancing technologies can increase privacy related to identity management systems. Further, interoperability is a well-known area in related areas such as eGovernment (e.g. Scholl, 2005), hence, applying it to digital identity brings forth opportunities as well as potential risks such as data protection and privacy concerns (e.g. Halperin & Backhouse, 2008; Otjacques et al., 2007). Thus, the tendency is clear, with the eID bringing new opportunities for an increasing number of areas, new sets of challenges are introduced due to its nature. These new challenges are particularly difficult to handle in specific contexts such as health case where any newly introduced threats are particularly severe for example related to integrity and privacy concerns.
Theoretical perspective

(Angst & Agarwal, 2009; DeCew, 1999). As exemplified by the challenges in the eHealth case (see Chapter 6), the introduction of eIDs in electronic healthcare (eHealth) bring new challenges (e.g. Stroetmann et al., 2011) that in turn can pose severe threats to patient confidentiality (e.g. Anderson, 2006). A future need of research focused on identity management has also been acknowledged in fields like eGovernment as a result of public digital services (e-services) becoming more advanced and dependent of personal data and in turn secure authentication processes (Dunleavy et al., 2006). Moreover, the increased need for identity management can also be seen as a result of individuals having multiple identities each bound to a specific electronic context or service and clearly related to the increased level of remote interaction and communication between individuals and organisations and governments (Beynon-Davies, 2006).

In addition, there is also a potential conflict or opposition between intrusiveness and convenience resulting from the introduction of digital identity technologies (Halperin & Backhouse, 2008) for example the potential privacy threats introduced by wireless technologies (Eckfeldt, 2005). However, being an emergent research area, Halperin and Backhouse describe a need for the identity research field to establish fundamentals of identity hence its conceptual foundation (Halperin & Backhouse, 2008) which in turn resembles the described identity seeking process of the ISR field. Other examples of studies on identity have focused on several different contexts such as biometrics in financial transactions (e.g. Assadi & Hassanein, 2009; Breward et al., 2009), identity fraud profiling (e.g. Jamieson et al., 2008) and policy engagement processes in identity projects (e.g. Whitley & Hosein, 2007). As predicted by scholars (e.g. Dunleavy et al., 2006; Halperin & Backhouse, 2008), in recent years a significant amount of identity research have focused on identity management (e.g. Barnard-Wills & Ashenden, 2010; Hansen et al., 2014; Jøsang, 2013) and often related to the management of national level eIDs in the context of eGovernment (e.g. Seltskis & O'Keefe, 2010) as will be described below.

This increasing development and use of identity management systems also result in efforts to increase the interoperability in order to minimize integration efforts of eIDs and provide seamless authentication across different organizations’ digital services. One way of achieving this is by separating authentication and authorization from the applications or digital services themselves. This strategy being most commonly known as a federated architecture where access and identity information is shared between organizations in an identity federation (Meinecke et al., 2005). More simply put, Schweighofer and Hötzendörfer (2013) describe this as “[T]he ‘re-use’ of user accounts across the borders of individual organisations.” (p. 231). With this kind of inter-organizational eID solutions, also exemplified by the eGov case (see Chapter 5), the authorization only has to be done once resulting in an issued security token then passed along between different applications provided by members of the federation (Meinecke et al., 2005). Common known examples of these kinds of solutions today are the user accounts of Google and
Facebook which can be used for accessing several types of digital services (Schweighofer & Hötendorfer, 2013). However, since the eID has been in active use in several areas such as eGovernment and eBanking for a considerable time, I argue that these kinds of second generation development efforts, in turn, will introduce new challenges as well as challenge a well established practice (see Chapter 5). This brief overview of the research field of eIDs shows a clear history of a technical focus. However, I argue that with the realization of benefits from digital identities and eIDs in an increasing number of areas of application, there will most likely emerge new challenges and obstacles that needs to be handled. Thus, in line with the described historical development of ISR, I argue that the interest in social and organizational implications of eIDs will most likely increase in related areas such as ISR and eGovernment. Hence, being subject to predominantly narrow technical perspectives in the past, in turn being a clear consequence of being related to new uses of technology, I argue that the eID as a research interest clearly moves towards more soft approaches putting forth social and organizational perspectives. However, in my readings, I have found a clear lack of social as well as institutional perspectives as suggested by this dissertation; perspectives that in turn are needed to be able to develop better understandings of the implications and influences caused as related to the eID.

3.4.3 An eGovernment enabler

In recent years, the interest in national level eIDs is significantly increasing, both in the form of smart cards, and other varieties such as software based or most recently different kinds of mobile eIDs. A significant driver behind this development, diffusion and use of national eIDs, as issued by the state as well as private market actors, is the described increased need of securely identified citizens related to the development of digital public services or e-services (e.g. Melin et al., 2013, 2016). The eID can, therefore, be seen as an enabler for secure identification as well as an enabler of current and future eGovernment efforts. Further, Rössler describes this as eIDs being of a “[P]aramount importance for almost any e-Government application.” (Rössler, 2008, p. 447). Hence, the eID is of great importance of secure authentication in an eGovernment context. Seltsikas and O’Keefe (2010) describe that the need for facilitating electronic identification of individuals becomes manifest when governments embrace the opportunities of eGovernment that in turn include a new electronic way of interacting and transacting with citizens and businesses. Hence, the service personalisation we have seen in recent years in areas such as eGovernment digital services also requires the users to securely declare their identity (Corradini et al., 2006). As described, this need can, in turn, be traced back to being the equivalent of the traditional ways of identification in service relationships where the identity has to be securely established in order for correct and non-reputable service provision (Strauß, 2011). Guided by the notion of having an eID to cover a nation’s entire population, an increasing number of countries have developed their own national eID solutions. With significant variations in success, eID research is also taking an increased interest in the inherent opportunities as well as challenges related to such efforts, as will be described in the next section.
3.4.4 National eID introductions – an overview

This section provides an overview of some typical examples of national eID introductions in Europe. This to be able to put the eID introduction in the upcoming eGov case into an international perspective. The overview will end with some comparative remarks. Thus, the aim of national eID solutions is to improve efficiency and secure authentication by supplying an eID to be used in the entire public sector in a country and is historically proposed by several initiatives on EU level. However, without any central coordination, these initiatives turns out to be quite different in practice which in turn pose significant obstacles for eID initiatives across borders (Aichholzer & Strauss, 2010) such as eIDAS described later. The national eIDs described below are selected motivated by showing important challenges and opportunities of national eID solutions. Sweden will not be included in the following overview since this description will be provided in Chapter 5. In short, the Swedish model is described as a rather complex solution based on a market approach with no central governance however with a good service supply and use compared to other European countries (Grönlund, 2010). Thus, this rather weak eID governance (Söderström, 2012) is described as lacking inter-governmental and public and private sector coordination (Melin et al., 2013) and with a history of being clearly path dependent (Kubicek & Noack, 2010a). However, as described, the introduction of a new version of the national eID in Sweden faces significant challenges (see Chapter 5).

Belgium

Often described as one of the pioneering countries in Europe, the Belgian card based eIDs (BELPIC) issued to all citizens begins rollout in 2004 (De Cock et al., 2004). The eIDs, are based on the national register number, are issued on municipality level (De Cock et al., 2006) and are mandatory for all citizens from 12 years and special kid’s cards are also issued between the ages of 6 and 12 to be able to access online services for children (De Cock et al., 2008). The potential risk of requiring card readers at home is estimated to be handled with an increased number of public digital services with clear benefits for citizens, and there is also a free card reader distribution programme (De Cock et al., 2006). Thus, even though the Belgian eID card strategy can be described as very strongly supported by government and inclusive hence a success in terms of development and diffusion, later studies identify clear obstacles and quite severe shortcomings. For example, citizens’ use and eID uptake in digital services remain limited for a considerable time. This is in turn described as a result of the lack of private sector convergence and public sector digital service development and in addition the distribution of card readers among citizens remains low (Marien & Van Audenhove, 2010).

Estonia

Together with Belgium, Estonia has often been described as one example of very successful eGovernment development in general and national eID introduction in particular. After receiving full independence in 1992, the government makes a clean slate start
introducing a new population register including a new unique personal identifier hence this is described as one of the factors facilitating the following eID development and introduction. The state issued eID is introduced in the form of a national identity card in 2002 however during the following years, Estonia shares similar results as Belgium regarding low levels of uptake and use. However, agreements between major banks, telecom companies and government facilitate a significant increase in use. Thus, the banks offering eID services to third parties such as government actors, become competitors to the national eID issued by the state (Martens, 2010). However, a high level of government digitization and online availability also introduce new risks as for example, in 2007, when denial of service attacks brought down online sites and services such as the parliament, agencies, banks, newspapers and broadcasters (Anthes, 2015).

**Denmark**
The first eID initiative in Denmark is traced back to the beginning of the 1990s as related to eGovernment initiatives at that time. However, public concerns against a mandatory eID card’s potential central storing of data result in the proposition of an optional card in 1996, but this project halts due to technical disagreements. At the beginning of 2000, eID efforts are renewed, and it is decided that an independent identity provider is to be used. A leading Danish telecom provider wins the tender, but as seen in countries such as Germany and Estonia, online banking develops rapidly at this time. An institution owned by the banks wins the second tender which should ensure the security in the national eID solution being rolled out. However, this eID initiative shows low levels in uptake and use mainly due to unclear benefits from using digital services as well as technical difficulties regarding the eID (Hoff & Hoff, 2010). Thus, in 2010, the government decides on a new strategy focusing on the market convergence between the public and banking sector. The new eID (NemID) offers the ability to be used in public sector digital services as well as in eBanking services (NemID, 2015).

**Finland**
The Finnish Electronic Identity (FINEID) card is based on the population register and integrated on a smart card issued to residents from the age of 18. Introduced in 1999 as a non-mandatory eID card to replace the previous ID card solution. This eID is created with having the benefits of use in public sector digital services in mind from the beginning. Hence, Finland is the first country in the world to introduce an eID to all residents, but acceptance and use is low due to the competition from existing eID solutions in areas such as online banking. The FINEID card is managed and provided by the Finnish Population Register Centre which in turn manages the central Population Information System. However, in 2010 the FINEID accounts for only less than one percent of all online transactions in public as well as private sector while the competing online banking eID (TUPAS), owned by a federation of banks, has over 99 percent. In 2003 it was decided that these markets should converge which brings the opportunity to use the TUPAS eID in public digital services (Rissanen, 2010).
**Germany**

There is a long tradition of identification and registration of citizens in Germany, and the possession of a personal ID card or passport is mandatory. Hence, this makes the use of any unique common personal identifier prohibited by law. The eID process starts in late 1990 with a focus on legislation of eSignatures and later a new digital ID card is chosen as the carrier for the eID. The process is driven by high levels of government with a clear focus on technical aspects and in 2009 a bill is passed that allows the eID to be used for online authentication. Since the new eID card also holds biometric data (fingerprints), the collection of such data causes a public debate due to integrity and privacy concerns which in turn further slows down the process (Noack & Kubicek, 2010). In addition to the ID card, there have been several other eID initiatives with potential eID functionality in Germany such as the electronic health (eHealth) card, the electronic proof of income (ELENA) and electronic tax declaration (ELSTER) (Horsch & Stopczynski, 2011). There is also a parallel process as the result of online authentication needs in the banking sector. Hence a common standard for online banking services (Home Banking Computer Interface, HBCI) is developed based on a smartcard solution. A potential market convergence with the public sector is also identified, and these plans are welcomed by Federal Government. However, as it turns out, most German banks are reluctant to support the HBCI standard and develops their own authentication and signing methods instead referring to obstacles such as usability, card reader requirements and a separate card for signing. Therefore, at the moment, the use of eIDs for authentication and signing in Germany is still very low, but hopes are put to new and emerging methods for mobile platforms (Kubicek & Söderström, Submitted).

**United Kingdom**

In the United Kingdom, there is a history of a failed attempt of trying to introduce a new national identity card that also should serve as a carrier of the eID. Initiated in 2001, this project is eventually abandoned in 2010 after a long series of challenges, strong opposition and may millions of pounds spent. It is also notable that this effort brought severe irregularities in government information systems violating human rights and data protection laws into the light (Beynon-Davies, 2011). Since then, a new online identity initiative is launched in the United Kingdom called the Identity Assurance Programme, a federated identity model, explicitly addressing some of the major pitfalls of the previous identity card programme. For example, with an extensive cooperation with identity providers there is no centralised identity database and due to its multi-provider setup security is deemed to be higher and less vulnerable (GOV.UK, 2015). With this model the state has lost its role as an identity provider but instead verifies the identity’s state based attributes such as citizenship and entitlement to benefits. Identity providers’ assurance levels and legal certainty is provided by accreditation schemes certifying identity providers to supply identity services to service providers in the public sector (Whitley, 2013). Different assurance levels are also offered to meet the need of security and protection levels varying across services (Brostoff et al., 2013). Thus, this approach actively
addresses several obstacles and concerns related to a centralized identity management system. Hence, with this type of federated identity systems, there seems to be a growing trend of governments opting out of the role as identity providers and rely on identity providers existing on the market instead (Brostoff et al., 2013).

**Additional remarks**
The described introductions of these national eIDs show clear variances but also several significant similarities. First, a unique personal identity number seems to be an important prerequisite for issuing eIDs on a national level. All featured countries except for Germany, have these common personal identifiers which in turn can be one of the reasons why the German eID efforts have struggled for a considerable time. Thus, the mandatory possession of an ID card or passport by law prevents the use of such an identifier hence potentially resulting in a fragmented landscape of identifiers among identity providers. Second, eIDs issued by the state seems to be a problematic concept. Hence, in Belgium, Finland, Estonia, Denmark and the United Kingdom, the first initiatives are eIDs as issued by the state but all these countries also face serious problems. Third, eIDs issued by the state are very dependent on available digital services with clear benefits for citizens. Hence, Belgium and Estonia show similar signs of poor uptake and use of the state issued eID due to lack of e-services. Fourth, the historical path of government has a significant impact on eID efforts. Estonia can, therefore, take full control in forming a new population register, and national identity cards are swiftly issued. This is contrasted by Germany where the law prohibits the common identifier, passports have a strong role and are prioritized over eID efforts and government applying a very technical and problem oriented focus during eID discussions.

Fifth, integrity and privacy risks can potentially an entire national eID effort at risk. This is most significantly exemplified by the United Kingdom where severe violations of data protection laws and human rights are part in the abandonment of the first eID initiative. Further, in Denmark as well as Germany concerns regarding potential threats to privacy and integrity severely challenge and stall the eID process. Sixth, finally, convergence with identity providers existing on the market is the key. Thus, in Estonia, Denmark, Finland and the United Kingdom, all current national eID solutions are the results of a market convergence where private market identity providers, preferably banks, and joint efforts of banks and/or telecom companies. Thus, in the end, it seems that relying on already issued, diffused and used eIDs have a significant positive impact on national eID efforts which in turn brings us back to the clear benefits of using eIDs in digital banking services. Based on the six identified recurring patterns of the described national eID efforts, I argue that these, in turn, can be used to identify the following three key factors of these efforts: the eID, diffusion and use and digital services. Thus, the eID itself must be secure and not by any means risk aspects such as personal integrity and privacy and it can not be issued with a clear lack of service contexts adding clear benefits to users hence taking advantage of existing diffusion and use becomes a great advantage.
Accordingly, this emerging insight of the importance of the aspects of the eID, diffusion and use and digital services in relation to national eID will be taken into consideration when comparing the outcome of this study in the light of these national eID introductions in the final chapter.

3.4.5 Cross border eIDs

As the eGov case will show (see Chapter 5), there are clear potential obstacles when trying to make departmental or organizational eID silos interoperable agreeing one unique common identifier (Whitley et al., 2014). However, there are current examples of eID interoperability on a much larger scale with the use of eIDs across national borders as predicted in 2008/2009 (e.g. Rössler, 2008; van Oranje-Nassau et al., 2009). As a result of the subsidiary role of the European Commission, each member state has more of less developed their own eGovernment systems, in turn, depending on different types of eID systems. As a result there is a clear fragmentation of eID development efforts across Europe and a multitude of potential ‘identity silos’ (Leitold, 2011; Seltsikas & O’Keefe, 2010). Nevertheless, several European initiatives and projects such as STORK\(^{25}\), in 2014 result in the adoption of an EU level regulation\(^{26}\) called eIDAS\(^{27}\) focused on cross border trust services and interoperability of eIDs to replace the only previous directive related to eIDs, the Signature Directive\(^{28}\). Accordingly, this cross border effort will eliminate the current electronic barriers between the European countries (Leitold, 2011). Hence, Europe is indeed currently on the road to cross border use of national eIDs for public e-services but even though member states have no chance of opting out since it is enforced law, is still a major complex undertaking operating on a very tight timeframe with a mandatory recognition of foreign eIDs by 2019 (see Section 5.1.11). In addition, there may even be resistance to such approaches (van Oranje-Nassau et al., 2009) and since it in fact potentially challenges the path of every introduced national eID. Since its adoption on EU level, there have been several views in research focusing on the aim and possible consequences of eIDAS (e.g. Cuijpers & Schroers, 2014; Hühnlein, 2014; Massacci & Gadyatskaya, 2013; Ruana, 2014; Schroers & Van Alsenoy, 2014). However, the fact remains as Dumortier and Vandezande (2012) point out; the real work of realizing the eIDAS is still depending on the success of its delegated implementing acts among member states. So, even though resistance to the regulation itself is futile, is being forced on member states without exactly knowing how it will turn out in practice. Hence, these efforts can potentially turn out to be problematic since cross border functionality is not a governing aspect of national eIDs in the past (Leitold, 2011).

\(^{25}\) Secure idenTity acrOss boRders linKed, several EU-level projects aiming at providing eID interoperability across borders within the union.

\(^{26}\) A legal act of the European Union immediately enforced as law in all member states.

\(^{27}\) “Electronic identification and trust services for electronic transactions in the internal market” (EU 910/2014, 2014)

\(^{28}\) An EU directive on the use of electronic signatures within the union.
3.5 Concluding remarks

To conclude this chapter, I will provide a short summary of the theoretical views selected to form the theoretical perspective of this dissertation. Hence, this perspective, as comprised of relevant theoretical propositions, will be used to relate empirical findings to existing research during the final analysis and discussion in Chapter 9.

Figure 9. Theoretical perspective – a conceptual map

In combination with the analytical perspective to be presented in Chapter 4, the theoretical perspective provides an ontological basis for further characterization and discussion of analytical findings. For clarity, selected propositions and concepts as motivated in previous sections are categorized, described and related to each other in the conceptual map illustrated in Figure 9. The research field of ISR (1), provides this work with the
needed interdisciplinary approach of an applied social sciences field advocating theoretical pluralism. Hence, this provides opportunities to seek theoretical view and explanation models in other relevant research disciplines without having to risk the perceived quality of research being performed. Social and organizational implications of ICT being one of the central research areas in ISR also corresponds well with the aim and purpose of this work to investigate these implications in relation to public sector eIDs. In line with the Scandinavian school of ISR, this work puts special emphasis on the grass root or operative level of studied organizations. The focused resistance to public sector eID introductions can also be seen as an example of the challenges of ICT that has to be overcome in the public sector eID context in turn relating to one of the core topics of ISR.

Next, eGovernment (2), as a sub-domain in ISR, focuses on the implications of ICT in public administration or government. Hence in research, there are underlying incentives clearly related to eIDs in terms of increased efficiency and availability via the delivery of public digital services. The safeguarding of personal data being one core property of eGovernment efforts as well as one of the main purposes of the eID by facilitating secure authentication to digital services. As described different forms of coordination are on the current agenda of eGovernment research as well as in present eID initiatives. A central challenge in eGovernment efforts as described in research is the historical independency of public sector actors which in turn present challenges for coordination efforts. Similar patterns are identified in the public sector eID area where the development so far seems to have been governed by needs of individual actors rather than central government coordination efforts. Hence, eGovernment of course also provides views on the challenges of ICT efforts in the public sector with the introduction of eIDs being a clear example.

The Social and organizational perspective (3) of ICT being a special research interest of ISR provides the opportunity to further investigate these dimensions of the eID as being in line with this work. The concept of organizational fit becomes a central point of departure to address the challenges ahead when the operational focus of the eID is applied. Research focusing on steering mechanisms and colonization of ICT efforts are particularly interesting since these views clearly resemble the institutional perspective applied in Chapter 4 hence any potential synergies between these two perspectives are potentially fruitful. Moving further towards research influenced by sociology, the concept of mutually dependent ensembles and sociomateriality is described as corresponding well to the institutional and sociological perspectives of the analytical approach described in Chapter 4. Hence, how these views are applied in relation to ICT provide valuable information. Existing research focusing on resistance to ICT as well as path dependency of ICT efforts provide important concepts and constructs to apply to upcoming analytical findings. This brings us to the central artefact of this work, the eID (4) as an enabler
of eGovernment efforts and in turn clearly dependent on the described social and organizational perspective. Thus research on digital identity as well as authentication and authorization becomes crucial. Insights from previous research regarding the dependency on the digital service context as well as the current trend of identity federations will facilitate further discussions. The use of the term of enrolment in eID research seems particularly interesting due to its strong relation to the applied analytical perspective of Actor-Network Theory (ANT). Since the eGov case presented in Chapter 5 is an example of a national eID solution, research focusing on these types of solutions becomes important to acknowledge. The similar applies to professional eIDs as related to the eHealth case in Chapter 6. The increased focus of eIDs for cross-border interoperability becomes an important factor to consider related to the eGov case, and organizational identity is of significant meaning to the eHealth case.
4. Analytical perspective

This chapter describes the analytical perspective needed in order for this dissertation to provide its purpose and aim. The institutional perspective covers underlying assumptions and basic concepts, specific propositions relevant to this work, its application in ISR and eID research as an overview of how it is applied in this work. The sociological perspective focuses on the suggested approach as related to Actor-Network Theory (ANT), its application in ISR, challenges and opportunities as well as a description of the framework to be applied. This is followed by the synthesized socio-institutional framework motivated and described in detail. This chapter covers the second research question (RQ-2) describing the applied analytical perspectives to investigate the resistance to eIDs as related to actors’ translations. The analytical perspective is later merged with the results from translation analysis (Chapter 7 and 8) and the theoretical perspective of Chapter 3 for further synthesis, analysis and discussion in Chapter 9.

4.1 Introduction

During recent decades, ICT is empowered with a potential to transform organizations as well as entire fields of industry and given a role of not only organizational support but also organizational development and change. This being in line with the potential of ICT in general as well as eGovernment related efforts in particular (see Section 3.2). As a result of an identified need to broaden the focus of ICT related studies, the following three perspectives are suggested: economic, institutional and social/cultural (Crowston & Myers, 2004). Hence, the economic approach focuses on the relations between organizations and their inputs and outputs, the institutional on contextual issues surrounding the organization and the social/cultural perspective on structures and processes within the organization itself (Crowston & Myers, 2004). As described this dissertation applies a process view investigating the relationship between actors’ translations and institutional resistance (see Section 1.1.4) hence I argue that equal emphasis is put on the sociological as well as the institutional perspective suggested above. First, it is clearly institutional, since it acknowledges institutional resistance as a social structure (e.g. Berger & Luckmann, 1967; Scott, 2014). This structure becomes a strong force influencing actions as well as decisions in organizations (e.g Bowring, 2000). In this study as a resistance to the pressure to introduce (e.g. DiMaggio & Powell, 1983) public sector eIDs. Second, it is also social since it integrates the perspective of sociomateriality (e.g. Orlikowski & Scott, 2008) (see Section 3.3.2) by applying a relationalistic perspective of actors’ translations of the eID, with an adapted framework from sociology (Callon, 1986). This approach can also be seen as a result of inspiration drawn from related ISR research acknowledging the need for social and organizational perspectives of ICT (e.g.
Jones & Karsten, 2008; Walsham & Han, 1990) (see Section 3.3.1). This work is also in line with previous research perceiving the institutional context as formed and reformed by a continuous process rather than a static force (e.g. Barley & Tolbert, 1997). Further, this analytical perspective is based on a described institutionalist perspective as influenced as sociology, in turn delimiting from focuses of traditional institutionalism such as formal structures and economic aspects (see Section 1.5.1). The relation between translations and resistance will thereby be put in the foreground which in turn results in the suggested synthesized socio-institutional framework described below. Prior research efforts to combine the institutional and actor centred perspective include institutional factors and actors such as actor-centred institutionalism (e.g. Scharpf, 1997). Although this perspective has mostly been applied in political science and policy research (e.g. Mur-Veeman et al., 2008), it has also been successfully applied as to ICT in general and eIDs in particular (Kubicek, 2010; Kubicek & Noack, 2010a). For instance by linking the institutional setting to operational level aspects such as actors, constellations of actors and modes of interaction (Mur-Veeman et al., 2008).

However, with a few exceptions (see further Schneiberg & Clemens, 2006), I argue that it still seems to be a shortage of research applying a relational process perspective on sociological and institutional aspects. In addition, the presented analytical perspective is also an answer to calls for an increased emphasis on the process of institutionalization (e.g. Barley & Tolbert, 1997; Tolbert & Zucker, 1996). To further motivate and explain the underlying causal relationship guiding this analytical approach, I will refer to Markus and Robey (1988)’s typology of causal structures in theories, in turn, divided into the dimensions of causal agency, logical structure and level of analysis. Thus, the analytical perspective presented in this work, the causal agency, as the identity of the agent participating and the direction of this causality, is categorized as providing an emergent perspective (Markus & Robey, 1988). The causality is assigned to the complex character of the eID context where the social and the material become intertwined and inseparable (Orlikowski & Scott, 2008).

This in contrast to the technological and organizational imperatives viewing the focused area as the sole casual agent (Markus & Robey, 1988). If the eID with its purpose of providing secure authentication for a specific individual, is excluded from its appropriate social context, it completely loses its purpose as well as its meaning. The eID is also assigned with a clear social meaning as represented by the focus on actors’ translations. The underlying assumption of this work is that negative translations among actors, as social meanings assigned to the eID, will act as a plausible cause for the institutional resistance to it to emerge. This emergent perspective also accounts for the different variations (Markus & Robey, 1988) found in translations among actors as affected by a similar artefact (see Chapter 7 and 8), since every translation is unique and related to its originating social setting. A logical structure, in theory, refers to the relationship between identified antecedents and outcome (Markus & Robey, 1988). The outcomes of
actors’ translations are far from deterministic, but rather the result of the relation formed between actors’ translations and the process of institutionalizing these translations into resistance. Hence, this is an example of a clear process theory as non-deterministic but still depending on specific antecedents (Markus & Robey, 1988). The level of analysis applied in this approach aims at synthesizing a perspective on individuals with a perspective of organizational or institutional resistance. This in turn corresponding to a combination of a micro and macro level of analysis described by Markus and Robey (1988) as mixed level analysis. Based on this typology, the analytical perspective described in this chapter can be characterized as a mixed level analysis of the emergent perspective focused on the process of actors’ translations as related to institutional resistance. Based on this motivation, I argue that the institutional and sociological perspectives described next fully align with the underlying assumptions of this work previously described as constructionist and hermeneutic (see Section 2.2).

4.2 The institutional perspective

4.2.1 Institutionalism

Institutionalism puts forth the importance of not only considering rational actions of managers and different kinds of experts in organizations but also to consider the irrationalities and embedded cultural systems, the institutions, of the organizational context (Avgerou, 2000). Institutionalism is, therefore, a perspective where the organizational environment is emphasized as a force actively influencing actions as well as decisions in organizations (Bowring, 2000). This is done through “[S]hared rules and typifications that identify categories of social actors and their appropriate activities or relationships” (Barley & Tolbert, 1997, p. 96). This perspective is also increasingly adapted in organizational studies since the 1970s (e.g. DiMaggio & Powell, 1983; Meyer & Rowan, 1977; Scott, 2014; Tolbert, 1985). To distinguish this perspective from traditional institutional approaches, it is often referred to as new institutionalism (Avgerou, 2000).

Accordingly, this is the result of a view of organizations based on sociology as opposed to the traditional views on organizing, focusing on financial aspects and formal structures (Meyer & Rowan, 1977). The increased interest in this perspective is a consequence of limitations in the efficiency of efforts based on traditional business perspectives on decision making and management as well as the treatment of variations in the organizational context as rational adaptations to surrounding conditions (Barley & Tolbert, 1997). In addition, the following description is also put forth: “[O]rganizations, and the individuals who populate them, are suspended in a web of values, norms, rules, beliefs, and taken-for-granted assumptions that are at least partially of their own making.” (Barley & Tolbert, 1997, p. 93). Hence, this puts forth the importance of applying a sociological perspective on organizations as implied by institutionalism. As described, institutionalism acknowledges social aspects such as norms, values and beliefs as affect-
ing the dynamics of organizations hence organizational legitimacy becomes an important factor (Suchman, 1995). The importance of legitimacy in social life can be traced back to Weber and actions guided by beliefs of a legitimate order (Scott, 2014). Suchman (1995) argues that the core focus of this intellectual transformation towards institutionalism should be on organizational legitimacy as a way of addressing these forces that “constrain, construct, and empower organizational actors.” (Suchman, 1995, p. 571). In this context, legitimacy is described as: “[A] generalized perception or assumption that the actions of an actor are desirable, proper, or appropriate within some socially constructed system of norms, values, beliefs, and definitions.” (Suchman, 1995, p. 574). Moreover, legitimacy in an organizational setting is also described as organizations seeking congruence between social values implied by activities and norms and values and acceptable behaviour in larger social systems (Dowling & Pfeffer, 1975). Therefore, I argue that legitimacy can be seen as the positive result of actions assessed by actors via common social systems of norms and values.

There are two central concepts in introduced by institutional perspectives; the institution and institutionalization. The term institution is a central concept of sociological studies used for describing socially established collective behaviours (Hughes, 1936). Institutions can, therefore, be described as social structures that guide as well as restrict behaviour in different social arrangements such as organizations (Scott, 2014). However, there are also two different approaches to institutions applied in institutional studies described as ‘environment as institution’ and ‘organization as institution’. Hence, the former refers to the reproduction of sector-wide social facts on the organizational level while the latter applies the perspective on the institution as the creation of meaning on an organizational level (Zucker, 1987). Environment as institution focuses on external coercive pressures (see isomorphism and institutional pressures below) put on organizations in a specific sector with a notion of this conformity related to positive estimated benefits referred to as myths (Meyer & Rowan, 1977). Hence, these institutional myths will result in benefits such as organizational stability, legitimacy and enhanced survival (Meyer & Rowan, 1977).

Organization as institution implies that institutional factors and elements emerge from the organization itself or from the imitation of other organizations (see also isomorphism below). Thus, these institutional elements such as values and norms are maintained over a considerable amount of time and usually remain unproblematicized (Zucker, 1987). The concept of institutionalization also has a clear relation to the philosophical assumption of constructionism (see Section 2.2.1): “Institutionalization occurs whenever there is a reciprocal typification of habitualized actions by types of actors. Put differently, any such typification (exemplification) is an institution.” (Berger & Luckmann, 1967, p. 54). This describes institutionalization as the state when typical social constructions become mutually inherent to existing habits as exemplified by non-reflected and inherent shared
norms and values as affecting actors as well as actions in an organization. Thus, institutionalization can be seen as a process as well as a property thus referring to the transfer of institutional norms and values socially defined to be real (the process) and the part of reality that is taken for granted (the property) (Zucker, 1977). Linking together these two concepts results in perceiving human behaviour as controlled by the institutions’ “predefined patterns of conduct” (Berger & Luckmann, 1967, p. 55). With an emphasis put on control as an inherent part of the institutionalization, these mechanisms can, therefore, be seen as systems of social control (Berger & Luckmann, 1967).

Institutionalized actions can therefore also be seen as being objective as well as exterior. Objective in a sense that these are usually repeated by other actors with a maintained common understanding and exterior when the understanding of the action is reconstructed as an intersubjective understanding and a part of the external world (Zucker, 1977). In my readings of institutional theory, there seems to be a shortage of studies focusing on how institutions change over time. This is also acknowledged by Scott (2014) referring to this perspective as institutional persistence. However, Zucker (1977) presents a more nuanced view of the process of institutionalization by defining three stages of institutional persistence as transmission, maintenance and resistance. Hence, transmission refers to the transfer of institutional norms and values among actors; maintenance covers the process of values and norms maintained as fact within the social system, and resistance denotes how well the institutional facts withstand pressures from external actors (Zucker, 1977).

Regarding how modern organizations act and develop, organizations are structured in the same line of business, and there are pressures and forces that make them become increasingly alike. This type of organizational homogenization is often described by the concept or isomorphism (DiMaggio & Powell, 1983). Thus, isomorphism refers to the restricting process forcing an organization to resemble other organizations facing similar external conditions. Two general types of isomorphism are identified, the competitive and the institutional, where the former predominantly exists in organizational fields of open and free competition and the latter is suggested to take into consideration other aspects such as institutional legitimacy and political power hence referring to a conformity with wide institutions (DiMaggio & Powell, 1983). Regarding criticisms of institutionalism, the field of organization studies has criticised this perspective for paying less attention to the actual processes of institutionalization (e.g. Barley & Tolbert, 1997; Tolbert & Zucker, 1996). This partly motivated by Zucker (1977)’s argument that institutionalization is to be considered as a process as well as a variable thus black-boxing the forming of institutions to a great extent and settling definitions of institutionalization such as “The institutionalization process simply defines social reality and will be transmitted and maintained as fact” (Zucker, 1977, p. 730). This evident lack, in turn, creating a need for more nuanced views of the phenomenon such as the effects of variations in institutionalization (Tolbert & Zucker, 1996) as well as their creation, alteration and
reproduction (Barley & Tolbert, 1997). These calls also apply to this dissertation applying a clear process perspective on institutional resistance in order to develop an improved understanding.

4.2.2 Scandinavian institutionalism

In Scandinavia, institutionalism starts to develop during the 1980s and is at this time influenced by the perspective of new-institutionalism in the United States. Hence, the Scandinavian perspective shares the common basis with the influence of scholars such as DiMaggio and Powell. The Scandinavian view of institutionalism related to organizing is one that puts equal emphasis on change as well as stability. Scholars in Scandinavia also argues that the focus on isomorphism can be seen as a consequence of a distance between the researcher and the organization under focus since an increased distance seems to result in an increasing tendency of perceiving institutional change as a product of isomorphic behaviour (Eriksson-Zetterquist, 2009). I argue that the present work is in line with this Scandinavian institutionalist approach since it clearly acknowledges proposed perspectives such as isomorphism (DiMaggio & Powell, 1983) and strategic responses to institutional pressures (e.g. Oliver, 1991). However, instead of focusing on how these institutional challenges can be managed on the surface to minimize negative consequences, this dissertation aims at more closely relating the new institutional perspective to sociology to potentially develop an increased understanding of how these factors emerge in the social contexts of actors and organizations. A clear sign of this focus is also the described delimitation from a traditional management perspective on organizational change as related to ICT (see Section 1.5.1).

4.2.3 Institutional pressures

As described, this work focuses on public sector eID introductions. Hence, these environmental, institutional pressures exerted by government aiming at conformity of eIDs in the public sector as a whole (eGov case) or in specific areas such as the health care sector (eHealth case) become central to this dissertation. To be able to describe and categorize institutional forces or pressures applied to organizations, two existing theoretical perspectives become relevant; the previously described concept of isomorphism (DiMaggio & Powell, 1983) and the three pillars of institutions as suggested by (Scott, 2014). Accordingly, three types of isomorphism are presented with coercive referring to the result of political influences and pressures, mimetic as related to reactions to uncertainty and normative associated with professionalism (DiMaggio & Powell, 1983). There are also different levels of volunteerism and reflected behaviour related this typology. In the case of coercive isomorphism, the organization is left with little or no choice but to comply and adapt. For example, rather strong pressures can be put on public sector organizations to comply and adjust by government especially in the case of laws and regulations. Further, institutional imitation can also be perceived as related to uncertainty thus relating to mimetic isomorphism (DiMaggio & Powell, 1983). Mimicking other organizations facing similar challenges may, therefore, be a rather effective
way of handling such uncertainties. In an ICT context, this can be exemplified by followers imitating the behaviour of first adopters of specific information systems merely based on the belief that this act will solve current problems without any further reflection on underlying incentives and motives. Finally, normative isomorphism is primarily related to professionalism in different areas. It is the collective efforts of a specific occupation of professional domain hence this type of isomorphism occur when a similar base of professionals act in the same way across organizational domains in response to forces put upon them (DiMaggio & Powell, 1983). Hence, a typical example being the response to new online threats and risks causing professionals working with ICT and cybersecurity to act upon these threats in a similar way in order to minimize potential risks and damage on organizational legitimacy and trust. In a similar way, Scott (2014) refers to these pressures as ‘the tree pillars of institutions’ thus emphasizing the aspects of specific differentiating underlying notions behind these pressures. The **regulative pillar** is related to legal and regulative aspects of institutions with the aim of regulating and constraining organizational behaviour (Scott, 2014) thus applying the mechanism of control described as coercive isomorphism (DiMaggio & Powell, 1983).

In addition, assessing the conformity to pressures, as well as a mandate to decide on sanctions, are included in the regulative processes governing these pressures (Scott, 2014). The regulative pillar is therefore associated with environmental pressures aimed at conformance at the level of organizational institutions. The **normative pillar** emphasizes normative rules and values hence introduces an obligatory, prescriptive and evaluative dimension (Scott, 2014). These governing norms and values are in turn associated with social systems for ensuring and maintaining legitimacy. Hence, norms specify how things should be done while values are related to the desirable including standards for assessment and comparison (Scott, 2014). These pressures are associated with normative and evaluative aspects of environmental pressures as social prescribing and legitimizing institutions in turn similar to the described concept of normative isomorphism (DiMaggio & Powell, 1983) as related to existing code of conduct in specific professional areas. The third pillar is defined as the **cultural-cognitive pillar**, hence emphasizes on the cultural-cognitive aspects of institutions thus in turn acknowledging the importance of shared meanings and perceptions of social reality (Scott, 2014). Thus, DiMaggio & Powell as well as Scott’s approach defines and categorizes these pressures as based on inherent underlying aspects can, therefore, be seen as exemplifications or specific applications of the perspectives perceiving the environment as an institution (e.g. Meyer & Rowan, 1977).

Since this work is also an effort to increase the understanding of how organizations act the way they do in response to these forces of eID conformity hence, is not related to any formal structures of organizations and management. As a first step in developing the socio-institutional framework bringing together sociological and institutional perspective, there is a need for a theoretical point of departure regarding organizations’
responses to institutional pressures. This is motivated by the focus on institutional resistance in turn perceived as an equally institutionalized force opposing the pressure to introduce eIDs. How organizations apply different strategies in response to institutional pressures, therefore, becomes important. In addition, several scholars also put forth potential predictors in efforts to potentially predict the outcome of institutional pressures (e.g. DiMaggio & Powell, 1983; Oliver, 1991). Thus, Oliver (1991) presents a suitable framework and typologies focusing on categorization and evaluation of pressures in order to predict outcomes. Therefore, I argue that this framework, covering different important aspects of pressures such as categories, predictive dimensions, strategic responses and tactics, aligns well with the aim as well as the applied process perspective in this dissertation. Hence, this framework provides a clear and structured approach for describing, identify, categorize and relate institutional pressures to responses and potential outcomes. In this framework, institutional pressures are categorized by focusing on their specific underlying institutional factors and predictive dimensions (Oliver, 1991). Five different factors are identified each related to a set of predictive dimensions. Estimated on a scale ranging from low to high, these dimensions are in turn used as a basis for predicting the outcome (Oliver, 1991). Accordingly, this motivates Oliver’s framework to be presented more in detail with institutional factors described next.

**Cause**
The cause relates to the underlying objectives or intentions regarding the institutional pressure exerted. The organization’s potential acquiescence (consent) will be in relation to the level of agreement with these objectives and intentions. The consensus prescribed by institutional theory is also related to the potential dissensus between existing expectations on organizational and institutional levels. Therefore, a low level of social legitimacy gained from conformity with the pressure is linked to a high probability of organizational resistance. Regarding efficiency or economic gain, low anticipated levels from conformance with the pressure will also most likely result in significant resistance (Oliver, 1991). However, there are areas where increased efficiency in strictly financial terms may turn out to be problematic. For example, in health care where cost efficiency can have a negative impact on the quality of medical services provided.

**Constituents**
The constituents of institutional pressures include actors such as the general public, state and professions, in turn, using pressures to impose expectations, regulations and laws upon organizations (Oliver, 1991). Since these constituents, in turn, have different and even contradictory demands and institutional definitions (Scott, 1987), exerted pressures can be far from coherent (Oliver, 1991). For instance, if there are different interest groups behind pressures in turn related to different expectations (Whetten, 1978) which result in a high level of multiplicity inherent to the pressure. Hence, a higher level of multiplicity of constituent expectations is related to a higher level of potential organizational resistance. Regarding the dimension of dependence, DiMaggio and Powell (1983)
suggest there is a clear relation between a high level of dependence and potential conformity with isomorphic pressures hence dependence is a factor facilitating organizations to become increasingly alike. When organizations are not dependent on the constituents exerting the pressure, resistance will more likely occur (Oliver, 1991). Thus, in this work, this can be related to public sector actors as dependent or independent of central government bodies.

**Content**
The institutional factor of content is closely related to the organizational goals since organizations tend to have a higher rate of conforming to pressures if these, in turn, are in line with the organizations’ internal goals (Oliver, 1991). There have been several examples of failing institutional pressures due to inherent inconsistencies with internal organizational goals (e.g. Covaleski & Dirsmith, 1988). Organizations may also show a lower willingness to conform to pressures if these have a lack of consistency related to their content (Oliver, 1991). Positive effects of conforming to institutional pressures taken aside, the act of compliance always introduces a form of constraint that tends to result in some kind of loss of freedom of action and autonomy (Pfeffer & Salancik, 2003). Hence, there is a potentially high level of resistance to pressures if consistency related to institutional requirements, norms and goals are low. Furthermore, if the imposed level of constraints put upon the organization is high, this will also result in a high level of resistance (Oliver, 1991). Accordingly, inconsistent and constraining pressures in turn clearly diverging from an organization’s perspective will potentially face a high level of potential resistance.

**Control**
Institutional control aims at describing the way pressures are imposed upon the organization and is related to the processes of coercion to legal aspects and diffusion of a voluntary nature as means of how the pressures are imposed (Oliver, 1991). Some distinct kinds of pressures leave little or no freedom of choice at all when for example law or government mandates force organizations to comply (DiMaggio & Powell, 1983). As a contrast, there are also pressures that rely on a voluntary diffusion and studies show that this voluntary diffusion is closely related to the level of institutionalization gained by this pressure (Tolbert & Zucker, 1983). Hence, voluntary pressures that over time become institutionalized have a higher rate of success. If legal coercion of the institutional requirements and norms behind the pressure are low, there is a potential of a high resistance to the pressure. Further, if voluntariness and diffusion of norms, values and practices are low, this poses a significant risk of pressure meeting a high resistance (Oliver, 1991). This implies a clear relation between legal coercion and voluntary diffusion of norms and values. Hence, to succeed this institutional factor of control thus becomes dependent on an equally high level of legal coercion as well as voluntary diffusion which I argue in turn can become a contradiction when the legitimacy of the pressure does not converge with the social legitimacy of the organization.
Context

The environmental context of the exerted pressure is related to the dimensions of uncertainty and interconnectedness (Oliver, 1991). Pfeffer and Salancik describe uncertainty as “[T]he degree to which future states of the world can not be anticipated and accurately predicted.” (Pfeffer & Salancik, 2003, p. 67). Since organizations tend to strive towards certainty and stability – a high level of uncertainty will most likely work in favour of the pressure (Pfeffer & Salancik, 2003). This also being in line with DiMaggio and Powell (1983) relating the tendency of organizations imitating or mimicking each other to the uncertainty of the external context as described above. Thereby, a low level of uncertainty in the organizational environment will potentially result in organizational resistance (Oliver, 1991). Next, interconnectedness refers to links formed between organizations in different forms described by “the existence of transactions tying organizations to one another” (DiMaggio & Powell, 1983, p. 148). These transactions can take on various shapes of forms for example via different forms of communication and collaboration. Interconnectedness becomes important since it facilitates the diffusion of existing institutional norms and values among participating organizations (Oliver, 1991). Thus, a low level of interconnectedness in the institutional context will in turn results in a higher possibility of organizational resistance to pressures (Oliver, 1991). Hence, organizations acting independently in times of uncertainty will most likely adhere to pressures more than highly interconnected organizations operating in a stable and predictable organizational environment.

Table 11. Institutional factors and predictive dimensions (based on Oliver, 1991, p. 160)

<table>
<thead>
<tr>
<th>Institutional factor</th>
<th>Related to</th>
<th>Predictive dimension</th>
<th>Potential resistance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cause</td>
<td>Objectives and incentives of pressure</td>
<td>Legitimacy</td>
<td>Low</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Efficiency</td>
<td>Low</td>
</tr>
<tr>
<td>Constituents</td>
<td>The actors exerting pressure</td>
<td>Multiplicity</td>
<td>High</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Dependence</td>
<td>Low</td>
</tr>
<tr>
<td>Content</td>
<td>Norms as requirements of pressure</td>
<td>Consistency</td>
<td>Low</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Constraints</td>
<td>High</td>
</tr>
<tr>
<td>Control</td>
<td>Means of exertion of pressure</td>
<td>Coercion</td>
<td>Low</td>
</tr>
</tbody>
</table>
The institutional factors and predictive dimensions described above is summarized in Table 11. This ‘typology of institutional factors and predictive dimensions’ is the first of two typologies presented by Oliver (1991) applied in this work and later integrated into the socio-institutional framework. This is motivated by the provided structure and guidance as well as clarity when characterizing different aspects of an institutional pressure (factors) as well as potentially assessing the outcome (predictive dimensions) as related to these factors. In Table 11, a column of potential resistance is added to serve as an indicator of levels of factors facing potential resistance according to Oliver (1991).

### 4.2.4 Strategic responses

As a way of characterizing how organizations respond to institutional pressures, Oliver (1991) presents a ‘typology of strategic responses’ with responses characterized as acquiescence, compromise, avoid, defy and manipulate. Each of these responses is in turn associated with three related tactics (Oliver, 1991). This enables identification and characterization of the different strategies and tactics that the organization can enact in order to negotiate and act upon the pressure exerted. Therefore, I argue that this provides a suitable typology for identification and characterization of responses to pressures as well as applied tactics in order to negotiate them. Hence, this is the second of two typologies provided by Oliver (1991) applied in this work and later integrated into the socio-institutional framework. A summary of these responses and tactics are presented in Table 12 below followed by a description of each response.
Table 12. Strategic responses (based on Oliver, 1991, p. 152)

<table>
<thead>
<tr>
<th>Response</th>
<th>Tactic</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Acquiesce</td>
<td>Habit</td>
<td>Following invisible, taken-for-granted norms</td>
</tr>
<tr>
<td></td>
<td>Imitate</td>
<td>Mimicking institutional models</td>
</tr>
<tr>
<td></td>
<td>Comply</td>
<td>Obeying rules and accepting norms</td>
</tr>
<tr>
<td>Compromise</td>
<td>Balance</td>
<td>Balancing the expectations of multiple constituents</td>
</tr>
<tr>
<td></td>
<td>Pacify</td>
<td>Placating and accommodating institutional elements</td>
</tr>
<tr>
<td></td>
<td>Bargain</td>
<td>Negotiating with institutional stakeholders</td>
</tr>
<tr>
<td>Avoidance</td>
<td>Conceal</td>
<td>Disguising nonconformity</td>
</tr>
<tr>
<td></td>
<td>Buffer</td>
<td>Loosening institutional attachments</td>
</tr>
<tr>
<td></td>
<td>Escape</td>
<td>Changing goals, activities, or domains</td>
</tr>
<tr>
<td>Defiance</td>
<td>Dismiss</td>
<td>Ignoring explicit norms and values</td>
</tr>
<tr>
<td></td>
<td>Challenge</td>
<td>Contesting rules and requirements</td>
</tr>
<tr>
<td></td>
<td>Attack</td>
<td>Assaulting the sources of institutional pressure</td>
</tr>
<tr>
<td>Manipulation</td>
<td>Co-opt</td>
<td>Importing influential constituents</td>
</tr>
<tr>
<td></td>
<td>Influence</td>
<td>Shaping values and criteria</td>
</tr>
<tr>
<td></td>
<td>Control</td>
<td>Dominating institutional constituents and processes</td>
</tr>
</tbody>
</table>

**Acquiescence**

Acquiescence or consent can take the forms of habit, imitation or compliance. Habit is described as “blind adherence to preconscious or taken-for-granted rules or values” (Oliver, 1991, p. 152), and imitation is consistent with the described concept of isomorphism here applied in the form of a conscious or unconscious mimicking of existing institutional models. Further, compliance refers to the conscious obedience to institutional requirements, values or norms (Oliver, 1991).
Analytical perspective

Compromise
Organizations may also consider the strategy of compromise as a way of handling conflicts or inconsistencies in response to pressures and the strategy of balance is a tactic to accommodate multiple demands in response to institutional pressures. Further, to pacify means to partially conform to one or several of the actors’ expectations while bargaining takes a more active form when meeting only some of the expectations or demands (Oliver, 1991).

Avoidance
Avoidance is described as to prevent the need for conformity by concealing nonconformity thus avoiding the pressure or escape from expectations and rules. Concealment means that nonconformity is disguised by acquiescence and buffering is when the external evaluation is prevented or minimized. The most dramatic tactic being the escape described as when the organization completely leaves the domain where the pressure originated (Oliver, 1991).

Defiance
Defiance being an active form of resistance to the institutional pressure where dismissal means totally ignoring rules and values of the institution while challenge means to contest or challenge the norms and rules of the institution involved in the pressure and attack means to departure from expectations and pressures in a rather aggressive way (Oliver, 1991).

Manipulation
Finally, manipulation, is considered to be a more active response than the ones described above since the intention is to change or exercise power over the actors involved in exercising the pressure or their expectations; a strategy that can take the form of co-opting the source of the pressure, to influence beliefs and values of the institution or try to control the actors that exercise the pressure by dominance and power (Oliver, 1991).

Therefore, I argue that Oliver’s framework provides a structured way to approach the concept of institutional pressures. It enables the identification and characterization of environmental pressures and an organization’s reaction to it in the form of strategic responses. In addition, the concept of predictive dimensions enables a theoretically grounded estimate of the potential outcome of such pressures. This provides opportunities to further investigate the relationship between institutional pressures as antecedents and predictive dimensions as potential outcomes. In addition, a set of tactics is presented to handle the potential resistance to pressures hence each applied tactic becomes linked to the anticipated outcome. However, being a part of this theoretically grounded framework, the suggested predictive dimensions suggested by (Oliver, 1991) needs to be examined based on empirical data. Thus, I argue that if this framework is applied to em-
empirical data, it provides a relevant approach to assess and analyse the process of institutional pressures as related to conformance or resistance with a potential high applicability regarding pressures as related to different aspects of ICT.

4.2.5 Institutional effects

As described, there are two streams of institutional theory categorizing pressures exerted on organizations, isomorphism (DiMaggio & Powell, 1983) and institutional pillars Scott (2014). In line with described arguments of Oliver (1991), organizations apply different kinds of strategies to handle these pressures with one central aim if creating or maintaining organizational legitimacy (Suchman, 1995). Maintaining this legitimacy can also be perceived as an active strategy to potentially minimize the negative consequences of institutional pressures. These two perspectives of isomorphism and institutional pillars are merged together in the form of a conceptual framework of institutional effects by Mignerat and Rivard (2009) illustrated in Figure 10.

![Figure 10. Framework of institutional effects (adapted from Mignerat & Rivard, 2009, p. 370)](image)

This framework also integrates the perspective of Jennings and Greenwood (2003). Since this framework is a result of a clearly integrative and process focused perspective applied to institutional pressures, effects and responses also including several of the described central institutional perspectives in this work, it is considered as an appropriate basis source of influence on the later development of the socio-institutional framework. Thus, regulative coercive pressures explain how coercion or tests of strength versus sanctions affect the behaviour of actors; normative pressures address social obligations of actors through values and norms, and cultural-cognitive and mimetic pressures relate to the mimetic behaviour of organizations in times of uncertainty. Hence these institutional pressures can be exerted upon organizations as well as sub-organizations and/or
individuals or groups (Mignerat & Rivard, 2009). As organizations are subject to these pressures, strategic responses are launched with the aim of addressing these pressures as categorized by the typology of strategic responses (Oliver, 1991). The aim of these strategies is creating or maintaining organizational legitimacy (Suchman, 1995) or more specifically manage its legitimacy in times of institutional pressures (Mignerat & Rivard, 2009). Hence, I argue that this conceptual framework provides a very clear illustration of the central concept of institutional pressures as well as the relation to strategic responses at the organizational level in order to address these pressures. In addition, this framework clearly shows that pressures can be exerted on individual organizations and groups or individuals within as well as on groups or organizations. This also corresponds with the approach applied in this dissertation where analysis of institutional pressures is performed at multiple organizational levels.

4.2.6 Institutional agents and carriers

In an agent based view of the construction of institutions, there are several types of different institutional agents or casual agents. First, the institutional agent of the government or nation-state, as focused in this work, have been described as “[B]ureaucratically organized administrative structure empowered to govern a geographically delimited territory.” (Scott, 2014, p. 119). Bureaucratization is based on the term bureaucracy with Max Weber often described as the founder of the perspective on organizations as attributed to aspects such as the division of labour, extensive rules and hierarchy of authority (Hall, 1963). This process can be seen as an act of homogenization that emerges as the result of the structuring of fields of organization (DiMaggio & Powell, 1983). Bureaucracies can also be described as a result of the introduction and emergence of centralized states and economic markets (Meyer & Rowan, 1977). While all organizations can be viewed as structures of governance, the state or government are clearly distinctive since the government, in fact, exercises authority over organizations (Scott, 2014).

In addition to its structure, the government agent also has privileges and special powers. Second, in economies of capitalism, corporations and other business organizations possess a great power to use economic resources for organization and mobilization. They have authority over the personnel and form networks with their allies. At the organizational level, they control the allocation of resources and at the industry level, they act as competitors or in cooperation with others. Third, in modern society, the professionals have come to play an increasingly important part, and Scott particularly emphasizes their role as constructors of new institutional frameworks where they make use of different combinations of elements such as ideas and knowledge. Different professionals take part in the forming of different kinds of frameworks such as normative and regulatory ones (Scott, 2014). Further, institutions can also be seen as transferred or conveyed by several types of institutional carriers (Jepperson, 1991) such as symbolic and relational systems, activities and artefacts (Scott, 2014). These institutional carriers, therefore, become aspects to consider in order to understand how institutions develop.
and change over time and these carriers also varies depending upon the institutional context. However, these carriers also affect ‘the nature of the message and the way in which it is received’ so they can not be seen as neutral vehicles of transmission (Scott, 2014). Institutional carriers are described as related to the three pillars (regulative, normative and cultural-cognitive) described above.

The symbolic systems are exemplified by rules and laws (regulative), values, expectations and standards (normative) and categories and typifications (cultural-cognitive) (Scott, 2014). Hence, artefacts complying with specifications are seen as related to the regulative pillar, artefacts meeting standards and conventions to the normative and finally artefacts possessing some symbolic values as related to the cultural-cognitive pillar (Scott, 2014). Further, artefacts and ideas will transfer through time and space and in the meantime be modified, transformed and translated which in turn can be the reason behind ideas materializing in organizational contexts at a given time and occurring unintended consequences. Thus, a translation model can be applied to be able to understand why the same text, as a carrier, at any given time can be given a different meaning or translation (Czarniawska & Joerges, 1996). If institutional agents are considered, one should also consider how these are translated across time and space. Accordingly, I argue that the public sector eIDs featured in this dissertation can be seen as examples of such institutional carriers. Thus, the applied perspective of actors’ translations is in line with the described notion of these carriers as subjects to translations.

4.2.7 Institutional actors

The need of broadening the institutional focus by including on actors’ behaviours is clearly put forth in existing research. For example, assessing strategies in institutional analysis, Schneiberg and Clemens (2006) state that “The behaviour of actors—whether individuals or other social actors—is attributed not to the characteristics or motives of that actor, but to its context or to higher-order factors.” (Schneiberg & Clemens, 2006, p. 195). Hence, this posits that individuals’ actions are based on cultural systems of a shared nature (Schneiberg & Clemens, 2006). By applying this perspective of sociologically constructed institutional actors, this approach interprets the actions of actors as shaped by institutional factors (DiMaggio, 1988; cited in Schneiberg & Clemens, 2006). This concept of institutional actors is fully in line with the suggested relationship of actors’ translations as influenced by and in turn influencing institutional resistance. However, since the focus of the approaches described above is on world polity and national policy, there is a clear underlying notion of institutional factors as influencing actors’ behaviours whereas, in this dissertation, this relationship is described as mutual suggesting that actors’ translations are influencing as well as are influenced by institutional resistance. Moreover, this institutional perspective also introduces clear challenges for researchers. Challenges that in turn are related to the ability to link different levels of analysis, for example, to identify and link explanatory factors on lower organizational levels to factors on a higher level of analysis. So, this makes quite a contrast to other perspectives in institutionalism such as political science and economics that does
not acknowledge aspects such as cognition and culture (Schneiberg & Clemens, 2006). Since this dissertation aims at linking together different levels in analysis, I argue that these challenges put forth must be acknowledged as well as handled.

4.2.8 Institutionalism in ISR and eID research

Turning to ISR, a great number of studies are adopting the managerial view of maximizing efficiency and effectiveness of ICT efforts and apply preferably technical and rational perspectives (Nicolaou, 1999). However, other scholars (e.g. Orlikowski & Barley, 2001; Teo et al., 2003) have instead turned to the institutional view which considers other aspects of the organization than the pure rational structures and actions (Mignerat & Rivard, 2009). On an epistemological level, Orlikowski and Barley (2001) argue that ISR can benefit from institutional analysis. Hence, the institutional context is needed to fully understand the implications of IS in an organizational setting. Further, related to ICT and an example of moving from the organizational domain to a more user centred approach, Lamb and Kling (2003) presents the concept of the social actor and describe it as an institutional approach focused on actors whose everyday actions are infused with ICT use. This perspective is also motivated by their argument that the use of ICT is only a limited part of a typical user’s working day hence there is a need to put the focus on a broader social actor based context (Lamb & Kling, 2003).

Kubicek (2010) applies actor centred institutionalism, institutional actor theory applied for policy field analysis (Scharpf, 2000), in combination with path analysis to investigate national eID management systems (eIDMS) in selected European countries. With a perspective acknowledging complex socio-technical systems, institutional actors are perceived as stakeholders faced with available technical options as well as taking organizational and regulatory in consideration negotiated while also influenced by norms and legal environment. Thus, this perspective provides a model where contexts and conditions, such as technology, culture and legal system, affects an interaction system of actors with varying resources, strategies and interests and results in an outcome of a technical system such as eIDMSs. In recent years, the study of the described relationship between institutional pressures and strategic responses toward conformity (Oliver, 1991), has been focused on several ISR studies (e.g. Ang & Cummings, 1997; Hsu et al., 2012; Liu et al., 2010; Moe, 2004; Vial & Rivard, 2012). The interest in this approach can be motivated by several factors. For instance, research shows that organizations formulate strategic responses of different kinds as a result of internal as well as external pressures of legitimacy (Ang & Cummings, 1997) and inconsistencies between expectations and objectives as well as conflicting institutional demands are common contradictions within organizations (Moe, 2004). In relation to ICT efforts, the adaption of institutional approaches within the IS field could also be seen as a consequence of endowing the artefact with an institutional character (Kling & Iacono, 1989). Based on these later developments in ISR, I argue that this dissertation aligns with a growing consensus in ISR putting forth that institutions are important to consider when studying social and organizational implications of ICT.
4.3 The sociological perspective

4.3.1 Actor-Network Theory

A sociological perspective is suggested to facilitate the investigation of actors’ translations of the eID (see Section 1.1.4). The selected approach called ‘the sociology of translation’ (Callon, 1986) described below, introduces an actor-centred approach where actors are focused on their own perspectives and placed in a relational network while facing obstacles when negotiating towards a common goal. Although this approach does not explicitly refer to the concept of actor-networks, Callon states in a note “To describe the network of constraints and resources that results from a series of operations of translation I have proposed the concept of the actor-network” (Callon, 1986, p. 27). I, therefore, interpret this as ‘the sociology of translation’ being a framework developed during early explorations that later developed into Actor-Network (ANT) (e.g. Latour, 1991; Law, 1999; Law & Callon, 1988). The selected approach of translation analysis applied in this dissertation is described as not being an ANT-approach per se, but nevertheless clearly related to it hence sharing underlying assumptions and perspectives. This clear relation between (Callon, 1986) and ANT is also implied by several scholars (e.g. Singleton & Michael, 1993; Tatnall & Gildning, 1999).

Therefore, I argue that the following more detailed description of the perspective provided by ANT still being relevant to be able to understand its underlying incentives and perspectives. The origin of the actor-network can be traced back to ‘acteur réseau’ in French that means actor network (Law, 1999). ANT is developed by the French sociologists Bruno Latour, Michel Callon and visitors such as John Law. According to Latour (1993), the world is full of hybrid entities consisting of both human and nonhuman elements which in turn is a fundamental point of departure for ANT. Hence, this theory is developed in order to analyse situations where the separation of these elements are proven to be difficult (Callon, 1999). Further, Tatnall and Gildning (1999) describe that what seems to be social can be partly technical and what seems to be technical can also be partly social. Accordingly, this complex relationship becomes the focus of ANT which applies a perspective here unilateral social or technical relations are denied instead offering a perspective of heterogeneity to include social as well as technical entities. With this perspective of heterogeneous entities (Bijker et al., 1987) questions regarding the social or technical origin are avoided thus ANT proposes a socio-technical perspective since social as well as technical determinism are considered to be flawed (Law & Callon, 1988). Bruno Latour describes this as “Contrary to the claims of those who want to hold either the state of technology or that of society constant, it is possible to consider a path of innovation in which all the actors coevolve.” (Latour, 1991, p. 117). ANT, has been widely applied in a variety of areas such as studies of the Luddite movement (Grint & Woolgar, 1997), car parking systems (Vidgen & McMaster, 1996), the achievements of Louis Pasteur (Latour, 1988), scientists laboratory research (Latour, 1987), the Kodak camera (Latour, 1991) and a public transportation system in Paris.
(Latour, 1996). Thus, ANT focuses on networks of both human and non-human actors and the mechanics of power through the construction and maintenance of these networks (Tatnall & Gildning, 1999); tracing the transformation of these heterogeneous networks (Law, 1991) made up of people, organisations, agents, machines and other objects (Tatnall & Gildning, 1999). A distinct aspect of ANT is its dislike of obvious tautological answers to problems (Tatnall & Gildning, 1999) like “the thing doesn’t work because it couldn’t have worked” (Latour, 1996, p. 121). Instead, ANT investigates the actors themselves with no a priori assumptions about the matter under investigation by studying the negotiations and trade-offs performed by these actors (Tatnall & Gildning, 1999). According to Law (1987), neither social nor technical aspects of elements in these heterogeneous networks should be handled in particular according to their explanatory status.

4.3.2 ANT in ISR

What differentiates the ISR field from other fields like computer science or organization studies is that ISR has the possibility to emphasize the interaction between the social and technical systems (e.g. Hanseth et al., 2004; Lee, 2001). As described, the application of social theory in ISR is widespread (see Section 3.3.3) where for instance approaches like sociomateriality further develops and strengthens a relational perspective on the social and material (e.g. Orlikowski, 2007; Orlikowski & Scott, 2008). Further, there seems to be a well-established notion of ANT in ISR since it is described as an inspiration to sociomateriality (Orlikowski & Scott, 2008) as well as described as an appropriate approach for addressing the relationship between the social and the material (Hanseth et al., 2004). Thus, ANT provides a unique and powerful set of tools to overcome shortcomings in understanding the IT artefact (Hanseth et al., 2004). There is a general consensus regarding the difficulties of separation between human and non-human elements (Callon, 1999). One clear example of this strong relation applies to ICT and the question of which part of software is an inanimate object and which part is the result of human interactions (Tatnall & Gildning, 1999); a difficulty in separation also acknowledged by other scholars (e.g. Cusumano & Selby, 1997; Sahay, 1997). Therefore, ANT addresses some of the previously described central areas of debate in the ISR field such as how to address the relationship between the social and the technical (e.g. Orlikowski & Iacono, 2001; Orlikowski & Scott, 2008). In ISR, ANT has been applied by several scholars (e.g. Bengtsson & Agerfalk, 2011; Faraj et al., 2004; Hanseth & Monteiro, 1997; Marres, 2004; Walsham & Sahay, 1999; Yoo et al., 2005). For example, Hanseth and Monteiro (1997) use ANT to conceptualise information infrastructures and describe standards as means used to form and stabilize actor-networks in order to address socio-technical obstacles concerning the relation between standards and behaviour of use. Further, Faraj et al. (2004) investigates how web-browsers are shaped by their environment and concludes that development of technology must be studied from a broad perspective taking interests, translations and technical as well as social arrangements into consideration. Empirical as well as academic tests (see Section 2.7.4) indicate
that ANT has a potential as an analytical perspective when studying complex relationships between a technological artefact and its surrounding social and organizational context. Therefore, I argue that previous applications of ANT in ISR research strengthens the choice of this approach for providing the sociological perspective on public sector eIDs.

4.3.3 Challenges and opportunities

However, ANT is over time subject to an extensive critique and is even contested by its founders. For example, John Law argues that the tension between the actor and the network, or in other words between structure and agency, is lost in ANT since the field evolves over time. This mainly being due to the tendency of handling ANT too easily in its application as well as in its criticisms. Law describes that ANT should be seen as a ‘semiotics of materiality’ in that the ‘relationality of entities’ is produced in relations and applied to all materials, not just linguistic ones (Law, 1999). In addressing the obstacles concerning ANT, Bruno Latour states: “[T]here are four things that do not work with actor-network theory; the word actor, the word network, the word theory and the hyphen! Four nails in the coffin.” (Latour, 1999, p. 15) and thus contests all four basic concepts of the theory. First, the use of the term network is described as unfortunate based on the later development of technology such as the Internet. Hence, its initial meaning is to capture a series of transformations and translations rather than to mean ‘transport without deformation’.

Second, actor in its hyphenation with network becomes too similar to existing social theory focused on agency and structure. Hence, the actor is not used here to take on the role of neither agency nor network to illustrate society since these, in fact, are only two faces of the same phenomenon. Third, ANT is never intended to be a theory of the behaviour of social actors but rather a way to understand actors and to: “[L]earn from them not only what they do, but how and why they do it.” (Latour, 1999, p. 19). Fourth, the hyphen between the words actor and the network is described as unfortunate partly based on the debate between agency and structure but also related to ANT simultaneously trying to deal with human and non-human agencies. This, in fact, placing it somewhere in between modern ways of thinking regarding nature, psychology, politics and theology thus the scope of ANT turns out to be much larger than first anticipated (Latour, 1999).

Critics have also objected to ANT’s claim that humans and technologies are the same in essence, but Hanseth et al. (2004) finds this critique to be unfounded since ANT assumes everything to be actor-networks.

The evolution of new technology involves a number of various actors each with an own set of interests, background, motivations and prejudices hence actors seeking to create coalitions must shape their own strengths with an aim of alignment of their own interests and interpretations with others (Monteiro, 2000). Regarding critique put forth against ANT, Walsham (1997) argues that it is important as an IS researcher to be aware of the existing criticisms and describes the following four areas of concern: limited analysis of
social structures, little attention to broader social structures (Harbers, 1995), an amoral stance, no attention to moral or political bias (Star, 1991), the problem of generalized symmetry, treating both humans and nonhumans as actants (actors) (Pels, 1995) and problems of descriptions, the attention to detailed results in extremely rich descriptions (Walsham, 1997). During this work, I am fully aware of this critique and argue that I actively address all four described areas. Broader social structures in the form of institutions are indeed added to the analytical perspective and synthesised with the sociological perspective, moral or political biases as associated to actors’ translations are revealed, any problems regarding generalized symmetry are handled as far as possible, and I have actively tried to keep descriptions related to the following translation analysis as condensed and clear as possible without loosing in detail and nuances.

As described, scholars such as Lee (2001) advocates for a need to emphasize the interaction between social and technological systems in ISR (see Section 3.1.1), and ANT can be seen as a unique and powerful tool to overcome these shortcomings in understanding the ICT artefact (Hanseth et al., 2004). Applying this approach is also an answer to Orlikowski and Iacono (2001’s)’s call for theorizing the IT-artefact to increase the theoretical understanding of the object of study. To be able to accommodate the analysis of these aspects in research, ANT seems powerful with its integration of technological, political and institutional factors (Hanseth et al., 2004) and it has also historically been proven effective when analysing innovation and diffusion of complex technology systems (Hughes, 1987). I am therefore confident that the opportunities of applying an approach related to ANT will provide the anticipated opportunities as long as it is applied in a highly reflective manner and any challenges along the way are handled with a positive outcome.

4.3.4 The sociology of translation

As described, the described approach of translation analysis applied in this study is inspired by Callon (1986), and the study of the scallops and fishermen. In St Brieuc Bay of France, a group of scientists try to form an alliance among affected actors with the aim of a potential domestication of scallops since these populations are threatened as a result of overfishing in the early 1970s. Thus, an analytical framework called ‘the sociology of translation’ is introduced with the aim to study of power relationships and the roles of science and technology in such relationships. Thus translation analysis refers to my interpretation and application of the framework of ‘sociology of translation’. Although, not clearly defined as a term by Callon (1986) but used to describe the general process taking place at each of the described steps, I interpret ‘translation’ in this context as closely linked to the concept of letting a single actor in the described network act as a spokesperson representing a larger group of actors or network. Hence, the perspective of this population gets translated and integrated into the network by the spokesperson.

29 While (Callon, 1986) uses entity and actor interchangeably throughout his study, to avoid any confusion, I have chosen a more strict approach only referring to actor(s).
Further, Callon argues that previous studies done by sociologists have not succeeded in allowing the studied actors to describe their perspectives in an open manner. Therefore, actors are not attributed correctly since there is a lack of aspects such as reason, truth or efficiency. Hence, the success of actors is described without any further investigation of the inherent reasons behind the success. Instead of denying the possibility of defining science and technology, Callon argues that there is indeed a possibility of analysing society as ‘uncertain and disputable’ (Callon, 1986). Although this way of letting an assigned actor ‘speak on behalf of others’ can also be seen as a potential source of bias, Callon tries to address this by applying the three principles described next.

In order to avoid inherent problems in studies of technological controversies such as neglecting social structures, identity and the importance of actors, the following three methodological principles are presented: agnosticism, where the observer acknowledges the actors’ own perspective and social environment, generalized symmetry, where possibly conflicting arguments and perspectives are explained in the same terms which also include social as well as technical aspects and finally free association, which imposes the observer to follow the actors when they act or describe their world treating social and natural elements in the same way (Callon, 1986). By interpreting and adapting this framework from Callon, my aim is to reveal how translations influence the course as well as the outcome (actual or anticipated) of the introduction of eIDs in the public sector. On a general level, my aim is to analyse, reveal and evaluate the power of translations in the two covered cases. This analytical approach also provides the opportunity to have a human as well as non-human actors playing on the same analytical arena without taking any sides hence with an explicit lack of any assumptions of what is to be considered right or wrong a priori. This is in turn made possible by Callon’s three methodological principles. Callon’s framework includes four so called moments of translation, problematization, interessement, enrolment and mobilization (Callon, 1986). However, in my own adaptation of the framework, I will refer to these moments of translation as stages to emphasize the analysis’ sequential style of progression. Further, I choose to extend the first stage with the additional interdefinition of actors and Obligatory Passage Points, previously integrated in the problematization. This is motivated by an increase in clarity and transparency by explicating these in the process. Further, a final stage of closure is added to the framework. Previously only touched upon only briefly by Callon, I argue that this is an important final stage to conclude the analysis. Accordingly, my interpretation and adaptations of this framework consist of seven stages as indicated by the numbering in the following sections also summarized in Table 13.
**Problematization, interdefinition of actors and OPPs**

The translation analysis starts off with (1) problematization where the overall problem or obstacle of the analysis is described from the main actors’ point of view followed by an (2) interdefinition of actors in the network where a synthesized view of how these actors are affected by the questions formulated by the main actor. The next step of the process is to define the (3) Obligatory Passage Points (OPPs) that must be negotiated and passed in order for the suggested programme of actions aimed at the domestication or scallops to succeed. Thus, a successful outcome becomes dependent on defined actors’ interest and ability to admit to the overall programme of actions as formulated by the main actor; a relationship that Callon refers to as the forming of a ‘Holy Alliance’. An example of the OPP from Callon’s study is illustrated in Figure 11.

![Figure 11. Obligatory Passage Point (based on Callon, 1986, p. 20)](image)

This illustration makes it clear that all actors in the network, the main actor (the three researchers) as well as the pecten maximus (the scallop), the fishermen and the scientific colleagues are all dependent on a successful passage of the OPP, the scallop’s ability or willingness to attach or anchor itself to the devices (collectors) placed in the sea to serve as a shelter against predators as they grow. Hence, this critical OPP must be passed with success in order to achieve the overall aim of domestication of these crustaceans. However, in line with the described guiding principle of agnosticism, problematization must further define the goals as well as obstacles for each participating actors since they all have different incentives and are facing different challenges in the network; the three researchers can not just assume that all actors will follow. Figure 12 illustrates this further problematization as performed by Callon showing the inherent alliances between the actors shaping their identity as well as their own paths in the network as based on obstacles and goals which in turn must be handled with a positive outcome to ensure each actors’ involvement in the network. For example, if the fishermen are deprived of their short term profit whey will most likely opt out of the network thus with a potentially negative effect on the overall goal to repopulate the bay. Further, the network itself is
totally dependent on pecten maximus’ ability of reproduction; without the scallops, the network as defined will inevitably fail.

Interessement
The aim of the next step, interessement (4), is to “[I]mpose and stabilize the identity of the other actors it defines through its problematization” (Callon, 1986, p. 8). This is a process of keeping the interest of the other defined actors by the construction of what Callon calls devices to keep other actors from influencing them otherwise, hence to try to weaken the links to other external influences by strengthening the link to the network. During the interessement, the main actor tries to overrule any risks, doubts or suspicions leaving the actors with no option but to participate the network or alliance. The interessement device, therefore, represents the attempts made by the main actor to minimize the negative aspects of elements that could possibly affect the ability of the network to successfully navigate the OPP in order to reach success. The interessement, as illustrated by Callon, is shown in Figure 13 where actor A tries to cut or weaken the link between

Figure 12. Problematization (adapted from Callon, 1986, p. 20)\textsuperscript{30}

\textsuperscript{30} When adapting this figure from Callon (1986), I choose to rename the labels of ‘Entities’ and ‘Goals of entities’ to ‘Actors’ and ‘Goals of actors’ since I will mainly use the term actors throughout the forthcoming analysis to avoid any further confusion.
the actor B and the group of other influences\textsuperscript{31} (C, D and E) outside the network. Hence, the properties and identity (Callon, 1986) of B are affected in a consolidating and refining way by B’s association with A and as Callon points out; the mechanisms and strategies to accomplish these kinds of interruptions or de-associations are quite unlimited. Further, Callon describes this as relationship as The triangle of interessement (Callon, 1986). Hence, the anticipated effects of the interessement device are shown by the arched arrow moving away from external influences.

\textbf{Enrolment}

However, there is no deterministic link between interessement and the forming of alliances in line with the proposed programme or network as defined by the main actor. The participating actors must still be enrolled and kept within the network to enable the possibility of a successful outcome. This is the aim of the next step of enrolment (5), as defined by actions, negotiations and roles accompanying interessement and potentially enabling it to succeed. Thus, the actors who accept them are attributed with a “set of interrelated roles” (Callon, 1986, p. 10). Callon further denotes that this step is also made up of “multilateral negotiations, trials of strength and tricks that accompany the interessements and enable them to succeed” (Callon, 1986, p. 10). However, there is also the question of representation. In previously described steps, from problematization to enrolment, there are only a few actors acting as representatives of a greater mass of anonymous or silent actors. This can be seen as a consequence in situations when a small number of individuals act as representatives and speak in the name of others. Moreover, some actors might not even speak at all, in a literal sense, since they are non-human and therefore rely on others to be their spokesmen. A clear example being the scallops with the main actor (the three researchers) acting as spokespersons (Callon, 1986). The enrolment focuses on the outcome of interessement, strategies launched by the main actor as well as active negotiations to keep the participating actors aligned within the network.

\textsuperscript{31} Callon (1986) refers to C, D, E as other entities with an interest to link themselves to B. However, I choose to refer to C, D, E as (external) influences. This to avoid any confusion with actors participating in the network.
Mobilization

Callon has chosen to call the next step *mobilization* (6) due to the fact that the aim is to try to render actors mobile. I interpret this as mobilization focusing on the represented groups of actors potentially actively aligning themselves to the network as a result of interressement. Thus, mobilization also indicates if the assigned spokespersons really are representative of their groups of silent actors. Further, according to Callon, the mobilization also becomes a physical reality through the materialization of displacements\(^3\), referring to his colleague John Law for a definition of this phenomenon who describes displacements as emissaries of three different classes, documents, devices and drilled people, and their role in long-distance social control (Law, 1986). Hence, the chosen populations as represented by the actors in the network are mobilized or displaced into another context as representatives to take part in the negotiations. Further, this is the part of the translation process when the successful enrolment (hopefully) turns into active support among populations as represented by actors in the network.

Closure

A potential last step of the sociology of translation is only briefly touched upon by Callon and referred to as ‘closure of controversies’. Despite the fact that Callon seems to perceive this as related to the conclusion of the study, summarized as dissidence, rather than an explicit step or moment of translation of the framework, I choose to integrate closure (7) as a separate and final stage in the translation process. Moreover, I interpret the term of ‘dissidence’ as clearly depending on the outcome of that particular study; hence I argue that a more general name would be suitable. According to Callon “[C]losure occurs when the spokesmen are deemed to be beyond question” (Callon, 1986, p. 16) hence I interpret this as the stage of a controversy and negotiations when a displacement, e.g. argument or action, that in its essence delivers an undisputable and non-negotiable message that puts an end to the controversy. This exemplified by putting the final nail in the coffin of a controversy or providing the final leap of success of negotiations. Thus, the closure can also be the effect of the consequences of actions or non-actions of the actors in the network. Examples from Callon’s study are the scallops that did not act as the researchers anticipated, hence anchor themselves at the designated places for a safer regrowth, or the group of fishermen who horded the scallops from the protected area. Thus, this particular study ended in a catastrophe regarding scallops’ regrowth and these moments of translation eventually failed (Callon, 1986). However, one should bear in mind that in some translation processes, the closure can become a reality first after a considerable period of time since some controversies tend to live on over long periods of time.

---

\(^3\) Since Callon (1986) does not clearly explain displacement, I have chosen to rely on the linguistic definition of acts of spoken language or other artefacts of communication to eliminate communicational time-space gaps.
Table 13. Summary of steps in translation analysis (adapted from Callon, 1986)

<table>
<thead>
<tr>
<th>Step</th>
<th>Name</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Problematization</td>
<td>Definition of problem from the main actor’s perspective.</td>
</tr>
<tr>
<td>2</td>
<td>Interdefinition (of actors)</td>
<td>Synthesized view of concerned actors within the network.</td>
</tr>
<tr>
<td>3</td>
<td>Obligatory Passage Points</td>
<td>Critical points that must be negotiated and accepted by actors in order for the network to succeed.</td>
</tr>
<tr>
<td>4</td>
<td>Interessement</td>
<td>Strengthening actors’ links to the network and the possible weakening of links to actors outside the network.</td>
</tr>
<tr>
<td>5</td>
<td>Enrolment</td>
<td>Activities that accompany the interessement in order for it to succeed.</td>
</tr>
<tr>
<td>6</td>
<td>Mobilization</td>
<td>Activities performed by actors within the network that comply with its overall goal.</td>
</tr>
<tr>
<td>7</td>
<td>Closure</td>
<td>When an undisputable and non-negotiable displacement puts an end to the negotiations or controversies within the network.</td>
</tr>
</tbody>
</table>

Due to the somewhat disappointing outcome of the study on the domestication of scallops, where the network fails due to the acts of a group of fishermen and the scallops’ inability to attach, one wonders what happened to the population of scallops. Well, as it turns out there has actually been a rebuilding strategy for the scallops in St Brieuc Bay going on from the 1970’s to 2009, and after a quick glance at this OECD report, it seems that the population is slowly recuperating (OECD, 2012). So, rest assured, the closure is not due to the total extinction of the scallops in this specific area; they persisted and continued to live on although far from happily ever after ending since they probably will continue to end up on our dinner plates.
4.4 The socio-institutional framework

4.4.1 Background and motivation

The overall aim of the following sections is to describe and introduce the integration and synthesis of the suggested institutional and sociological perspectives applied in this dissertation. Hence this approach fully embraces the notion of ICT as infused in the social context of the user (e.g. Lamb & Kling, 2003) and institutions as important factors affecting decisions and actions in organizations (Bowring, 2000). Hence, as described these institutions can also be seen as mutually dependent ensembles (Orlikowski & Scott, 2008) since the focus is on the interplay and relationships between institutions (see Section 3.3.2). Further, it acknowledges and addresses the intertwined relationship between the social and technical, an area in ISR clearly influenced by sociology. This approach is also in line with the call for broadening the institutional focus (e.g. Barley & Tolbert, 1997) as well as my own described call for a broader focus on public sector eIDs.

The described strategy is to apply a sociological perspective focused on actors’ translations to be able to investigate and understand how these actors act and interact as related to the artefact (the eID). Thus, actors’ perspectives including aspects such as beliefs, translations, and actions are seen as influencing as well as being influenced by introductions of eIDs in the public sector. This sociological perspective will, therefore, provide the described sociomaterial view (e.g. Orlikowski, 2007; Orlikowski & Scott, 2008) of this work since there are no clear boundaries between the social and the technical. Instead, the focus is put on the relationships between these human and non-human as equal actors participating in this network. In addition, the perspective provided by ANT has been previously published hence has already been assessed and discussed in a research context with a positive outcome (Söderström & Melin, 2012a).

As described, the approach I suggest to achieve this is to develop an analytic framework integrating the described institutional perspectives as put forth by scholars as Oliver (1991) and Mignerat and Rivard (2009) integrated with the sociological perspective of translation analysis based on the sociology of translation (Callon, 1986). This is the applied strategy for developing an increased understanding of how resistance to institutional pressures is formed, reformed and possibly handled to minimize negative effects of eIDs introductions in a public sector context. So, in an effort to characterize this analytical perspective, I will in the following refer to it as equally centred on the sociological perspective on affected actors as on the institutional context of resistance related to the artefact (the eID). Therefore I argue that synthesising these two perspectives into a socio-institutional framework adds a new dimension to the sociological as well as the institutional perspective. This approach comes with several challenges, and I argue the most evident one being the described linking of different levels of analysis (Schneiberg

126
Analytical perspective

& Clemens, 2006). Hence, when the synthesis of the sociological and institutional perspective, will require special attention in order to facilitate a positive result from this framework rather than just proving the possibility of synthesis. Since this is my first effort of trying two integrate these two perspectives into an integrated whole, the socio-institutional framework presented should at its current state be considered as tentative or work in progress.

4.4.2 The institutional perspective

First, since I argue that the concept of resistance in the context of this analytical perspective has an underlying notion of manageability, I see a growing need to formulate a new concept to be able to acknowledge the risk and possibility of this resistance developing into an unmanageable and non-negotiable state. I will in the following refer to this resistance as institutional barriers as indicated by the title of this dissertation. Further motivating this decision is the fact that the concept of barriers has already been used in institutional ICT studies with the purpose of categorizing this kind of strong resistance (e.g. Janssen et al., 2012). Thus, institutional barriers will henceforth be the concept applied in this work to relate to these institutional forces actively opposing institutional pressures. This approach will address potential existing gaps in research regarding how institutional pressures develops and in turn influence the development of institutional barriers.

It is clear that these are created on the institutional level affected by as well as affecting shared norms and values – but on what grounds are they formed and how? As described, compared to studies focusing on the manageability of institutional pressures, there seems to be a shortage of research putting institutional barriers or resistance in the foreground. However, I argue that the reasons behind institutional barriers, formed against institutional pressures, are very important to investigate to be able to facilitate an increased understanding of the implications of pressures as well as barriers. Therefore, I argue that instead of estimating the effects of responses to pressures there is a clear potential for an increased understanding of the causes of barriers and resistance to facilitate more well-informed and empirically grounded decisions. Thus, the suggested approach of institutional analysis aims at moving towards a more proactive and well-informed perspective on pressures as well as barriers in contrast to existing reactive approaches.

The existing institutional perspective to be integrated in the framework will be institutional pressures and strategic responses (Oliver, 1991). In addition, this framework will include relevantly described typologies such isomorphism (e.g. DiMaggio & Powell, 1983), three pillars of institutions (Scott, 2014), linking institutions to actors’ actions (Barley & Tolbert, 1997) and to some extent managing legitimacy (Suchman, 1995). Further, the central stages in the framework will draw inspiration from the previously described framework of institutional effects (Mignerat & Rivard, 2009) (Figure 10 above). Although the described perspectives on institutional pressures clearly are related
Analytical perspective

to external environmental pressures with the aim of conformity applied on organizations, I argue that these pressures can also arise and be exerted within the organization itself (e.g. Combs et al., 2009; Zucker, 1987). Thus, if applicable, as exemplified by the eHealth case, the external pressure gets transferred and institutionalized into an internal institutional pressure of conformance.

These institutional pressures should not be seen as only related to the external ones striving for an increased isomorphism in a specific field of organizing (e.g. DiMaggio & Powell, 1983) but also to pressures aiming at conformance and/or homogenization of a specific area or application within organizations. This will also facilitate the use of similar theoretical concepts and categories for external as well as internal pressures which in turn will provide opportunities for identifying similarities and recurring patterns across the institutional and organizational level of analysis. In addition, I argue that in an institutional sense barriers can be seen as the antagonists of pressures since they focus on counteracting their respective incentives and effects. Thus, similar to external and internal pressures, the similar analytical perspectives can potentially be applied on pressures as well as barriers which in turn potentially will facilitate interesting insights. Thus, I argue that this approach of reusing already existing analytical perspectives on emerging concepts such as barriers is well in line with this dissertation’s aim of building on and further developing existing research and theory rather than reinventing already existing research (see Section 2.2.3).

4.4.3 The sociological perspective

Even though the current study differs in several aspects from the original study performed by Callon (1986), I still argue that my interpretation of this approach brings significant benefits when integrating this framework into the analytical approach of this dissertation. As described, ‘the sociology of translation’ (translation analysis) provides the opportunity to investigate the individual actors involved in the processes on their own terms as participants in a network. Hence, insights on how and why the affected actors actively resist these eID introductions are provided. Since there are some clear differences between this study and Callon’s original study, this results in some informed choices during its application. First, Callon has the three researchers as the main actors in his study assigned with an aim and mission considered as rather clear and indisputable; put shortly their mission is to restock the bay. However, this dissertation, although clearly focused on the introduction of public sector eIDs, the contexts in which these introductions take place are of a much more complex organizational character which in turn brings challenges as well as opportunities. The challenges are for example related to ensuring analytical clarity and transparency when focusing on quite complex intra- and inter-organizational contexts. Nevertheless, I argue that the opportunities outweigh the challenges by far since this approach brings the opportunity to identify and describe aspects that influence the eID introductions in a clear way but are seemed elusive and hard to handle from the main actors’ perspectives. Second, the original study by Callon is based on secondary data such as written records from the 1970s while the current
study is mainly based upon a rich set of primary qualitative empirical data. Hence, the challenge here is how to adapt Callon’s framework to a multi-source multi-level empirical context with rich sets of different kinds of first hand qualitative data in some cases collected over a period of several years such as in the eGov eID case. The first stages of translation analysis, problematization through interessement, pose no problems since these are based on the main actor’s perspective hence this analysis is based on the perspective as put forth by the main actor in each case.

However, the question then is when primary empirical data from other affected actors’ perspectives, as participants of the network, should be introduced in the analysis. Thus, I choose to integrate this data from the stage of enrolment and onwards. This is motivated by the stage of enrolment being focused on the enrolment of these actors, how the main actor succeeds in keeping the within the network and aligned with its common goals. The negotiations and actions that relate to the enrolment are based on what actually happened among the actors in the network when the main actor tried to introduce the eID. Not being able to cover the entire introduction process in this type of very detailed analysis, a selection of important events are used as key points to be further investigated in this way. Therefore, I argue that the potential benefits of this analytical approach are clear. It will provide a way to entangle the quite messy relationships between the technical and social contexts during negotiations and controversies among actors featured in the cases focusing one common goal; the introduction of eIDs. Being a structured approach, it also enables comparison between the eGov and the eHealth case and further analysis to facilitate positive insights and contributions. The aim of my adaptation of translation analysis is to acknowledge actors’ translations and based on the prescribed notions of agnosticism, generalized symmetry and free association (Callon, 1986) achieve an impartial analysis of how affected actors have translated the eID. Since this approach also puts an actor in the leading role as the main actor coordinating the introduction of the eID, one should also get a good notion of the kind of obstacles and opportunities this particular actor faces during the introduction process.

4.4.4 The synthesized framework

Having described and motivated the institutional as well as the sociological perspective, the time has now come to bring them together into the suggested socio-institutional framework. Using Mignerat and Rivard (2009)’s framework as a starting point, the following four stages of analysis have been identified: (1) pressure, (2) barrier, (3) negotiation and (4) institutionalization. Accordingly, this provides the process view of institutional pressures as exerted from institutions (1) causing resistance in organizations in turn developing into barriers (2). These barriers become subjects of different kinds of negotiations (3) and the outcome will affect barriers as well as pressures by the process of institutionalization (4). Since these stages take place in a sociological as well as institutional context, each stage is influenced by institutions and actors’ translations in the following stage as well as influencing institutions and translations in the following stage.
as illustrated by the arrows. Hence, this also denotes that the interplay between these stages is an ongoing process. This four stage institutional model is illustrated in Figure 14.

Figure 14. The four stage institutional model

This results in the forth stage being formulated as institutionalization thus referring to the process of barriers developing into a shared social consensus across organizational contexts. This also in turn enabling institutional barriers to influence the continued exertion of institutional pressures. Hence, I argue that barriers also become antecedents to continued pressures, since these pressures tend to change over time. The purpose of this model is to provide a general overview of the four basic concepts or stages to be covered in the upcoming analysis applying the socio-institutional framework (see Chapter 9).

Moreover, if compared to the original process model provided by the framework by Mignerat and Rivard (2009), strategic responses as means of management to gain organizational legitimacy are instead translated into strategic responses enacted during negotiations of barriers. As described, legitimacy is generally seen as an important central incentive behind the concept of institutional pressures, and although touched upon in the upcoming final analysis and discussion, legitimacy will not be put in the foreground as a central incentive of this process. Hence, legitimacy as a sought after the outcome of strategic responses in the original framework is left out in this analysis. This instead implies a view of legitimacy as an underlying incentive of pressures as well as barriers and even a positive side-effect of a positive outcome of all four stages taken together. Thus legitimacy in the context of this work can be described as related to conforming to an institutional pressure not related to any significant barriers. Therefore, I argue that this is the state that occurs when institutional pressures and institutional barriers converge as based on affected actors’ translations and the pressure can be institutionalized across the organizational setting in a positive sense. In an effort to illustrate how these four stages apply to Mignerat and Rivard (2009)’s original framework of institutional effects, this the original framework is updated with the integration of the four stages as illustrated in Figure 15.
I argue that this illustration provides a clear overview of the process of the four stages to be focused in the upcoming analysis in Chapter 9. In addition to Stage 1: Pressure, this model adds the Stage 2: Barrier as an institution influencing the focused inter- or intra-organizational level from a different direction. Further, in Stage 3: Negotiation, the arrows are reversed to illustrate that these strategies aim at negotiating the barrier rather than just being strategies launched to in order to ensure the success of the pressure. Further, the institution of pressure, as well as the institution of the barrier, have been assigned with bi-directional arrows to illustrate that these institutions do not only influence the organizational context, the organizational context inevitably influences these institutions. Thus, Stage 4: Institution is added between the organizational and institutional level since I argue that any institutionalization starts at this level and then emanates or transfers to the institutional level when shared norms, values and actions become socially accepted and shared as ‘taken for granted’. Hence, the addition of bar-
barrier as an institution is fully in line with the suggested approach and aim of this dissertation as well as the described approach of potentially addressing pressures and barriers as equals regarding the applied analytic approach. Hence, the pressure, as well as the barrier, is assigned with a similar set of pillars which in turn will provide an opportunity for interesting upcoming analyses.

4.5 Concluding remarks

As described, the aim of this study is to investigate institutional resistance or barriers related to the introduction of public sector eIDs and how these barriers, in turn, can be identified, analysed and possibly handled in a more informed way. This can, of course, be interpreted as this approach being assigned with the aim of facilitating more effective proactive management of such institutional barriers, but I argue that the focus applied in this work is significantly different. Hence the emphasis here is not put on management but rather on an increased understanding of the causes and origins of institutional barriers in order to develop more informed and context aware approaches to public sector eID introductions in the future. Further, the analytical perspective presented in this chapter rests on the notion of institutions as social structures guiding as well as restricting actions and behaviours; a perspective, in turn, being a result of the described increasing interest of sociology in institutionalism. This institutional view is linked to the sociological perspective with the described frameworks focused on actors, networks and translations. Since both perspectives are based on assumptions of social constructionism and acknowledging the importance of relationships between social entities or actors, they are fully converging with the described underlying assumptions of this work, in turn, facilitating a potential positive synergy described as the socio-institutional framework. Hence, I argue that this approach provides the opportunity to better investigate and understand this reported resistance or barriers against public sector eIDs. Accordingly, this socio-institutional framework described as tentative will be addressed in detail in Chapter 9 in the light of the empirical evidence presented in Chapter 5 to 8 and facilitate a final analysis and discussion.
Part III – Empirical evidence and analysis

The third part presents empirical evidence from the two cases focusing on public sector eID introductions. The eGov case is covered in Chapter 5 followed by the eHealth case in Chapter 6. These chapters include an initial analysis that provides important input to the sociological perspective applied during translation analysis performed on each case and presented in Chapter 7 and 8.
5. The eGov eID

This chapter presents the eGov case focusing on a public sector eID introduction in Sweden. The first two sections cover the emergence of the current Market eID and the introduction of the new eGov eID with a special focus on opportunities, challenges and important events. Three different perspectives of the eGov eID as represented by the Government, the Service Provider (SP) and the Identity Provider (IdP), will follow and the chapter ends with a comparison between the identified challenges of the eGov eID introduction and its outcome. This provides the empirical findings and initial analysis of the challenges and controversies leading up to the resistance to the eGov eID that will be further analysed in Chapter 7 and synthesized with the institutional perspective in Chapter 9. This chapter addresses the first and second research question, clearly describing the resistance to the eGov eID and how this resistance affects the introduction (RQ-1) and linking this resistance to different actors’ perspectives (RQ-2).

5.1 The public sector eID

Since this chapter presents the emergence and current state of the public sector eID area in Sweden, some 15 years of government efforts and development is covered. Since my aim is to provide as accurate picture as possible, the presented level of detail in the following sections is therefore rather high and covers a large number of and events. Therefore, I argue that to be able to develop a better understanding of the current challenges of the eGov eID (the whole), this accurate picture of the emergence leading up to these challenges is needed (the parts). In addition, a result of my studies of this field is also the identification of a shortage of a comprehensive overview of the eID development in the public sector in Sweden. Hence, apart from providing the empirical base for the eGov case, this chapter also serves the purpose of providing such an overview.

5.1.1 At the outset

This chapter presents the emergence and problematic state of the eGov eID and further investigates the suggested relation between challenges and government applying a too narrow technical and regulatory focus during its introduction. The risk of placing non-technical aspects such as social and organizational in the background, therefore, becomes imminent. Thus, the applied focus becomes potentially problematic as exemplified by the lack of acceptance and active resistance to the eGov eID (see Section 1.1.3). Moreover, the eGov eID has become subject to an extensive critique which in turn suggests a clear gap between the introduction with its aims and purposes on the one hand, and on the other hand, the affected actors in the public and private sector. The current
eID solution henceforth referred to as the Market eID, is a successful convergence between the private and public sector. Private sector Identity Providers (IdPs) have for a considerable time supplied the public sector authorities as Service Providers (SPs) with eID services authentication in digital services (e-services) aimed at citizens and businesses. Thus, this has become a significant part of ongoing efforts to increase efficiency as well as availability in the public sector’s delivery of services, eGovernment (see Section 3.2.2). Hence, the Market eID model is a successful convergence between the public and private sector but still related to several shortcomings such as lack of central coordination and based on proprietary eIDs. Moreover, BankID is the dominating eID in the Market eID solution today, provided by a number of commercial banks, and used in private as well as public digital services.

This is the result of the market convergence initiated in the early 2000’s when the government decided to benefit from the diffusion and use of private market solutions. The BankID is well established and so far unthreatened on the Swedish eID market with an estimated uptake of over 8 million users and an estimated transaction volume of 2 billion in 2015. However, the private use of BankID still covers 92% of the total transaction volume (BankID, 2016b). Furthermore, several authorities such as the Tax Agency (Skatteverket, SKV) reports a continued very strong development of the use of BankID as the preferred way of authentication and signing in their digital services whereas the use of other eIDs steadily decreases. With a growing mobile digital service market, the Mobile BankID turns out to be very successful and the fastest growing authentication method in recent years (SKV, 2015c). The aim of the eGov eID is therefore to replace a successful solution developed over more than a decade. Accordingly, to be able to understand the current challenges in the public sector eID area in general and the resistance to the eGov eID, in particular, we must first investigate and understand the emergence of the Market eID in the public sector, the decisions and events resulting in the eGov eID as well as its introduction.

5.1.2 The emergence

One important prerequisite for the eID in a Swedish context is the history of using personal numbers or coordination numbers as the unique identification number for individuals in public as well as in regulated areas of the private sector such as the banking sector. This in contrast to many other countries using different identifiers for different

---

33 This name is chosen because this eID solution is based on a supply of eID services as provided by IdPs on the private market.

34 With the exception of the Board (sv. E-legitimationsnämnden, recurring references to authorities will be done in the form of first providing the English translated name followed by the Swedish name and abbreviation. Thereafter, only the Swedish abbreviation is used.

35 The coordination number assigned to individuals temporarily residing in the country.

public sector contexts as for instance health insurance numbers in health care. Implemented in 1947 as the first system in the world covering an entire population, the Population Registration Act (1946:469; 1967:198; 1991:481) regulates the assignment of these identifiers. After centralizing this function at the beginning of the 1990s, the identifiers are issued and assigned by SKV which also administers the national registration database (SKV, 2015a). All residents in Sweden receive a unique identifier as provided by the public sector at birth (SKV, 2015b). Thereby, Sweden already has an established system and infrastructure for this kind of identification system as implemented in authorities’ back office systems and assigned to physical identification documents; an ability described as very critical in relation to eID solutions (EC, 2011). Hence, transferring this identifier into a digital context is not a very far step. The emergence of the Market eID is often described as directly related to the first signed agreements between public authorities\(^{37}\) and private sector service providers at the end of the 1990s regarding eIDs for authentication of employees (PTS, 2004).

At the beginning of the 2000s, the government starts to investigate how to realize the aim of being fully accessible to citizens and businesses 24-7 via online content and an increased level of interactivity (Statskontoret, 2000). This increased availability of public sector services also results in increased handling of sensitive information that in turn creates a need for securely identified and authenticated citizens. In 2000, the government assigned the National Tax Agency (Riksskatteverket\(^{38}\), RSV) to investigate how to meet this need of eID services, i.e. identity certificates and electronic signatures, in the public sector. Conducted as a joint effort, this project is called Society’s Electronic Services (Samhällets Elektroniska Tjänster, SAMSET\(^{39}\)) (RSV, 2003c). SAMSET describes that most major authorities are planning for increased online communication, and in line with its commission to consider already existing solutions on the private market, recognizes the banking sector as a potential provider of eID services to the public sector. Also motivated by this sector already at this point having approximately 2 million identified customers in electronic banking service (eBanking) with a significant part being potential users of public sector digital services. As a result, a mutual interest is created, and commercial banks propose a shared eID model where banks act as IdPs and supplies the SPs with eID users and eID services to be integrated into public sector digital services (RSV 2000:15). At this time, there are actors already issuing eIDs, such as the National Postal Service (Posten AB\(^{40}\)) and Telia AB\(^{41}\), a telecommunications company. However,

---

\(^{37}\) Since this chapter provides an overview, public sectors actors are referred to as authorities hence this term will refer to the larger agencies as well as smaller actors such as municipalities and county councils.

\(^{38}\) The Tax Agency (Skatteverket, SKV) from 2004.

\(^{39}\) The project was active between 1998 and 2007.

\(^{40}\) PostNord from 2009 as result of the merger between the Swedish Posten AB and Danish Post Danmark.

\(^{41}\) In 2003 merged with the Finnish telecommunications company Sonera and included in the group TeliaSonera AB, since 2016 Telia Company.
the banking sector has no actual eID solution that is suitable for use in public sector
digital services, but nevertheless the banks are willing to support this development mo-
tivated by potential synergies and offer the following authentication model illustrated in
Figure 16. Thus, (1) the banks provide the customer with a identity certificate (eID), (2)
the customer contacts government, i.e. the authority’s digital service, (3) the authority
requests a validation of the certificate against the bank and (4) the bank accepts or rejects
this request (RSV 2000:15) and in turn if successful authorizes the customer to access
the digital service.

Figure 16. Banking eID service model (adapted from RSV 2000:15)

The business model in this proposed solution is transaction based\(^{42}\) hence the cost is
based on the number of transactions or validations performed by the IdP upon request
from the SP. The estimated benefits of providing secure digital services in this way de-
scribed as cost efficient. However, being a cooperative model where the authority sign
agreements with only one bank, clearing arrangements between banks are needed to
enable the SP to gain access to the entire stock of identified customers of IdPs (RSV
2000:15). This clearing agreement, illustrated in Figure 17 (below), where the agree-
ment between the Authority and Bank A allows for access to identified customers of
both Bank A and Bank B. This setup would also eliminate the competition among join-
ing banks regarding the delivery of eID services as well as simplify the agreements au-
thorities and banks.

\(^{42}\) In practice often referred to as tick-based where the ‘tick’ corresponds to one transaction.
In the next step, the RSV coordinates the needed guidelines and procurement requirements (RSV, 2003a, 2003b) and in accordance with public sector procurement law, the Swedish Agency for Public Management (Statskontoret) at the end of 2001 signs framework agreements with several current and potential eID suppliers on the market. The government appoints Posten AB and Telia AB and the three major commercial banks Föreningssparbanken\textsuperscript{43}, Handelsbanken and Nordea as IdPs to provide eID services to the public sector (RSV, 2003a). This is the first agreements between the public and private sector to facilitate a joint supply of eID services resulting in a convergence model between these two sectors. This first agreement, eID-2001\textsuperscript{44}, is in turn based on guidelines and common standard regarding public sector eID services as investigated and proposed by SAMSET (e.g. RSV 2000:15; RSV, 2003a, 2003c). The motives for signing with actors in the private market are described as “Since most citizens do not have frequent contacts with authorities, they have no reason to get an eID solely for simplifying their government contacts.” (RSV, 2003a, p. 5). This offers citizens a high level of accessibility by being able to use the same eID in different service contexts independent of sector. The government decision to make use of existing eID solutions with already a significant diffusion (RSV, 2003a) also turns out to be a crucial decision since reaching positive diffusion and use have proven to be a significant challenge for public sector eID introductions (see Section 3.4.3). This strategy is, therefore, the result of government deciding not to reinvent the wheel, develop and invest in a state owned eID solution. Described as the market approach, it has since its inception been regarded as one of the success factors of the Swedish public sector eID model (see Section 3.4.3). This approach also makes it possible for authorities to adapt to the existing use of eID services.

\textsuperscript{43} Swedbank from 2006

\textsuperscript{44} Framework agreement for electronic identification (Ramavtal för elektronisk identifiering 2001, eID-2001) (Statskontoret 2001:32)
already existing in society (RSV, 2003b) thus providing a rapid integration when developing secure digital services.

5.1.3 The BankID

Two of the banks selected to sign the first framework agreement (eID-2001), together with several other banks soon start a collaboration regarding eID services (RSV, 2003b). This effort will facilitate the very important clearing agreement between banks described above (section 5.1.2) where the SP only has to sign with one member bank to be able to access the total stock of identified customers. In detail, a consortium of several commercial banks as members forms with the aim of developing a common infrastructure for eID authentication to be shared among banks and used in private as well as public digital services. As a result, the company Finansiell ID-Teknik BID AB is created 2002 to facilitate and lead this development as co-owned by member banks and focused solely on providing eIDs and related services to be issued or sold by the member banks (BankID, 2015). Thus, Finansiell ID-Teknik is the Certificate Authority (CA), and the member banks act as IdPs that issue eIDs to their customers.

Several member banks also provide eID services for authentication and signing to businesses as well as public sector authorities for integration in secure digital services. Being a deliberate strategy to let the banks act in the foreground while developing and maintaining the technology in the background, this offers the opportunity of consolidating the technology and expertise needed. Therefore, the BankID, as the current dominating instantiation of the Market eID, is the result of the public as well as the banking sector identifying a need for joint efforts in the eID area. While the banks show a clear interest in letting their customers use the eBanking eID in other service contexts such as the public sector, the government can benefit from its already significant diffusion, use and further technical developments such as mobile eID solutions. However, still requiring an established relation between the bank as IdP and the citizen as an identified bank customer and eID user.

5.1.4 The eID enabling eGovernment

With the supply of eID services in place, the public sector initiates the development of secure digital services with the Tax Agency (Skatteverket, SKV) and the Social Insurance Agency (Försäkringskassan, FK) being among the first to suborder from the eID-2001 framework agreement. SKV soon launches several secure digital services such as the tax declaration of VAT and payroll taxes for businesses as well as editing and signing.

---

45 Föreningssparbanken (later Swedbank) and Handelsbanken (RSV, 2003b)
46 A Certificate Authority of Certification Authority is an issuer of digital certificates e.g. to be used on eIDs.
47 Currently Danske Bank, ICA Banken, Ikano Bank, Handelsbanken, Lånsförsäkringsar Bank, Nordea, SEB, Skandiabanken, Sparbanken Syd, Swedbank, and Ålandsbanken (BankID, 2016a)
of the income tax return for citizens. FK presents digital services for parental benefits and the Patent, and Registration Office (Patent- och registreringsverket, PRV) opens up for online business registration. The following years, businesses, as well as citizens, are presented with the opportunity of accessing an increasing number of public secure digital services online with the same market provided eID solution (PTS, 2004). This development is described as: “Overall, this means that the ‘railway track’ for electronic identification and electronic signing has been established and the SAMSET-authorities will take the lead and ‘drive the train’ at an increasing speed.” (RSV, 2003b, p. 4). This solves the technical and regulatory challenges of the eID used in the public sector, in turn, facilitating a rapid development in line with current and following central recommendation and guidelines regarding eGovernment in general as well as digital services and eID services in particular.

Initially managed by the Swedish Agency for Public Management (Statskontoret) (e.g. Statskontoret 2002:13, 2002), this responsibility is thereafter transferred to the Board for Electronic Government (Nämnden för elektronisk förvaltning, E-Nämnden) (e.g. E-Nämnden 04:02, 2004; E-Nämnden 05:03, 2005). The following years several eGovernment initiatives launch in parallel such as the 24h-delegation (24-timmarsdelegationen). Active between 2003 and 2005, this delegation has the mission to focus on the added value of public sector digital services available to citizens and businesses as well as the increased efficiency of the public sector (Dir. 2003:81). The 24h-delegation presents several reports focusing on the development of digital services (e.g. SOU 2004:56; SOU 2005:119). The benefits of using a common coordinated public sector eID solution are also acknowledged, and the Market eID is described as offering a secure basis regarding the technical solution (24-timmarsdelegationen, 2005).

5.1.5 Renewed agreements and business model

When the eID-2001 agreement expires, a renewed procurement process results in the next version of the agreement (eID-2004) valid between 2004 and 2006 with a 24-month renewal option. By 2006 agreements are signed with five IdPs and the business model is further developed into a transaction based model associated with low fixed costs and SPs are also offered pre-packaged fixed priced options (Verva, 2006a). Hence, the SPs pay for the validation (sv. spärrkontroll) of the eID (Verva, 2008a) in turn resembling the model used for credit card validation (PTS, 2004). There is also an agreement called Infra-2003 valid between 2004 and 2008 with two assigned suppliers. With this agreement, these suppliers act as resellers of all IdP’s and offer a comprehensive range of services in order to authorities in eGovernment development efforts including

---

48 In parallel there is a development of digital services between government and businesses starting in the beginning of the 1990s for example concerning tax declaration and payroll data. Accordingly, these can be seen as the first digital services as mainly driven by RSV in cooperation with other actors such as Posten.

49 At this time described as the 24 hour web (24-timmarswebben) (Statskontoret 2002:13).

50 Just prior to eID-2004, the eID of Posten AB is sold and transferred to TeliaSonera.
basic services to support the eID enabling of digital services (Verva, 2006a). Renewed once more, the eID-2008 agreement is valid between 2008 and 2012 with a maximum extension to 2016 (Kammarkollegiet, 2011). This agreement has four assigned IdPs\(^{51}\) hence to be able to get access to these providers’ total stock of electronically identified customers; the SP has to sign agreements with at least three providers (Kammarkollegiet, 2015a). Being the last framework agreement of its kind between the public sector and market actors regarding eID and eSigning services in its current form, the maximum renewal option of eID-2008 is until mid-2016; a date will play a key role in the continued development of the eID and used as an argument to replace it. In 2005, a specific suborder from the current agreement called G9\(^{52}\) is performed as a joint initiative between different authorities led by The National Labour Market Board (Arbetsmarknadsstyrelsen, AMS\(^{53}\)) (Verva, 2006a).

After extensive negotiations, an agreement is signed that ensures a pre-paid fixed priced supply of eID services to the G9 member authorities (Verva, 2007). However, members of this group are not allowed to take advantage of any additional financial support for developing eID enabled services as offered by Verva (Verva, 2006b). This settlement gained significant attention in media and is described as a contract of considerable size between SPs and IdPs (e.g. Computer Sweden, 2005; Ny Teknik, 2005). Thus, this fixed-price agreement will offer the ability to easier predict and budget for eID costs (e.g. Stockholms Stad, 2011). However, a clear downside of this agreement setup eventually puts an end to the G9-group since it later turns out those authorities with an already existing digital service infrastructure benefit more than less digital service enabled authorities. This being a consequence of the rather high volume of eID transactions needed to reach a turnover in the fixed price model (Söderström, 2011).

5.1.6 Verva

In late 2006, the government decides to assign the task of coordinating the public administration’s development in areas such as secure electronic information interchange to the Administrative Development Authority (Verket för förvaltningsutveckling, Verva). With an assignment also including leading and coordinating public sector eID efforts, Verva is instructed to cooperate with several designated\(^{54}\) as well as other relevant authorities (Fi2006/6773 Fi2006/967). Regarding technical solutions, the government describes a clear need for increased interoperability and consistency across

---

\(^{51}\) Nordea AB, Swedbank AB, Svenska Handelsbanken AB and TeliaSonera AB

\(^{52}\) A part from AMS, this group included The Tax Agency, The Social Insurance Agency, and the health care region of Västra Götaland, county councils of Östergötland and Stockholm as well as the municipalities of Stockholm, Göteborg and Malmö.

\(^{53}\) From 2008 integrated into The National Employment Service (Arbetsförmedlingen)

\(^{54}\) The Data Inspection Board (Datainspektionskv), the Swedish National Financial Management Authority (Ekonomistyrningsverket, ESV), the Swedish Post and Telecom Authority (Post- och telestyrelsen, PTS), the National Archives (Riksarkivet) (Fi2006/6773 Fi2006/967)
society. Hence, technical solutions used by citizens and businesses for contact with authorities should also be used in contact with municipalities as well as private actors. This aim created a need for common guidelines, methods and specifications based on the requirements and needs of citizens and businesses (Fi2006/6773 Fi2006/967). This acknowledges the Market eID as well as an increasing need for coordination in public sector eID development efforts. In later directives, the government assigns Verva with the task of promoting eID use by offering financial support for the introduction of the eID in secure digital services resulting in a three-year program aimed at authorities across the public sector. Further, Verva should also investigate authorities’ plans for the development of eID based digital services and standardize the sub-ordering procedure from current framework agreements (Fi2006/3207). By financial support, standardization and guidance, the government anticipates an increasing number of authorities more actively developing secure digital services and in turn increasing the number of suborders from current framework agreements. Verva presents several regulations, guidelines and reports in several relevant areas and also plans for an investigation of the framework agreements, i.e. eID-2004 and Infra-2003, as a preparation for renewed procurement processes (Verva, 2008b).

In 2007, Verva presents a report focusing on the eID and suggests that the management of the public sector eID should be adapted to follow existing procedures and management of physical identification documents such as ID-cards. A more open and competitive market for the public access and use of eIDs is also suggested as well as a detailed roadmap of how these aspects of the eID can be realized. The potential benefits of this strategy are described as providing a much needed increase in competition and cooperation aligned with forthcoming EU-level eID initiatives as well as an improved level of privacy (VERVAR 2007:13). Before being decommissioned in 2008 (SOU 2008:22), Verva describes the following main challenges and problems of the eID area as related to: (1) the current procurement model, (2) technical problems, (3) the complex business and pricing model and (4) the lack of transparency and sustainability. In addition, there are several identified problems related to the acquisition, use and updating of the eID from a user perspective (5) (Verva, 2008a). Thus, Verva suggests a regulated and coordinated public sector eID area including a constitutional definition of the terms such as the Swedish eID (Svensk e-legitimation) and the Swedish Professional eID (Svensk e-tjänstelegitimation). The design of an eID certification scheme, enabling the National ID card as a carrier of eID certificates and development of regulations for business certificates are other aspects brought forth. To be able to coordinate and support this development of a coherent, open and sustainable use of the eID in the public sector, Verva proposes the creation of a central coordinating authority with the sole responsibility for coordinating and developing the public sector eID (Verva, 2008a). Hence, this is the

---

55 Such as management of electronic invoices (VERVAFS 2007:1), secure inter-organizational information exchange (VERVAFS 2007:2) and automation of public sector case processes (VERVAV 2007:1)
first time a government actor acknowledges and suggests the need of a coordinating actor in the public sector eID area.

5.1.7 The E-delegation

After the decommissioning of Verva, a new government delegation is suggested to realize the current eGovernment action plan (Regeringskansliet, 2008) and the E-delegation (E-delegationen) is awarded the mandate to guide and coordinate public authorities’ ICT related development efforts in several areas such as eGovernment, eGovernance and standardization (Dir. 2009:19). The Market eID is at this time described as a relatively successful solution but still associated with several shortcomings. For instance, there are some cases of high costs for SPs as well as problems regarding the Market eID’s flexibility and technology. Also brought forth are problems of using the eID on public and business computers\(^{56}\), issuing of eIDs to non-residents and under aged citizens as well as the challenges of using the current non-standardized eIDs and user interfaces. Thereby, the E-delegation describes the need of establishing a coordinating function focused on public sector eIDs and related services as an independent board organized within the Tax Agency. This suggested coordinating function, the Board for e-coordination (Nämnden för e-samordning), should be awarded the right to issue regulations, i.e. to be able to act in the same way that Verva did in order to coordinate and regulate the public sector eID area (SOU 2009:86).

It is also reasonable to be able to use the same eID when communicating with the public as well the private sector with an emphasis on accessibility regardless of any disabilities. Thus, the E-delegation concludes that the public sector eID is in need of a common infrastructure and technological strategy in line with for instance identity federations\(^ {57}\) (SOU 2009:86). The aim of this infrastructure is to make efficient use of existing as well as new technology in order to provide authorities and users with the needed services and make these routines simple, understandable and in accordance with applicable law (SOU 2009:86). This is an intention to protect the benefits of the Market eID legacy while preparing for the best use of new technologies. The E-delegation also states that the Market eID will be able to cover the public sector’s eID needs. However, supporting this eID solution should not exclude the possibility of developing new eID solutions as long as they are accepted by the coordinating board (SOU 2009:86). Thus, being in full agreement with the suggestions put forth by Verva, the strategy resented by the E-delegation focuses on an increased coordination and standardization of the public sector eID area.

\(^{56}\) For security and privacy reasons the use of so called “soft” eIDs, i.e. software based, discourages the use of eIDs on public and business computers (SOU 2009:86)

\(^{57}\) An infrastructure enabling relying parties, i.e. IdPs, to trust and accept the same eID (SOU 2009:86)
5.1.8 The eID gets audited

In 2009, the Swedish National Audit Office (Riksrevisionen, RiR) presents an assessment of the current state of the Market eID, and this audit is based on categories such as legal security, availability, cost efficiency and technical neutrality (tech neutrality) in turn expressed as important aspects of the eID by Government. RiR concludes that the Market eID to a large extent meets the requirements of these categories but the government and responsible authorities, have not fully acted in accordance with the Parliaments (Riksdagens) intentions regarding the development in this area (RiR 2009:19). Thus, RiR states: “The overall picture is that the eID system itself has had a positive effect on the development of eGovernment. However, there are some areas for improvement of the eID system regarding security, availability, cost efficiency and technical neutrality.” (RiR 2009:19, p. 8). The proposals suggested by the E-delegation are also acknowledged in order to meet central eID requirements (RiR 2009:19), and a summary of this assessment is presented in Table 14.

Table 14. Summary of assessment (RiR 2009:19)

<table>
<thead>
<tr>
<th>Criteria</th>
<th>Assessment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security</td>
<td>Sufficient, but lacking specific supervision to ensure personal integrity.</td>
</tr>
<tr>
<td>Availability</td>
<td>Lack of user centred perspectives has resulted in complicated end user solutions.</td>
</tr>
<tr>
<td></td>
<td>Lack of developed digital services has delayed the development of eGovernment.</td>
</tr>
<tr>
<td>Cost efficiency</td>
<td>Sufficient, but limiting agreement model regarding competition, pricing and technological development.</td>
</tr>
<tr>
<td></td>
<td>A few authorities have gained significant benefits regarding an increase in efficiency.</td>
</tr>
<tr>
<td>Tech neutrality</td>
<td>Insufficient and locked to existing suppliers preferably in the banking sector.</td>
</tr>
<tr>
<td></td>
<td>Lack of standardization, interoperability, and risk of “technological lock in”.</td>
</tr>
</tbody>
</table>
Regarding security, RiR considers the Market eID to be secure, but the system itself lacks any supervision. Hence, there is a need for specifications regarding the responsibilities of supervision of security to ensure personal integrity during management of large quantities of personal data. The availability of the eID is clearly insufficient with a lack of a user centred perspective resulting in complex end user solutions. Moreover, the lack of central coordination and control regarding eGovernment development results in authorities not prioritizing digital service development adequately and this lack of digital services, in turn, results in a lack of eID incentives from a citizen’s perspective (RiR 2009:19). Thus, according to RiR, authorities could have done more to promote the use of the eID in their digital services. Although cost efficiency is satisfactory, the current procurement model results in a very limited competition that may negatively influence pricing and future technological developments. Leading authorities in the digital service area are therefore the only ones gaining the benefits of a more cost effective eID management (RiR 2009:19). Further, the competitive pricing model is described as not working since the Market eID is based on an existing customer relation e.g. via eBanking hence a new IdP aiming at entering the eID market must already have a significant diffusion and use of eID services to be considered. The government decision of not supporting an eID issued and managed by the state has resulted in an eID solution strongly associated with the banking sector. Not fulfilling the requirements of free competition and tech neutrality as well as interoperability, it is concluded that the eID area would need more active coordination from the government (RiR 2009:19).

5.1.9 Directives for a new eID model

In 2010, the future strategy of the public sector eID is presented by the government as a sustainable supply of market based solutions meeting requirements of availability, reliability and technical interoperability with increased control and coordination of authorities’ handling of eIDs (Prop. 2009/10:175, 2010). Therefore, a special investigator is assigned with the task of preparing for the implementation of a dedicated board for coordination of the handling of eIDs and eSigning in the public sector; a board that will be located under the SKV’s administrative body (Dir. 2010:69). Accordingly, this is the point in time when the idea of a central coordinating authority regarding eIDs and eSignatures as suggested by Verva (Verva 2008:12), the E-delegation (SOU 2009:86), and the Audit Office (RiR 2009:19) is finally acknowledged and implemented. Since this eID board (E-legitimationsnämnden), henceforth referred to as the Board, will start its operations on January 1st 2011, the investigation’s final report is scheduled to December 31st 2010 (Dir. 2010:69), Thus, the work of laying the foundation for this board gets very focused on time from the start. This timeframe is also motivated by the expiring of the current framework agreement (eID-2008) on the 30th of June 2011 (Dir. 2010:69)58. Three main areas of the Board are described as: (1) ensuring the eID to be used with all public sector digital services for citizens and businesses, (2) improving the conditions

58 With a possible extension until 30th of June 2012 (Dir. 2010:69) - a suborder made on the expiration date will therefore last another four years until mid-2016 at a maximum.
for competition and development in the eID area as related to eGovernment efforts and (3) limiting the authorities’ cost of eID services as a result of central coordination and procurement (Dir. 2010:69). Thus, this puts full focus on realizing the benefits as put forth by current and previous investigations. To ensure the supply of eID service in the public sector, the government will continue to make use of existing market solutions and procure these services in accordance with the law on public procurement (SFS 2007:1091). Providers will be approved by the Board also acting as the signing party entering agreements with IdPs, providers of eSigning services as well as Certificate Authorities if needed (Dir. 2010:69). SPs joining the solution will, therefore, be able to access all services provided with approved IdPs though a proxy agreement signed with the Board. The governing directive also clearly states that the investigation should be done in close cooperation with several relevant authorities as well as The Swedish Association of Local Authorities and Regions (Sveriges Kommuner och Landsting, SKL) as advocates for local government and if necessary other authorities, municipalities and private actors should be consulted (Dir. 2010:69). Thus, the aim and focus of this investigation are to coordinate the public sector eID area, to prepare and implement the Board with the Tax Agency as a host from January 1st 2011 and to define the eID services needed to accomplish this coordination.

5.1.10 Identified challenges

Although the purpose of the investigation is described as to coordinate the eID area as well as to prepare and implement the Board (Dir. 2010:69), this effort, in fact, results in a report (SOU 2010:104) that also contains a very detailed technical blueprint of the eGov eID infrastructure. This unexpected outcome of the investigation also results in significant negative comments from a number of affected actors in public as well as the private sector as exemplified by the comments of the following referral process. Therefore, I argue that this implies a quite drastic move in the public sector eID area; from a decentralised model of renewed procurement processes to a coordinated and controlled public sector eID on multiple levels such as regulatory, legal and technical. Thus, bilateral relations and mutual trust developed over considerable time between SPs and IdPs as well as individual business needs on the organizational level will no longer be governing eID development in favour of central coordination, control and standardization. Thus, motivated by the discrepancies between the aim and outcome of the initial investigation as well as how it is perceived by practice, I argue that this calls for a detailed assessment of the potential challenges described in SOU 2010:104 (2010). This assessment, presented in full in Appendix 3, will also serve as a basis for a comparison with the actual outcome in these areas assessed as crucial as well as potentially problematic for the eGov eID introduction. This to enable the identification and verification of a set of central challenges for further analysis in following chapters. The summary of this first assessment formulated as eight challenges described in Table 15.
Table 15. Challenges and descriptions (based on SOU 2010:104)

<table>
<thead>
<tr>
<th>#</th>
<th>Challenge</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>The need of an appropriate level of information security and personal integrity</td>
<td>During its introduction, the eGov eID fails to deliver a sufficient level of information security, assurance levels and personal integrity</td>
</tr>
<tr>
<td>2</td>
<td>The need of establishing the eID model in current practice</td>
<td>The eGov eID model is not sufficiently established in public sector eID practice</td>
</tr>
<tr>
<td>3</td>
<td>The importance of cooperation and dialogue with affected actors</td>
<td>Failing to cooperate and keep an active dialogue with actors affected by eGov eID model</td>
</tr>
<tr>
<td>4</td>
<td>The identity providers will need to accept and join</td>
<td>Consequences of the eGov eID will prevent current identity providers from joining</td>
</tr>
<tr>
<td>5</td>
<td>The service providers will need to accept and join</td>
<td>Consequences of the eGov eID will prevent digital service providers from joining</td>
</tr>
<tr>
<td>6</td>
<td>The incentives of the eGov eID model need to be accepted</td>
<td>The incentives of eGov eID model are not accepted by a significant part of the affected actors, i.e. service providers and identity providers.</td>
</tr>
<tr>
<td>7</td>
<td>The need for legal amendments to support the eGov eID procurement model</td>
<td>Current law on public procurement will prohibit the new procurement model of the eGov eID</td>
</tr>
<tr>
<td>8</td>
<td>The eGov eID must be realized within the private market</td>
<td>If the private market is not included in the eGov eID solution, this solution will cover only the public sector and not reach profitability.</td>
</tr>
</tbody>
</table>

These challenges (Table 15) indicate that the way forward will be far from straightforward for the Board. With several obstacles of a critical character such as maintaining the level of information security, establishing the solution in current practice as well as ensuring the acceptance from SPs as well as IdPs will most likely present significant challenges to handle with a positive outcome. Several of these challenges are also assessed as having a high probability as well as the high impact on the introduction hence I argue that these obstacles must be considered and handled with caution to avoid any negative impact on the introduction process. Moreover, the proposed eGov eID is, in
fact, a cooperative or collaborative effort of a considerable magnitude covering the entire public sector with an inherent need for a clear and solid grounding in practice introduced on a tight timeframe.

5.1.11 eIDAS

A potential interoperability and cross-border use of eIDs is investigated on EU level during several years. In line with the i2010 initiative with the aim of developing and modernizing the public sector in Europe, the IDABC programme is created with a clear focus on the benefits of cross-border interoperability (IDABC, 2009). This work is clearly related to the “Action Plan on e-signatures and e-identification to facilitate the provision of cross-border public services in the Single Market” adopted by the European Commission in 2008 which in turn is a combination of the work of several focused areas (EC, 2008). The Single Market here referring to the free movement of people, goods, services and capital; one of the cornerstones in the EU policy framework (EC, 2014b). Within the IDABC programme, a project called eID Interoperability for PEGS identifies the trend of an increasing development of systems to manage eIDs in member states; a development that in turn would pose potential obstacles for interoperability. Thus the main challenge to address for this project is to propose a common technical architecture for eID interoperability across borders (IDABC, 2007b).

This is the first time EU proposes the SAML 2.0 standard as the preferred technology to achieve this pan-European eIDMS, and this is motivated by stating: “The SAML is the only standard adopted by a significant portion of the identity management frameworks, and it is the only standard which is already gaining implementation popularity in the Member States.” (p. 39). In addition, this standard offered the required functionalities to realize this solution (IDABC, 2007a). Further, the STORK project continues on the proposed route of using SAML for the secure exchange of authentication and authorization in turn motivated by stating that it would provide Single-Sign-On (SSO) to be able to browse multiple trusted web sites without re-authentication. It should also provide the federated identity enabling the exchange of user information between partners in a secure way as well as providing flexibility and interoperability with other existing technological standards (STORK, 2014a). To address the identified obstacles identified by previous projects, a proposal is adopted by the European Commission in 2012 describing the needed legal aspects to accomplish mutually recognized eIDs within

---

59 i2010: Information Society and the media working towards growth and jobs
60 Interoperable Delivery of European eGovernment Services to public Administrations, Business and Citizens (IDABC)
61 Pan-European eGovernment Services (PEGS)
62 Secure IdentiTy acrOss boRders linKed (STORK) consisting of the member states of Austria, Belgium, Estonia, France, Germany, Italy, Luxembourg, Netherlands, Portugal, Slovenia, Spain, Sweden, United Kingdom and Iceland
the union (COM(2012) 238). This proposal is later realized as the regulation on electronic identification and trust services for electronic transactions in the internal market (EU 910/2014) (eIDAS regulation). This regulation describes the importance of trust in the online environment in order to facilitate a positive social and economic development. Thus, the aim of this regulation is to “enhance the trust in electronic transactions in the internal market by providing a common foundation for secure electronic interaction between citizens, businesses and public authorities” (EU 910/2014, p. 1). As a result, there will be a potential of increased effectiveness for public as well as private e-services, e-business and e-commerce within in the EU (EU 910/2014). The eIDAS regulation operates on a very tight timeframe with the final mandatory recognition of all member state’s eIDs in 2018. Hence, this regulation inevitably affects the ongoing eGov eID introduction.

5.2 The introduction

5.2.1 The Board

The Board (E-legitimationsnämnden) applies a clear focus on ensuring the supply of eID services for public agencies hence this poses an inherent risk of limiting the scope of efforts to this particular type of authority. Governed by the Ministry of Enterprise, Energy and Communications (Näringsdepartementet), the Board, acts as an independent authority led by members appointed by Government. The official purpose of the Board is described as to support and coordinate the public sector’s needs for a secure eID solution and digital signing also including participation in international initiatives in areas such as standardization and information interchange related to the eID area (SFS 2010:1497). Thus, on January 1st 2011 the Board starts its operations as governed by (SOU 2010:104) and regulated by (SFS 2010:1497) with rather limited resources to develop, coordinate and introduce the eGov eID in parallel on a tight timeframe. The focus of this effort is clearly on providing a common eID solution for authorities used in secure digital services for citizens and businesses. Also motivated by the need of development in procurement and integration of eID services where an updated legislation on public procurement prevents a continued strategy of renewed framework agreements. Further, there is a need for a smooth integration of eID services in digital service development. The eID infrastructure also relates to a need for a continuous and coherent development for applications and use within the public sector. The emerging new demands and requirements on eIDs for instance in new channels for digital communication push forward the development in these areas (E-Legnämnden, 2012).

63 Later the Ministry of Enterprise and Innovation
5.2.2 The project

After its first year of operations, the Board describes long-term goals as to support and facilitate an increased use of eID services in public sector digital services, an increase in the number of IdPs and predictable, transparent and cost effective terms and conditions for SPs as well as IdPs. In addition, a smooth transfer from the Market eID to the eGov eID will also be facilitated (E-Legnämnden, 2012). Fully focused on setting up operations and building relations on national and international levels, the Board also arranges an open hearing in cooperation with the responsible ministry hosts several technical workshops and setting up a technical test environment in cooperation with the Swedish University Computer Network (SUNET). The Board takes several important strategic decisions such as the identified need of a common technical base structure utilized by the public as well as the private sector. Another identified critical question is the possibility of a central service for eSigning, which complies with legal demands as well as user-related and technical security demands. The timeframe is set for eGov eID infrastructure to be fully operative in 2013 (E-Legnämnden, 2012). This is the first occasion that the timeframe as proposed by SOU 2010:104 (2010) is revised. At the beginning of 2012, the first annual Swedish eID day is arranged acting as a forum for actors concerned with the eGov eID development (E-Legnämnden, 2013a). At this event, the current IT minister strongly emphasizes the importance of the national eID stating: “Without a secure eID there will be no momentum in the development of digital services.” (IT Minister, 2012).

Hence, the work continues, and the aim during 2012 is to provide affected actors with the option of connecting to the new eGov eID infrastructure as soon as the necessary amendments to the law on public service procurement are made final, i.e. the System of Choice (SoC). Other central areas are the procurement of central services, an overall security analysis of the eGov eID concept and the creation of a central communication plan. The Board clarifies user and security related issues of the central eSigning service and invites a number of affected actors to participate in a reference group with the aim of establishing and legitimizing the eGov eID. There are also extensive efforts to create the regulations including the needed trust framework governing the solution and acting as a basis for cooperation and trust between actors joining the solution. The Board participates in national as well as international efforts related to the EU regulation on elec-

---

64 Named The Swedish eID (Svensk e-legitimation).
65 The System of Choice is based on existing law (SFS 2008:962) which prescribes that all providers, meeting the requirements, are accepted and entitled to sign agreements with the Board in turn making it possible for eID users to select their preferred provider since all contracted IdPs become available to all SPs assigned to the solution (see Appendix 3).
The eGov eID

electronic identification and trusted services. The Board is the responsible authority regarding the Swedish participation in the EU-level STORK 2.0 project\(^{66}\). Regarding the timeframe, the Board maintains the plan to make the eGov eID available for joining as soon as the SoC and technical infrastructure are in place in 2013 (E-Legnämnden, 2013a). In 2013, the Board focuses on finalizing outstanding issues such as the regulations, accession process, branding of eGov eID, and the financial compensation (business) model. Left to handle are outstanding issues such as central federation and eSigning services, and the SoC (E-Legnämnden, 2014a). The SoC is successfully amended to law and effective from July 1\(^{st}\) 2013 (SFS 2013:311). The Board also takes an important decision regarding the eSigning service when selecting a procurement strategy instead of providing the service itself. The revised timeframe communicated in 2011 is not kept since there are still outstanding issues but at this point, the Board refrains from communicating any revised schedule (E-Legnämnden, 2014a).

In late 2013, a representative describes that the Board is moving into a new phase of the project. Hence, since the Board has solved outstanding issues, the next step will be to seek acceptance for the eGov eID among affected actors by keeping an open dialogue and handle incoming comments and views in an appropriate way. The dialogue at this time shifts from an initial critique of the model to issues regarding its consequences in practice. However, the Board reports that there are no formal and systematic procedures for handling incoming comments hence these are accounted for on a case-by-case basis (Head of Secretariat 26/11/2013). In 2014, the Board states that private IdPs report a trend of a steadily increasing use of the eID in public services. This year the Board is fully focused on seeking acceptance and promoting the eGov eID to get relevant actors, i.e. SPs and IdP, to sign and join the solution (E-Legnämnden, 2015b).

During spring 2014, the Board presents authorities with the opportunity to sign official agreements. Meanwhile, the dialogues with several selected banks in their roles as IdPs are intensified. “A guidance for the user interface in Svensk e-legitimation” is also presented as the result of the work of a dedicated reference group (E-Legnämnden, 2015b). There are several workshops with a focus of public sector authorities joining the solution. In fall 2014, the Board establishes the Governance Forum (sv. Förvaltningsforum) with the aim of governing and further developing the eGov eID. However, this forum is exclusive to members joining the solution (E-Legnämnden, 2014j). Hence, in 2014, the foundation of the new solution, i.e. the technical, regulatory and legal aspects are in place and the process moves into the next phase, i.e. dealing with outstanding comments and issues as well as seeking acceptance and an increased dialogue in order for SPs as well as IdP to sign agreements and join.

\(^{66}\) Secure idenTity acrOss boRders linKed 2.0 will contribute to the realization of a single European electronic identification and authentication area. It builds on the results of STORK, establishing interoperability of different approaches at national and EU level, eID for persons, eID for legal entities (STORK, 2014a).
However, in parallel with this process, several actors identify security risks of the eGov eID and the following events related to this discovery affects the willingness to accept the solution. Thus, while seeking acceptance for the solution, the Board also faces the difficult task of managing the critique and pressures regarding the security risks put forth by potential SPs, IdPs and other relevant authorities. Moreover, I argue that this development is rather remarkable since aspects of security such as technical information security are maybe the most critical aspects of this security solution.

5.2.3 The infrastructure

The infrastructure or the identity federation model is described as a model for cooperation between SPs, IdPs, and the operator of the federation (the Board) (E-Legnämnden, 2014d). On a technical level, this infrastructure is based on the SAML 2.0 standard\(^\text{\textsuperscript{67}}\), in turn, suggested by EU level initiatives such as the described IDABC, PEGS and STORK as the preferred standardized technology to ensure cross border interoperability between identity management frameworks (e.g. IDABC, 2007b; STORK, 2014a). Thus, the aim of this identity federation is to ensure the SPs to be able to access services from every IdP approved and assigned to the federation. Hence, there will be no need to implement specific technical solutions related to a specific IdP accomplished by standardizing agreements and technical solutions that in turn are managed by the federation operator.

\[\text{Figure 18. Agreements of the federation (adapted from E-Legnämnden, 2014d, p. 2)}\]

The joining of SPs, as well as IdPs, will be a result of signing an agreement with the Board. By signing this agreement, the members of the federation will accept to the terms and conditions of the eGov eID infrastructure e.g. regarding trust levels and technical specifications. The Board signs agreements will IdPs on behalf of SPs resulting in a

\[^{67}\text{A technical architecture used mainly for propagating identity certificates and attribute certificates among several trusted web domains, i.e. to provide Single-Sign On to multiple web sites.}\]
standardised agreement model where a contractual relationship is established with the federation operator acting as a central agreement node or proxy (E-Legnämnden, 2014d). Figure 18 illustrates this relationship together with added agreements. This model will form the basis of the SoC, which in turn provides the digital service user with the option of selecting a preferred IdP for authenticating the eID used. The infrastructure will also provide a common infrastructure or base structure, operated and managed by the Board, including functionality for electronic identification and signing. Further, a trust framework for issuing eIDs and regulations covers this base structure as well as the parties joining the federation. Any additional services needed by SPs for instance handling of attributes or signing will need additional agreements outside the federation. However, a general agreement administrated by Kammarkollegiet named EGovernment support services 2010 will provide SPs with the opportunity to make suborders of additional services from approved providers.

Figure 19. The expanded federation (adapted from E-Legnämnden, 2014d, p. 2)

Further, the agreement model also makes a clear distinction between intermediary IdPs (sv. leverantörer av eID-tjänst) and IdPs (sv. utfärdare av Svensk e-legitimation). Thus, the intermediary IdPs provides identity tickets\(^{68}\) (sv. identitetsintyg) to be trusted within

\(^{68}\) Also referred to as SAML-tickets where SAML is a technical architecture used mainly for propagating identity certificates and attribute certificates among several trusted web domains, i.e. to provide Single-Sign On to multiple web sites.
the federation while the IdPs issue the eIDs. This provides the opportunity for several IdPs to be associated with the same provider of identity tickets (E-Legnämnden, 2014d). Figure 19 illustrates this expanded identity federation model highlighting the agreements and contractual relationships between the members.

5.2.4 The business model

The initially proposed business model in (SOU 2010:104, 2010) is described as having a semi-fixed layout. Thus, for SPs and IdPs annual fees are calculated and for the local government such as municipalities and county councils, based on a number of potential users while fees for SPs on agency level are based on the number of employees. This setup is described as maintaining the model used in the Market eID thus with SPs financing the use of eID services in the public sector. Further, the market share of the eID model regulates the level of financial compensation to IdPs. This is described as the requested simple, transparent and sustainable business model of the eGov eID SOU 2010:104 (2010). However, this initial model offers several challenges since it results in a complete abandonment of the current transaction based pricing model. With the current trend of rapidly increasing transaction volumes regarding eID services paired with constantly decreasing prices per transactions, none of the affected actors will, in fact, be able to benefit from this development due to the semi-fixed nature of this model. This critique put forth by affected actors in the public as well as private sector in different forums such as the referral processes. During the introduction, the Board, therefore, presents a revised business and pricing model in order to facilitate the acceptance. However, the updated business model presented in 2015 turned out to be very complex where costs for SPs and compensations for IdPs are calculated based on factors such as a fixed price for monthly users, number of monthly users, base price and average values for the number of identity tickets issued per monthly user (E-Legnämnden, 2015e). Hence, this marks the move from a poorly accepted but at the same time simple and transparent business model to a very complex model that still does not acknowledge the requests of a fully transaction based pricing model as the current Market eID setup.

5.2.5 The referral processes\textsuperscript{69}

In spring 2011, the responsible ministry requests comments on SOU 2010:104 (2010) by issuing a referral process (N2011/559/ITP)\textsuperscript{70} among potential affected and relevant actors in the public as well as the private sector. With a high response rate of 102 answers, the comments show a significant variance in how different authorities and actors perceive and translate the eGov eID with a selection presented below. The strategy of a centrally controlled and coordinated solution with market actors supplying eID services is fully supported by some (e.g. .SE, 2011; Arbetsförmedlingen, 2011; Domstolsverket, 2011) while others, preferably representatives for local government instead strongly recommend a state issued eID (e.g. Norrköpings kommun, 2011; SKL, 2011). There are

\textsuperscript{69} For English translations of actors not previously mentioned see Appendix 4.

\textsuperscript{70} The comments received are later compiled and distributed by the ministry in PM N2011/559/ITP (2011)
also criticisms put forth since the Market eID is perceived as successful and authorities are very dependent on a fully working eID solution (e.g. Försäkringskassan, 2011). A majority of the responses can be placed somewhere in between since they acknowledge the benefits of the coordinated eGov eID while at the same time identifying several important aspects lacking or not fully investigated. Some authorities even present clear requirements for accepting and joining when for instance SKV describes that the security requirements must be set on a very high level in order for the eGov eID to be accepted (SKV, 2011). The lack of information regarding the transfer to the new solution is also put forth (e.g. CSN, 2011; SKV, 2011) as well as the need for clear guidelines regarding this process (e.g. CSN, 2011). A lack of descriptions on how the eGov eID will affect already existing eID solutions is also identified (SKL, 2011) as well as how eIDs for professional use will be handled by the new infrastructure (e.g. Nacka kommun, 2011). Regarding these concerns, a special emphasis is put on the consequences of the eGov eID in the health sector (e.g. Jämtlands Läns Landsting, 2011; Sandvikens kommun, 2011). The importance of the eGov eID being able to support cross sector digital services, services developed in cooperation between public and private actors is also put forth since this type of collaborative services between sectors are not covered (e.g. Jämtlands Läns Landsting, 2011; Jordbruksverket, 2011; Länsstyrelsen Örebro län, 2011; Nacka kommun, 2011). Further, a lack of strategy about how the eGov eID will handle accessibility based on functional ability is also described (Handisam, 2011). The need of a well performed and comprehensive risk analysis is emphasised (MSB, 2011) as well as how under-aged and non-residents will be handled in the solution (e.g. SKL, 2011).

Several authorities also describe that (SOU 2010:104) itself as very challenging to analyse due to its perceived complexity on technical as well as legal levels (e.g. CSN, 2011) and there is a need for a clear conceptual model of the eGov eID to increase understanding and minimize misinterpretations (e.g. Sandvikens kommun, 2011). Overall, the timeframe is seen as being too optimistic since there is an imminent risk of authorities not being able to complete the transfer on time (e.g. Försäkringskassan, 2011). A very strong emphasis is also put on the importance of continued work to be done in close cooperation with SPs and IdPs (SKV, 2011). The business model is perceived as transparent and predictable by some authorities (e.g. Bolagsverket, 2011; CSN, 2011) while others describe it as too complex, uncertain, and most likely associated with increasing costs (Jämtlands Läns Landsting, 2011; Länsstyrelsen Västra Götalands län, 2011). IdPs comment on the business model and describe it as completely different from the current transaction based model (e.g. Finansiell ID Teknik, 2011). Hence, the new business model will make it impossible for IdPs to predict a positive coverage of required investments, therefore, requesting a clear relation between transaction volumes and financial compensation (e.g. Svenska Bankföreningen, 2011). Thus, a common view of market actors as potential IdPs is the risk of IdPs not joining the solution due to poor financial compensation (e.g. Finansiell ID Teknik, 2011; Handelsbanken, 2011;
Swedbank, 2011). Further, RiR states that the comments presented in the previous audit (RiR 2009:19) are mainly accounted for still but comments on outstanding issues regarding availability from an end user (citizen) perspective and the communication efforts needed for affected actors to recognize the benefits of a common eID solution (Riksrevisionen, 2011). In November 2012, the ministry issues a second referral process now with a focus on the proposed amendment to the law, i.e. the System of Choice (SoC) (Näringsdepartementet, 2012). From the comments received on this memorandum (N2012/5484/ITP) it is clear that the majority of respondents are in favour of the SoC as an appropriate way to handle the access to eID and eSigning services in the absence of a procurement law able to handle multiple providers of similar services (c.f. SFS 2007:1091). In addition to commenting on the law amendment, several authorities, however, take this opportunity to comment on the eGov eID solution, in general, resulting in a significant critique of the solution. For instance, the challenges and costs of parallel eID solutions when still supporting the Market eID while the eGov ID is being phased in (Försäkringskassan, 2012), authorities still advocating a government issued eID (e.g. SKL, 2013c). The need for further investigations related to information security (FMV, 2013) and stronger financial incentives for private sector IdPs (TeliaSonera, 2012) as well as the crucial role of IdPs in the solution (Transportstyrelsen, 2012) are also views put forth. In line with the first referral process, this second process confirms that the eGov eID area is still very problematic associated with several conflicting views and translations. A summary of the most frequent concerns put forth by affected actors in these two referral processes is provided below.

- Required security levels and security analyses
- Lack of information and guidelines regarding transfer
- Implications on current eID solution (Market eID)
- eIDs for professional use (health care)
- Support for cross sector digital services
- Accessibility based on functional ability
- Need of risk analysis
- Complexity of (SOU 2010:104)
- Timeframe as too optimistic
- Need of cooperative efforts
- Business model as complex and uncertain (SPs)
- Increased costs
- Poor financial compensation (IdPs)
- eIDs should be issued by the state
5.2.6 Changes to the eGov eID programme

There are some significant changes made to the eGov eID programme during the Board’s mandate. For instance, in 2011 a future integrated eID infrastructure to be applied to the public as well as the private sector is presented (E-Legnämnden, 2011) as a clear contrast to the divided infrastructure described in SOU 2010:104 (2010). However, if coordinating the public sector eID proves to be problematic, including the private sector in these efforts will be even more challenging, if possible at all. In 2013, the Board makes another important change to the model regarding the central eSigning service described in SOU 2010:104 (2010). In the referral process (N2011/559/ITP) this aspect of the eGov eID received significant critique which in turn results in the decision of letting external actors provide this service rather than the Board itself. This in turn motivated by inefficiency and financial aspects of keeping parallel infrastructures for identification and signing. Therefore, the Board assesses that the appropriate way to allow access to eSigning services to public sector actors in the eGov eID model is provision under a general agreement from which actors in need of such services can make suborders (E-Legnämnden, 2013b).

Accordingly, eSigning services of the eGov eID are integrated into the current general agreement managed by Kammarkollegiet on eGovernment support services (E-förvaltningsstödjande tjänster 2010, EFST-2010) (Avropa.se, 2010). This new approach to signing is later officially presented with specifications and requirements (E-Legnämnden, 2014e) and with additional guidance of the sub-ordering process (Kammarkollegiet, 2015b). Even though one of the incentives of the eGov eID is to move away from general agreements governing the eID area, the need of eSigning services forces the Board to reassess their role in this process. The third change to the eGov eID regards the provision of identity tickets to propagate identity certificates among the members of the identity federation (SAML-tickets). The report (SOU 2010:104, 2010) states that these tickets will be provided by the IdPs themselves.

However, at the eID Day of 2015, the Chairperson of the Board presents that IdPs will be offered the option of not supplying these tickets hence only having to support authentication as in the current Market eID model. This accommodates the demands of the IdPs in the banking sector not willing to expand their delivery of such services that will result in increasing costs for additional development and adjustments. With IdPs not providing the identity tickets, the Board will provide this service via procured services from external suppliers. In addition, this change to the eID model will also eliminate consequences for SPs since it becomes the sole responsibility of the Board to deliver additional identity tickets when needed (Chairperson February 4 2015).
5.2.7 The security risks

In December 2013, two authorities and representatives from the banking sector CA and a bank meet with the Board. Initiated by one of the authorities, this meeting focuses on the security risks in the eGov eID model identified by the CA (Security Architect, 2013-11-27). This meeting is, in turn, the result of an active dialogue between one authority and the CA initiated in October 2013 coming to a mutual understanding of the severity of these risks (Security Specialist Agency#1 December 13 2013). This meeting attracts a lot of interest with several representatives from other authorities participating unannounced. This event is described as a breakthrough since the participants including the Board agree upon the main critical areas to be addressed to eliminate the identified risks, and a joint action plan is formulated (Security Specialist Agency#1 December 13 2013). However, in January 2014, the Board distributes a Letter of Intent (LoI) to the 17 member authorities of the E-delegation with an urge to support the eGov eID and sign which in turn causes one authority to react very negatively. On January 15th 2014 the E-Delegation has a workgroup meeting with a discussion of the eGov eID on the agenda (Security Specialist Agency#1 January 16 2014).

At this meeting, several authority representatives show clear concerns about the status of the eGov eID but at the same time, a representative from the Board claims that there are no outstanding issues regarding the solution (Security Specialist Agency#1 January 16 2014). As a result, one authority’s confidence in the Board drops significantly since one of the current tasks of the Board at this time is to form the working group to address the most critical security issues as agreed upon at the previous meeting in December. Consequently, at this point, this authority decides to end the dialogue with the Board and pursue other means to influence the eGov eID in the appropriate direction, i.e. with a correct handling of the identified security risks (Security Specialist Agency#1 January 16 2014). At the annual eID Day in 2014, a representative from the Board confirms the problematic aspect of the identified security risks. However, these risks are seen as symptomatic and a result of the current process moving into the next phase of the introduction with a higher level of interest regarding the consequences of the eGov eID. To cover all possible threats is described as an impossible task for the Board hence these identified shortcomings will need to be discussed further and handled along the way (Head of Secretariat January 30 2014).

In February, as a result of the Board’s handling of the identified security risks, an authority sends a request to the Swedish Civil Contingencies Agency (Myndigheten för Samhällsskydd och Beredskap, MSB) requesting an impartial investigation focusing on the identified security risks of the eGov eID solution. This action in turn based on this authority perceiving the Board not taken appropriate measures to handle these important issues. Even though the Board invites the actors participating at the meeting in December to a new meeting in February to further discuss these issues, this authority clearly
doubts the Board’s ability and competence to handle these issues. Thus, MSB is considered a suitable impartial external party to further investigate these issues as based on this authority’s responsibility for information security on a national societal level (Security Specialist Agency#1 February 17 2014). This request is entitled “A request for an analysis of the eGov eID technical solution” and describes a list of possible risk scenarios. Hence, MSB is requested to investigate if these scenarios exist in the eGov eID solution and perform an analysis to detect any other potential risks or threats with the solution (Agency request February 11 2014). Almost simultaneously, a similar request for a security analysis is submitted to MSB by another authority (Agency request February 17 2014). Even though these two requests are significantly different from each other they are still sent from the two authorities attending the meeting in December 2013 (Security Specialist Agency#1 February 17 2014). Therefore, I argue that this is the result of two separate internal enrolment processes at authority level in turn based on the same grounds, i.e. the eGov eID as associated with severe security flaws and in dire need of an external analysis.

Later a third authority also joins to this call (Agency request February 24 2014). One important aspect these three requests have in common is the concern of the end user perspective being been left out of previous risk assessments of the eGov eID as well as online threats such as distributed denial of service attacks (DDoS). However, there is also critique raised against these calls for an external analysis tracing these requests back to the security assessment made by a market actor, i.e. the banking sector CA. Hence, this action is described as being performed in collusion with market actors wanting to uphold their current strong position on the eID market (Technical Specialist March 13 2014). On the other hand, I argue that this is a shared consensus among actors with high expertise in the security area. Other relevant public sector actors also acknowledge these security risks describing the risk of manipulating the communication between the user and the digital service and exploiting vulnerabilities on the user’s client. Further, DDoS attacks would possibly affect all connected digital services and most likely put citizens’ overall trust in society at risk (Infrastructure and Security Specialist April 14 2015). Hence, the Board seemingly fails to address these well-known cybercrime threats and the following events will prove if this critique is well grounded.

5.2.8 The security analysis

In May 2014, the responsible ministry issues a commission in response to the request for a security analysis made by the three authorities. However, in the ministry’s press release it is stated that the Board itself will be awarded the mandate to lead this security investigation that will be performed in cooperation with MSB and the final report is scheduled to end September (Näringsdepartementet, 2014). Thus, the Board is to investigate its own proposed eGov eID solution from an overall “security perspective” and

---

71 Distributed Denial of Service (DDoS) - a malicious attempt to make an online service unavailable to its users
perform it in close dialogue with MSB. It is also stated that several other relevant authorities should be a part of the dialogue (N2014/2207/ITP). The ministry motivates this approach by stating: “It is critical that users and authorities have confidence in the model of the Swedish e-ID. It is, therefore, important that the model is characterized by a sufficient degree of security and that in-depth analyses from a security perspective are performed.” (N2014/2207/ITP, p. 3). The government, therefore, chose not to mention that several major agencies had found potential security flaws in the model but instead it is announced at ministry level as “A government assignment for a safe and secure eID” (Näringsdepartementet, 2014). The request of having an external independent party leading the investigation of identified security risks is toned down to a scenario where the Board is set to lead an analysis of its own eID solution. Although this government decision is welcomed, in general, one of the requesting authorities shows concerns regarding how the assigned roles and relations between the Board and MSB will affect the outcome of this analysis; if it will be conducted in an objective and fair way (Security Specialist Agency#1 May 9 2014).

Moreover, I fully agree with arguments saying that this approach of self-investigating or auditing is questionable. If the Board fails to deliver a sufficiently high level of information security, this might indicate that maybe this authority may not be best suited to coordinate and conduct such an analysis. A clear mistrust, therefore, starts to develop among authorities since the anticipated independent investigation turned out to be a highly dependent one. In the wake of the requests, the eGov eID gets significant media attention, and a leading Swedish IT news site describes it as the eGov eID process is entering a critical state regarding the challenge of gaining acceptance from affected actors (ComputerSweden February 17 2014). Several following articles focus on areas such as the requested external security analysis (ComputerSweden March 12 2014, 2014) and the eGov eID process is described as messy and poorly grounded in practice (ComputerSweden May 9 2014). Moreover, the author is interviewed and describes the current obstacles during the introduction as: “[I]t is not entirely unproblematic to coordinate the entire public sector regarding this area; with its diversified activities, requirements and services.” (ComputerSweden February 17 2014).

In August, the Board officially requests comments from selected authorities regarding their view of the eGov eID to provide the starting point for the security analysis. Areas covered in this request are if the security analysis is motivated, potential risks in the eID model, if and how usability should be weighed against security, the clarity and scope of the regulations framework and how the dialogue between the Board and SPs can be improved (E-Legnämnden, 2014c). The overlap is, therefore, significant between the

72 Arbetsförmedlingen, Bolagsverket, Centrala studiestödsnämnden, Försäkringskassan, Skatteverket, Sveriges Kommuner och Landsting och Vetenskapsrådet/SUNET
initial requests for the security analysis and the Board’s request for additional information to be able to perform the analysis. This request also results in respondents again having to assess the entire regulatory framework of the eGov eID, which in turn is very complex. End September, the Board presents the result of the security analysis on site at the ministry, and during this presentation, nothing unusual or critical is ever mentioned regarding the previously reported security risks (E-Legnämnden, 2014f). When asked if there will be any written report of the analysis, the Board replies that they are considering presenting one. Hence, the Board has already reported this assignment. This presentation is therefore in clear contrast to the report that MSB presents later in October as a list of recommendations for actions to be taken to provide a more secure eID solution on a general as well as a very specific level (MSB, 2014a).

Moreover, the complete MSB report gets classified by the Swedish Publicity and Secrecy Act (Offentlighets- och sekretesslag) (MSB, 2014b) and thus, referring to secrecy with the aim of the prevention of crime (SFS 2009:400). During their analysis, MSB with its mandate of supporting and coordinating information security in society (SFS 2008:1002)\(^\text{73}\) cooperates with relevant actors in the security area such as The Swedish Armed Forces (Försvarsmakten), the National Defence Radio Establishment (Försvarets Radioanstalt, FRA) and the Swedish Defence Research Agency (Totalförsvarets forskningsinstitut, FOI) (MSB, 2014a). Thus, MSB puts forth 22 recommendations for the Board ranging from general recommendations, regulations and agreements, crypto-algorithms, technical requirements (SAML) as well as the central infrastructure (MSB, 2014a). MSB puts forth several recommendations to identified shortcomings such as the need of adding strategic technical competence either directly to the Board or by the support of relevant authorities with expertise in technical information security. Further, the need of a complete information security assessment of the eGov eID when the solution is operational as well as regularly and on major changes is strongly suggested (MSB, 2014a).

The regulations and agreements concerning the eGov eID should also define a minimum of requirements regarding security, plan for future development based on affected actors’ needs, supply relying on parties with risk information and provide a similar end user interface when authenticating and signing (MSB, 2014a). The Board should also develop guidelines for non-repudiation and DoS/DDoS attacks as well as perform regular assessment and control based on structured methodology. Regarding technical requirements, the Board is recommended to perform a risk analysis and handle the identified risks, and the central infrastructure should be subject to a complete security assessment and to a higher degree relate to common standards and best practices in the field of information security (MSB, 2014a). Thus, in summary, MSB strongly suggests that the Board integrates a clear information security perspective in their current and future

\(^{73}\) Regulation (2008: 1002) with instructions for the Swedish Civil Contingencies Agency
work and take needs and comments from current and potential members of the eID federation into consideration. Moreover, I argue that judging from the coverage of these recommendations, MSB is presenting the result of a very thorough and detailed analysis and identifies a clear lack of an information security perspective and grounding in practice which in turn may explain the previously identified risks. The fact that MSB presents these suggestions in the form of recommendations tones down the severity but is, in turn, a result of MSB’s mandate and role in the analysis. Hence, I argue that this analysis confirms the identified security risks first brought forth in December 2013. Later in October, the Board presents its written final report of the analysis, suggesting actions such as an increased focus on information security and a general overview of potential high-risk areas. Since the Board’s report does not emphasize or focus on identified risks, it is significantly different from MSB’s report. The Board chooses to include comments from only a few of the responding authorities regarding their views of the eGov eID including two of the agencies that already, at this time, had accepted and joined the solution (E-Legnämnden, 2014g).

The perspectives of the two authorities requesting the analysis are therefore not described hence one can assume that the authorities that the Board refers to in this document are the strongest supporters of the eGov eID at this time. In media, the presentation of these two reports again attracts attention with headlines like “Classified report confirms security flaws in the eID system” (ComputerSweden October 27 2014). In summary, the security analysis resulted in two official reports, and this in turn raises questions about how to translate and measure these reports against each other. The fact that MSB chose to classify some of the content also raised concerns about the severity of these findings. In addition, an authority’s requests to get access to the classified report is rejected with a motivation that it will counteract with the efforts to prevent and manage peacetime crises (Security Specialist Agency#1 November 26 2014). However, the security analysis performed is on a general level and perceived as positive. One of the requesting authorities describes that they intend to use MSB’s recommendations as a checklist to ensure that these aspects are handled in a correct way prior to accepting and joining the solution (Security Specialist Agency#1 November 3 2014).

These events also result in a clear change in the Board’s attitude towards these security issues. From describing them as based on individual business needs and a result of authority level consequence analyses, that the eGov eID had no significant outstanding issues and stating that the eGov eID is as secure as the current one, the Board shifts towards being positive of the security analysis. Thus, from initially focused on developing the internal technical, legal and regulative framework of the eID, there are pressures

---

74 “Government commission: In depth analyses of the Swedish eID from a security perspective” (E-Legnämnden, 2014g)

75 SKL, Arbetsförmedlingen, Skatteverket, Bolagsverket, Datainspektionen and SUNET
put upon the Board to consider, acknowledge and include potential SPs and IdPs perspectives regarding these issues. Nevertheless, several authorities signed and joined the eGov eID during fall 2014 despite the ongoing security process.

5.2.9 The action plan

Regardless, these two reports focusing on the security set the agenda for the following eGov eID introduction since the Board needs to consider and handle the recommendations put forth. Still very concerned about how these issues will be handled, one authority considers approaching other relevant actors if the Board fails to address them properly (Security Specialist Agency#1 December 2 2014). In December, a meeting is also held with representatives from the two strongest opposing authorities, the Board and the responsible ministry with the aim of discussing these outstanding security issues (Security Specialist Agency#1 December 11 2014). Thus, the Board informs that the Board itself in cooperation with the Governance Forum will handle MSB’s recommendations. The Board presents a draft action plan, but a representative reports the lack of further specifications regarding how and in what timeframe the Board will solve the recommendations. Still, the Board seems to have the full confidence of the ministry to solve these issues (Security Specialist Agency#1 December 18 2014). Thus, it is clear that the newly formed Governance Forum will have a very important role in the coming efforts to adhere to these recommendations.

The forum has its first meeting in November and consists of representatives from the Board as well as from authorities that had joined the eGov eID. The mission is described as to support and coordinate the further development of the eGov eID and eSigning in public sector digital services (Förvaltningsforum November 4 2014). During following meetings, the forum continues to address the recommendations and the action plan as suggested by the Board (Förvaltningsforum December 16 2014, 2014) as well as topics such as the competence needed in the forum (Förvaltningsforum February 17 2015, 2015), the status of the eGov eID (Förvaltningsforum March 18 2015, 2015) as well as the status of member authorities work on adapting and transferring to the solution (Förvaltningsforum April 17 2015, 2015). Regarding how the draft action plan is perceived by affected actors, one authority shows concerns over that fact that the Board transfers the responsibility of managing the recommendations to the forum thus arguing that although the incentives of the forum are positive, it is still the Board that must lead this work due to the resources needed.

This authority also argues that the action plan needs to be specified further in order to provide a basis for the work to be done and put forth amendments such as clearer timeframes and the importance of continuously ensuring the security of the solution (Security Specialist Agency#1 January 19 2015). These comments on the action plan are submitted in accordance with agreements made at the meeting in December 2014 (Action plan review January 19 2015). Another authority describes that the presented plan is a good start but in need of further work and specification and also emphasizes
the importance of solving the outstanding problems as soon as possible (Action plan review January 20 2015). The Board presents the finalized action plan in February 2015 and contains a description of the analysis and suggested actions to each of the 22 recommendations. On a general level, these action points are categorized as issues to be handled by the Board, issues concerning all SPs, issues based on the needs of the public sector and issues that are important for IdPs in the federation (E-Legnämnden, 2015a). Thus, I argue that one could assume that the Board’s version of action points would match the recommendations put forth by MSB in relation to their prioritization but a comparison of these two documents shows interesting differences. The most significant discrepancy is regarding recommendation #20 described by the Board as:

“The eID Board should consider having an independent third party to conduct a comprehensive security review (architecture, implementation, hardware, software (both proprietary and COTS) of the central services of the Swedish eID such as the metadata service.” (E-Legnämnden, 2015a, p. 20)

However, the original recommendation by MSB states:

“As for the central infrastructure MSB recommends that the eID Board should let an independent third party to conduct a comprehensive security review (that include architecture, implementation, hardware, software: both developed and COTS) of the central services in the Swedish eID, including metadata service.” (E-Legnämnden, 2014h, p. 4)

Thus, the priority changes from the original “recommends that”, i.e. the highest priority in the MSB report, to “should consider” that in fact is described as only the third highest priority in the action plan. This example together with other differences between these two important documents indicate that the recommendations are clearly subject to interpretation and translation by the Board. However, I argue that this is an example of an unfortunate event since MSB presents the original recommendations in a form that allows a subjective re-interpretation of the weighing and priority given to these issues.

5.2.10 The confirmed risks

In March 2015, The National Defence Radio Establishment (Försvarsveterens radioanstalt, FRA) announces that they are releasing their security audit performed in 2014 as a part of the security analysis led by MSB. Although being classified to a significant extent,
the release of this report brings new media attention to the eGov eID reporting that “FRA condemns the common eID solution” (SVT, 2015) and there are several arguments stating that the government must take this critique seriously (e.g. Kolsjö, 2015). However, there is no agenda behind the release of this report hence it is just the result of a private person requesting access to the classified version of the report and FRA assessing if it could be made publicly available with adjustments (Spokesperson FRA April 22 2015). Focusing on FRA’s security audit, it states that: “In its present form/execution, it is the FRA’s assessment that the use of [the eGov eID] exposes users and authorities to considerable risks.” (FRA, 2014, p. 2 Appendix 1). Thus, in this document, there are several clear statements describing the severity of these problems such as; “The security of the eID infrastructure assumes user clients are unaffected [i.e. by malicious software, authors note] which is an absurd view that that must be abandoned by the Board. The risk of identity thefts is currently imminent.” (FRA, 2014, p. 2 Appendix 1).

The eGov eID infrastructure is described as: “The infrastructure shows several technical weaknesses which in combination with other associated problems can result in severe effects.” (FRA, 2014, p. 2 Appendix 1) and “An infrastructure where vital security mechanisms to counteract against everyday online and ICT threats are missing from the start may result in extremely difficult problems to solve.” (FRA, 2014, p. 3 Appendix 1). Also described as problematic are existing problems regarding cooperation and dialogue: “[P]rivate as well as public actors and authorities have expressed concerns over the Board not heeding to views and suggestions. Members of the federation, therefore, rely on informal channels, in turn, resulting in a varying exchange of information and uneven security levels.” (FRA, 2014, p. 3 Appendix 1). Thus, FRA is much clearer and outspoken regarding the security flaws and risks of the eGov eID than the previous two reports. After this report is presented to MSB in 2014 as a part of their cooperation, FRA reports that they are maintaining an active dialogue with the Board (Spokesperson FRA April 22 2015) and the responsible ministry reports that there is a continued confidence that the Board will solve the outstanding security issues (Head of Section April 20 2015).

MSB reports that they also deem the Board as fully capable of solving the identified risks hence no active follow ups will be performed (Project Manager Security Analysis April 24 2015). Symptomatically, the interest and media coverage of the eGov eID security risks that follows puts a renewed strain on the process of gaining acceptance for the solution. Regardless, several affected actors in public as well as private sector started to question how the security risks are handled by the Board (Product Manager Bank#1 April 29 2015; Security Specialist Agency#1 April 28 2015). Further, the issue of agencies not accepting the eGov eID received increased interest on ministry level initiating an investigation of individual authorities’ views of the eGov eID (Product Manager Agency#1 May 4 2015). This most likely being the first step of escalating the discussions regarding the solution’s problematic aspects to ministry level as opposed to the previous discussions where individual agencies had communicated with the ministry.
responsible for the eID. In addition, this would also facilitate and increase the potential for a more intensified political debate regarding the eID. Also confirming the severity of these risks, a government investigation focused on information and cyber-security refers to this incident by stating: “This can result in severe and extensive loss of information. An incident as such would be a direct danger to society.” (SOU 2015:23, p. 306).

5.2.11 The search for acceptance

In a Letter of Intent (LoI) distributed in January 2014, the Board describes that the members, as indirect supporters of the eGov eID initiative, need to clarify their intentions to join the solution. Although this is no binding agreement in a legal sense, it is described as a much needed next step in the accession process (E-Legnämnden, 2014b). However, authorities perceive this action as a means of the Board to force acceptance of the eGov eID to be able to present a positive progress at the coming eID Day end January 2014. Actors also translate this event as a means to increase the strength of the eGov eID in order to put an increased amount of pressure on the IdPs since for instance, the banks show no signs of an increased willingness to join the solution. The situation becomes far more complicated since the Board does not live up to the agreements regarding the handling of the identified security risks in December 2013. The LoI is then perceived as an act of enforcing eGov eID acceptance while avoiding taking the agreed upon action. To remain in control and not losing any means of pressure, the authority urges that the LoI should not be signed until the security risks have been solved (Security Specialist Agency#1 January 14 2014).

This decision of unconditionally accepting the eGov eID at this stage is also anchored at director general level at this authority thus any LoI to be signed will have to clearly state that the identified security risks must be handled and fixed in a secure way (Security Specialist Agency#1 January 15 2014). Nevertheless, the LoI gets signed by the members of the E–delegation and SKL in January (E-Legnämnden, 2015b) but getting to this stage proves to be a cumbersome process due to the previous criticisms and resistance to the eGov eID by some authorities. Objections to the LoI results in the following change of formulation: “The intention is to sign the agreement with the Board as soon as all necessary conditions have been met” (E-Legnämnden, 2014b). Although, considered a very positive step forward in the Board’s process of gaining acceptance for the solution by leading authorities, the formulation in the agreement also opens up the possibility for authorities to make strong demands on the Board in order to sign the actual agreement. Thus, I argue that the LoI becomes a double-edged sword by showing progress regarding eGov eID acceptance but at the same time acting as an incentive for specific authorities to stall the process of signing the actual agreement with the Board further. Also, worth noting is that E-delegationen is one of the authorities initially proposing and supporting a centrally coordinated eID model. At the annual eID Day 2014, the chairperson of the Board comments on the signed LoI and says that it will make things much easier since these leading authorities are willing to act as early adopters of
the eGov eID (Chairperson January 30 2014). To get a sense of urgency; at this event, an agency representative strongly emphasized the need of the eGov eID meeting the security requirements by stating: “If it fails, it will be a disaster” (Agency Representative January 30 2014). In an effort to promote public authorities to join the Board arranges workshops in June and September with the focus of discussing outstanding issues from the SP’s perspective (E-Legnämnden, 2014i, 2014j). The first one focused on aspects such as the status and outstanding issues of the eGov eID process, authorities’ responsibilities, preparations, the process of joining, relations to EU initiatives such as STORK and eIDAS as well as some selected technical aspects. However, the Board’s mandate to lead the security analysis is only very briefly discussed (Workshop June 4 2014). A participant of the second workshop describes that the Board confirms that no one had signed the agreement to join yet hence this raises questions about the status and potential success of the project as a whole.

As participants put forth the need of having a backup plan to secure the supply of eIDs if the eGov eID would fail to get acceptance from the current key actors such as IdPs, the Board declined to answer which in turn is translated into a clear lack of such a plan (Security Specialist Agency#1 September 5 2014). Regardless of the ongoing controversies and significant resistance, I argue that the single most important indicator of eGov eID acceptance is the number of authorities accepting and signing legal agreements with the Board to join the solution. In September 2014 there are three authorities, i.e. Bolagsverket (2014), SKV (2014) and Transportstyrelsen (2014), and at the beginning of October, a fourth authority joins (Arbetsförmedlingen, 2014). The process of getting authorities to sign shows positive progression and in spring 2015 eight authorities have joined (E-legnämnden, 2015d). However, I argue that this is a very low acceptance rate since there is a potential of 336 authorities in the Swedish public sector in total (Regeringskansliet, 2013). Thus the proportion of agencies having joined is only approximately 2 percent. In May 2015, the majority of the public sector as well as private sector IdPs still not accept the eGov eID. At the annual eID day 2015, the chairperson of the Board emphasizes the shortage of time, referring to the final deadline of the extended time of the last framework agreement in mid-2016, and emphasizes the importance of public sector actors joining. There are several positive incentives such as the ability to influence the process via the Governance forum and no costs involved when joining. It is also up to the actors themselves to decide when the eGov eID should be operational in their services. Nevertheless, affected actors must complete preparations needed as soon as possible to avoid any interruptions in the eID delivery process. Thus, the chairperson strongly emphasizes that all authorities, agencies as well as municipalities, must join as soon as possible (Chairperson February 4 2015). In late May 2015, together with the leading banks and Finansiell ID-Teknik (BankID), the Board invites

---

76 Bolagsverket, Skatteverket, Arbetsförmedlingen, Transportstyrelsen, Kronofogdemyndigheten, Pensions-myndigheten, Rekryteringsmyndigheten and Lantmäteriet.
The eGov eID

representatives from the already joined authorities, the authorities of the E-Delegation as well as SKL, The eHealth Agency (eHälsoomyndigheten) and The Swedish Transport Administration (Trafikverket) to a stakeholder meeting. The aim of this meeting is to present the status of the current work of gaining acceptance from private market IdPs. At this time, about ten agencies have joined, a number considered much too low.

The importance of getting the banks to accept the eGov eID is emphasized and very important to facilitate a broader acceptance. The dialogues between the Board and the three major banks\textsuperscript{77} are described as intensified, and a mutual plan of connecting the Market eID (BankID) to the eGov eID is negotiated (E-Legnämnden, 2015c). At authority level, this invitation creates interest but also clear concerns since the call for this meeting is translated as a means of the Board trying to force an acceptance from the banks (Security Specialist Agency#1 May 20 2015, 2015). Even though the invitation focuses on the progress in the dialogue between the Board and the banks and their intention to join (E-Legnämnden, 2015c) a bank representative clearly points out that they experience a clear pressure to accept and join before summer 2015 but did not perceive this as realistic mainly due to the adjustments needed to the eGov eID model. The banks’ intention is still to join but in the longer term and provided that the outstanding security issues identified by MSB and FRA are resolved (Product Manager Bank#1 May 21 2015).

Thus, the Board postpones this plan to negotiate and overcome one of the main obstacles in the acceptance process, i.e. getting the IdPs to accept and join, until later in fall 2015. In June, the Board also made clear that it is not mandatory to join the eGov eID and that affected actors are solve eID related issues by themselves, e.g. via bilateral agreements with IdPs. However, the Board stresses that these services must support the coming eIDAS regulation (Offentliga Rummet, 2015a). So this is also a new direction in contrast to the arguments saying that public sector would have no option as to join (Chairperson February 4 2015); a development also noticed by authority representatives (e.g. Product Manager Agency#1 June 9 2015) as well as bank representatives (Product Manager Bank#1 June 16 2015).

5.2.12 Need of a backup plan

The different handling of the eGov eID seems quite hard to motivate as compared to other ICT related solutions. Hence, the normal way of handling it when one strategy fails would be to negotiate agreements with alternative providers. Since these types of agreements take the time to formulate and negotiate, the need for a plan B to ensure the continued supply of eID services for public authorities should become increasingly critical as the deadline of 2016 is fast approaching. In June 2015, the Board places the interim solution higher up on the agenda. Hence, since several authorities initially put forth this need on a workshop in September 2014, the Board takes considerable time to

\textsuperscript{77} Swedbank, Nordea and Handelsbanken
acknowledge and act upon this request. However, the result of investigating these issues on authority level, i.e. by legal means, indicated that there should be not significant obstacles to proceed with renewed bilateral agreements with one of the dominating banking sector IdPs (Security Specialist Agency#1 September 5 2014). With the recent strong development of BankID one agreement with an IdP providing BankID will in fact cover over approximately over 90 percent of the current eID market hence the availability to citizens and businesses will still be at a reasonable level. According to statistics of one authority, in spring 2015 the BankID has even surpassed 99 % of the total transaction volume of authentications in this authority’s digital services (Security Specialist Agency#1 May 5 2015, 2015). Moreover, one authority describes three existing alternatives regarding how authorities can handle the supply of eID services. They can join the eGov eID (Plan A), they can hopefully get some interim solution via the Board to be able to use the Market eID model for a limited time (Plan B) and they can go ahead and procure the eID directly from the current market IdPs directly or via intermediaries (Plan C) (Infrastructure and Security Specialist April 20 2015). Summarized in Table 16 are the positive and negative consequences of these three alternatives.

Table 16. The eGov eID alternatives (Infrastructure and Security Specialist April 20 2015)

<table>
<thead>
<tr>
<th>Pros</th>
<th>Cons</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Plan A (Join eGov eID)</strong></td>
<td><strong>Plan A (Join eGov eID)</strong></td>
</tr>
<tr>
<td>Potential new IdPs</td>
<td>Increase in cost (4-9 times)</td>
</tr>
<tr>
<td>Compatible with EU (eIDAS)</td>
<td>Questionable timeframe</td>
</tr>
<tr>
<td></td>
<td>Resources to migrate quickly (6 months)</td>
</tr>
<tr>
<td></td>
<td>Private sector incompatibility</td>
</tr>
<tr>
<td><strong>Plan B (Interim solution)</strong></td>
<td><strong>Plan B (Interim solution)</strong></td>
</tr>
<tr>
<td>No initial need to migrate</td>
<td>No details published yet</td>
</tr>
<tr>
<td>Private sector compatibility</td>
<td>A temporary solution</td>
</tr>
<tr>
<td></td>
<td>Pricing according to the new model</td>
</tr>
<tr>
<td><strong>Plan C (Procure directly)</strong></td>
<td><strong>Plan C (Procure directly)</strong></td>
</tr>
<tr>
<td>No need to migrate</td>
<td>A monopoly</td>
</tr>
<tr>
<td>Private sector compatibility</td>
<td>How to connect to EU (eIDAS)</td>
</tr>
<tr>
<td>Current pricing</td>
<td>eGov eID compatibility</td>
</tr>
<tr>
<td></td>
<td>The end of eGov eID?</td>
</tr>
</tbody>
</table>

Plan A (to join) is the scenario where the authority joins the eGov eID and gets access to the new IdPs as well as the compatibility with EU level (eIDAS regulation). However, this alternative has the negative consequences of significantly increased costs, a questionable timeframe, the challenge to allocate resources for a quick migration and the
incompatibility with the private sector. Plan B (interim solution) delivers the benefits of using the current Market eID solution hence there is no immediate need for migration and this approach fully supports private sector compatibility. However, the Board has not at this time published any details of such an interim solution hence questions like how such a temporary solution would affect the process and if the pricing would be according to eGov eID are not accounted for. Finally, Plan C when authorities procure directly from current IdPs will result in authorities continuing to run the current solution with no need to migrate, continue to provide private sector compatibility at the current or possibly lower pricing levels. However, this scenario will continue to support the monopoly of the banks while not accounting for EU interoperability (eIDAS).

Further, this plan will potentially be the end of eGov eID, if all authorities continue with current IdPs the purpose and aim if the eGov eID would be obsolete. However, the Board finally acknowledges the potential risk of actors not being able to join and adjust to eGov eID on time by the deadline in mid-2016 and presents the transition service (sv. övergångstjänst) at the end of June 2015. This solution bridges the potential gap of eID service delivery by providing the possibility to use the Market eID solution as managed by a new agreement model. Hence, the Board will sign agreements with current IdPs with their services provided to the SPs in a power of attorney agreement. Acting as a proxy, the Board describes that this agreement will be valid until end 2017 (Förvaltningsforum June 16 2015). Hence, this is also described as a way to simplify the agreement process for authorities not being able to transfer to the eGov eID before the deadline (Head of Secretariat 26/06/2015). There is a referral process of the additional agreement needed for the transition service (E-Legnämnden, 2015f) and the agreements are established in one version for the IdPs (E-Legnämnden, 2015g) and one version for the SPs (E-Legnämnden, 2015h).

5.3 The government perspective

5.3.1 The Ministry

The responsible Ministry of Enterprise and Innovation describes the work of defining a future vision for the public sector eID as very important since this will provide a clear policy of the future aims and goals for the public sector eID. This also the point in time when the government’s perspective of the eID is changing from being focused on the introduction on a technical, regulatory and legal level to a perspective where the eID becomes a significant part of the bigger picture for the current and future development of eGovernment on a national as well as international levels. Hence, as described, the eGov eID moves from a clear introduction phase into a phase focused on gaining acceptance for the solution (see Section 2.4.1). These visions are important in order to provide the needed clear, solid and hopefully more positive grounding in favour of the eGov eID. Hence, clear and positive incentives of the eGov eID in the context of the entire public sector can potentially minimize any resistance. However, these efforts are
separate from the Board’s actual introduction of the eGov eID hence the aim is to facilitate future development rather than address current challenges. The ministry describes this visionary work as the future development of the eID using the eIDAS regulation\(^\text{78}\) as a lever. Even though the ministry is fully aware of the problematic state of the eGov eID as well as the criticisms and resistance to it, the ministry instead tries to avoid getting involved in these discussions stating: “Now it's time to lift our eyes and look forward, not backward” (Head of Section 10/04/2015).

According to the ministry, in the past, the eID has not received the attention and focus needed on ministry level and has mainly been focused on the current Market eID solution based on renewed public procurement processes (Head of Section 10/04/2015). Further, the election in 2010 results in a transfer of eGovernment issues from the Ministry of Finance (Finansdepartementet) to the Ministry of Enterprise (Näringsdepartementet). During this transfer, issues related to the eID ends up handled by officials with legal expertise at the ministry. This is a consequence of several aspects such as the current very narrow perspective on the eID as well as limited resources for the ministry. At the time, the referral process for SOU 2010:104 (2010) is performed, and the legal perspective is still seen as relevant for specific aspects of the eGov eID such as the agreements, framework of regulations and the System of Choice (SoC) (Head of Section 10/04/2015). However, at this time, government perceives the eGov eID as mainly an expense for the state and the lack of interest from the political level continues. The previous government, therefore, decides that the new model should be funded by members’ fees hence the Board is not seen as entitled to any significant funding as compare to the scope of the task to develop and introduce the eGov eID. The perspective at this time (2010-2013) can be described as rather short termed, and the technical aspects of the eID are handled in an isolated way with important aspects such as cooperating with affected actors and acceptance taken for granted. This limited perspective also results in the acceptance and joining of current leading IdPs not being sufficiently grounded and problematized in SOU 2010:104 (2010). This is also acknowledged as a clear weakness of this initial investigation (Head of Section 10/04/2015).

However, with the view on the eID changing into an increased contextual perspective, the ministry since 2014 supports the Board as much as possible in its work but also describes that this is a matter of assigned mandate and responsibilities. The ministry must be cautious since the Board, as an awarded authority, owns the responsibility of

---

\(^\text{78}\) To address the identified obstacles, a proposal was adopted by the European Commission in June of 2012 that described the needed legal aspects to accomplish mutually recognized eIDs (COM(2012) 238). This proposal was later realized as the regulation on electronic identification and trust services for electronic transactions in the internal market (EU 910/2014) (eIDAS regulation) with the aim of addressing the weaknesses of the Signature Directive (EU 910/2014) regarding cross-border and cross-sector interoperability in order to accomplish usable, trustworthy and secure electronic transactions.
introducing the eGov eID. The role of the ministry concerning the eID is, therefore, to work on a higher strategic level rather than getting involved in operational issues. The aspect of getting public authorities to accept the eGov eID is acknowledged and seen as problematic by the ministry but is at the same time related to the independency of Swedish authorities. As a final option, the government has the possibility of enforcing authorities via directives, but as far for other actors such as municipalities, the government has no ability to exert pressures in specific directions. Thus, municipalities are completely independent and out of the Government’s control which in turn is a clear matter of concern regarding the acceptance. An alternative could also be to exert political pressures on the eGov eID process but with a remaining question being when it would be appropriate (Head of Section 10/04/2015). In spring 2015, several the ministry initiates several initiatives with the aim of developing an increased understanding of the current challenges related to the eGov eID as well as eIDs future potential in the public sector. In relation to the ongoing introduction of the eGov eID, there is a clear sense of lack regarding a current and future agenda for the eID (Head of Section 10/04/2015).

Hence, this is the result of responsible officials on ministry level starting to realize the importance of the eGov eID from a public sector perspective. The problematic state of the process is also described as in need to move the eID higher up on the political agenda, but since these insights are quite novel, the ministry struggles to understand how the problematic state of the eGov eID process had come to be. As a result, several initiatives are initiated to further investigate the area to provide a better picture of the current status and the future prospects of the eGov eID (Head of Section 10/04/2015). These efforts are conducted in the form of an investigation of the current affairs of the process and the potential of more authorities accepting and joining the solution (Investigator January 30 2015). In addition, an investigation focuses on the future potential an eID in a national as well as international perspective with a timeframe set to 2020\(^79\) (Consultant April 23 2015). Moreover, I argue that the obstacles in the eGov eID process relate to the difficulties of handling ICT issues on central coordinating political levels. One clear example, besides the eGov eID, being the handling of personal integrity as related to ICT that has been investigated with aims for an increased coordination on several occasions, most recently in (SOU 2015:31). Regarding how individual authorities have accepted and joined the solution can also be related linked to specific authorities receiving specific instructions in their government directions regarding actions to take towards and introduction of the eGov eID. This applies to directions given to the National Employment Agency (Arbetsförmedlingen) (Regeringen, 2013a), the National Board of Housing, Building and Planning (Boverket) (Regeringen, 2013b), the Swedish Transport Administration (Trafikverket) (Regeringen, 2013d), the Swedish Transport Agency (Transportstyrelsen) (Regeringen, 2013e) and the National Archives (Riksarkivet)

\(^79\) This perspective on the year of 2020 was later revised to 2025 (Offentliga Rummet, 2015b).
(Regeringen, 2013c). Thus, these agencies are instructed to prepare to join in their directions from government seem to correlate well with the agencies that have currently signed and joined eGov eID.

5.3.2 The Board

From the Boards’ perspective, the eGov eID introduction is associated with a number of obstacles based on different perspectives of the eID and the difficulties of gaining acceptance for the solution. In spring 2015, the criticisms and resistance to eGov eID seem to decrease. However, but the Board has no knowledge if this is due to an increasing level of acceptance among affected actors or related to other factors. The very low acceptance rate of the eGov eID relates to the move to a completely different eID model. This, in turn, results in significant transitions and adjustments for authorities and such transitions take considerable time. The Board puts forth several aspects, which could have had a positive impact on the introduction. For instance, financial aid to SPs to support the transfer to the eGov eID. However, this kind of support still not being possible due to the Board’s limited funding and mandate. In line with the ministry, the Swedish governance model of highly independent authorities is also a significant challenge for cooperative efforts to handle. Nevertheless, the Board is still confident that the eGov eID will gain acceptance and momentum over time as a result of major authorities leading the way and with the joining of the banks (Head of Secretariat 26/06/2015).

Nevertheless, the magnitude of the scope, potential obstacles and inherent contradictions of the eGov eID are still problematic: “Many are saying that this is an impossible mission for the Board from the beginning. Low funding, providers requesting high compensation and authorities are requesting low costs. It should make things easier, and at the same time the authorities need to make changes.” (Head of Secretariat 26/06/2015). Also acknowledged is the fact that the Board may have underestimated the importance of addressing different actors’ perspectives and expectations on the eGov eID since they are clearly diverging. With this in mind, it could have resulted in a better understanding and acceptance of the eGov eID as well as more successful support and management, i.e. more clear and strict directives from the government (Head of Secretariat 26/06/2015). The Board manages cooperative efforts described as related to the hosting of several different forums and reference groups, the E-delegation (E-Delegationen), bilateral meetings as well as meetings focusing on specific aspects of the eGov eID. The Board invites actors to submit comments throughout the process and the information is available on the Boards’ website. The Board maintains an active dialogue with some leading authorities as well as several major banks. Submitted comments are analysed, and some have resulted in adjustments, preferably in the regulatory framework.

80 Skatteverket, Bolagsverket, CSN and Försäkringskassan
A more intensive dialogue with three banks\textsuperscript{81} since summer 2014 is also confirmed (Head of Secretariat 26/06/2015). In summer 2015, the Board is focusing on critical areas of the solution such as how to get the banks to accept and join as well as to solve the outstanding security issues. Ensuring the security, therefore, becomes an important lever to facilitate the final goal of gaining a broad acceptance in public as well as private sector. The Board also points out the challenges in trying to solve these issues in in parallel with the introduction of functionality continuously added to the solution. Other challenges put forth are for example that management of issues and comments of a principal character such as repeated requests for the eID provided by the state since this is clearly outside the Board’s official mandate. The Board could, therefore, have been more explicit and clear about its mission; that issues outside government aims and goals of eGov eID should be addressed directly to the ministry (Head of Secretariat 26/06/2015).

5.4 Service Providers’ perspective

5.4.1 The Market eID

The eID is of great importance authorities across the public sector being the foundation of the security of employees as well as for providing secure digital services to citizens and businesses. One authority even describes the eID as trusted by SPs in the public sector as a prerequisite for modern society to work (Infrastructure Manager Agency\#1 October 14 2013). A typical example of an existing positive view of the current Market eID describes it as a well-functioning solution. As issued by banks it is perceived as a positive initiative with a sufficient security level offered at a reasonable cost (CIO Agency\#1 15/10/2013); a perspective confirmed by several other authorities (e.g. Business Developer Agency\#2 17/03/2015; Head of Digital Channels Agency\#1 05/06/2014; Information Security Manager Agency\#1 12/06/2014; Security Specialist Agency\#1 19/11/2013). The dominance of the banking sector IdPs is not perceived as a problem but rather just a result of market development (Head of Digital Channels Agency\#1 05/06/2014), or as one official put it “Government has quite deliberately created the oligopoly we have today” (Information Security Manager Agency\#1 12/06/2014). From an SP’s perspective, the current solution being a proprietary one could, therefore, be seen as subordinate (IT Security Manager Agency\#1 14/02/2014). Hence, the market dominance of the BankID is not seen as problematic if compared to other ICT related areas e.g. where development over time has led to dominating software solutions (CIO Agency\#1 27/06/2014). However, several authorities do not share this consequentialist view of the Market eID especially local government applying a more ideologist perspective still suggesting a state issued eID. It should also be noted that the eID is in fact provided by several banks hence there are in a sense not one single provider (CIO Agency\#1 27/06/2014). It is also clear that there is one category of authorities

\textsuperscript{81} Bank\#1, #2 and #3 selling the eID to public sector actors.
being especially dependent on a working and secure eID solution; the ones managing financial cases such as tax returns and allowances (Infrastructure Manager Agency#1 October 14 2013).

As exemplified by the Tax Agency and the Social Insurance Agency, these are also among the early adopters of the Market eID to be able to provide secure digital services to their customers during the first half of 2000. These authorities quickly identified and realized the benefits of secure communication and online transactions replacing manual handling of these tasks and today there are even examples of completely automatized the handling of routine cases (CIO Agency#1 15/10/2013). Thus, extremely dependent on the well-functioning solution as provided by the Market eID, which in turn have provided very important steps towards the realization of modern eGovernment development with a clear focus on internal and external back office efficiency and timeliness as well as increased accessibility for customers (CIO Agency#1 15/10/2013). The requested security levels regarding electronic identification internally as well as externally are therefore strong factors pushing the development, integration and use of the eID (Infrastructure Manager Agency#1 19/11/2013).

This high dependency of a well-functioning and secure eID solution is shared by all four major authorities featuring in this study (e.g. Business Developer Agency#2 17/03/2015; Information Security Strategist Agency#3 19/03/2015; IT Security Manager Agency#4 March 30 2015); or as one official answers to the question what would happen if the eID fails: “Then we’ll have to go back to handling papers again” (Business Developer Agency#2 17/03/2015). The strong positive development of the mobile platform as part of the current digital channel strategy is also confirmed (e.g. Area Manager Agency#1 03/03/2014; Business Developer Agency#2 17/03/2015; Head of Digital Channels Agency#1 05/06/2014; IT Architect Agency#2 17/03/2015) hence this introduces new types as uses of mobile digital services as facilitated by mobile eIDs such as the mobile BankID. As the currently strongest developing eID in public digital services (e.g. SKV, 2015c), this development is the result of a positive match fulfilling the needs and requirements of specific user groups with access to the mobile banking eID. Hence, the mobile eID becomes an important facilitator for developing mobile digital services in the public sector. Since the eGov eID should not introduce any obstacles regarding the future development of digital services, the lack of support for mobile services in the eGov eID is seen as highly problematic (CIO Agency#1 27/06/2014). Further, authorities do not acknowledge the positive financial incentives of eGov eID such as lower costs for SPs: “Our agency will have to pay 50% more for exactly the same thing we have today. It is a bad deal. It will be both worse and more expensive.” (IT Security Manager Agency#4 March 30 2015). Further, from a local government perspective, the cost estimates as based on maintained transaction volumes, the eGov eID will result in five to nine times higher costs for eID services (Infrastructure and Security Specialist April 14 2015). This in turn quite being a significant contradiction to one of the main
incentives of the eGov eID that is described as lowering the costs for the local government in addition to improved transparency and predictability (E-Legnämnden, 2012).

5.4.2 The eGov eID

Although acknowledging and emphasizing the need of an increased level of cooperative efforts regarding eIDs within the public sector, the incentives and motives behind the coordination as related to the eGov eID are perceived as unclear: “It sounds good, but we wonder if we really need it?” (CIO Agency#1 15/10/2013). Promoting competition on the eID market and moving towards a more standardized solution sound good but according to authorities, the most important aspect is that the eID solution actually works and meets the requirements for instance regarding security levels. When talking to authorities, it soon becomes evident that security is one highly prioritized area. One representative describes that a security solution such as the eGov eID failing to deliver on security will never gain the acceptance needed (Security Specialist Agency#1 19/11/2013). Therefore, it comes as no surprise when several authorities perceive the handling of the security risks as far from optimal in turn resulting in a stronger resistance to the eGov eID.

A CIO describes that this agency is still not accepting and joining the eGov eID and, especially staff working with security, are very dissatisfied with how the Board handles the identified security risks as a result of a perceived lack of participation, information and handling of the security issues (CIO Agency#1 27/06/2014). SPs are also fully responsible for the security the along the entire chain of information: “We cannot accept a service that introduces potential threats to our customers.” (Information Security Manager Agency#1 12/06/2014). Regarding actors criticising this authority for running the errands of the IdP, one official states: “It’s not because we want to defend the BankID solution in any way. It’s because we want an eID solution that’s secure for us and our customers.” (Information Security Manager Agency#1 12/06/2014). Therefore, as long as the identified security risks remain unsolved, several authorities will not accept the eGov eID. Another obstacle of the eGov eID introduction is described as the neglecting the importance of the important parts played by SPs, IdPs and eID users or customers. If one of these important parts is missing in this network, the eGov eID will not be a success. An authority comments on this relationship by stating: “It is strange that a lot of people does not understand this. It is the foundation that has to be there. Otherwise, it [the eGov eID] will fail.” (Information Security Strategist Agency#3 19/03/2015). Hence, for an eID introduction to reach success there must already exist an eID with a significant diffusion and use in society and reaching this initial step can be very cumbersome: “It’s very difficult, and the most difficult part is to get the citizens to accept and use the eIDs.” (Information Security Strategist Agency#3 19/03/2015). For example, the National Post Office did not manage to get enough diffusion and use when introducing its own card based eID solution. The diffusion also serves as an important incentive for SPs to develop digital services and this part of this relationship relates back to the emergence of the Market eID.
Without any digital services, there are also no incentives for issuing and diffusing eIDs (Information Security Strategist Agency#3 19/03/2015). So this becomes a chicken and egg dilemma: which comes first – diffusion of eIDs or development of digital services? Hence, the Board neglects the need of eID diffusion and use in order for the eGov eID to succeed; “We can only deliver digital services. No one has been responsible for this aspect of eID users in eGov eID:” (Information Security Strategist Agency#3 19/03/2015). The public and private market convergence of the current Market eID model facilitates the use of the same eID in public as well as private digital services. This approach also lets public and private SPs to be integrated into the same digital service context, e.g. in health portals with public as well as private caregivers. Officials describe this convergence as one of the major strengths of the Market eID, and the eGov eID must address this public and private sector synergy in a different way.

Since the solution only supports use in a public digital service context, from an SP’s perspective, the eGov eID must support the use in mixed digital service contexts. Another issue of eGov eID put forth from a local government and health care perspective is how the solution will integrate with eID solutions for professional use where there is a clear need for employees to be able to authenticate themselves both in their professional as well as in their private roles (Infrastructure and Security Specialist 20/04/2015). This applies in contexts where there is no interoperability between the professional eID and the authority’s digital service. For example, the health care sector solves this by integrating a private certificate on the professional smartcard as exemplified by the SITHS solution described in Chapter 6. However, the lack of compatibility with professional eIDs results in a lack of trust between the professional and public digital service context. By focusing solely on the citizen’s perspective on the eID, this delimits the solution from professional use. On repeated occasions, SPs inform the Board of these shortcomings without any success. It then becomes clear that the Board had never put the eGov eID in a practice context and scaled up its implications and consequences which in turn is notable since it will affect the entire public sector (Infrastructure and Security Specialist 20/04/2015).

5.4.3 Cooperation and dialogue

Inter-organizational cooperation is nothing new in the public sector since one authority describes that they have been actively working with trying to increase the cooperation between authorities for a considerable time. These efforts have for example covered the development of back office communication solutions based on an authority certificate aiming at facilitating information interchange across agencies with a higher level of security and trust\(^\text{82}\) (Infrastructure Manager Agency#1 October 14 2013). The main incentives behind these initiatives have been mutual benefits among the members. Hence several authorities have significant difficulties acknowledging the unclear benefits of eGov

\(^{82}\) The authority CA (sv. MyndighetsCA)
The eGov eID

eID. One important aspect having a significant impact on the acceptance of the solution is how the Board has handled cooperation and dialogue during the introduction. In reply to this, one authority states: “Normally, authorities tend to cooperate and develop solutions based on mutual benefits but in this case; here’s the solution – comply or die!” (Information Security Manager Agency#1 12/06/2014). Thus, this describes the lack of cooperation and the introduction as forced upon authorities. Since these views are shared among several authorities this critique has to be taken seriously as possibly related to an insufficient grounding in practice: “The biggest problem is that they (the Board) have built the solution without establishing it among affected actors and without a dialogue and the problems we see today is a direct result” (Business Developer Agency#2 17/03/2015).

The apparent lack of cooperation is also described as: “The Board has shown a complete lack of ability in getting the authorities and providers to cooperate in this work.” (IT Security Manager Agency#4 March 30 2015). Also put forth as a critique is the Board’s unwillingness to communicate with the banks as well as maintaining the dialogue with authorities in a highly unstructured way and only focused on a few authorities (IT Security Manager Agency#4 March 30 2015). Another challenge is the Board repeatedly neglecting to take action and keeping agreements: “On several occasions, we have agreed to discuss specific issues with the Board, but at the actual meeting their agenda has been completely different.” (IT Security Manager Agency#4 March 30 2015). There are several examples of agency representatives addressing questions to the Board without getting any answers or the Board responding that they did not agree. “If this happens too often you just lose your trust in the other party. This is serious when it comes to an infrastructure like this one – then trust becomes very important.” (Information Security Manager Agency#1 12/06/2014).

The Board’s response or lack thereof translates into an unwillingness to keep an open and honest dialogue. Another obstacle is the divergence between the Board and affected authorities regarding the technology used for the eGov eID. While the Board claims the solution is based on open standards as prescribed by previous successful EU initiatives, authorities describe that the wrong technology is used to solve the problem. In addition, authorities perceive that the Board did take advantage of the existing competence in the public sector, i.e. expert authorities, but instead turned to external consultants to realize the proposed strategy (IT Security Manager Agency#4 March 30 2015). One official comments on the presented plan by stating: “I had not been able to imagine that they [the Board] would come up with something completely new and at the same time violating their mandate.” (Information Security Manager Agency#1 12/06/2014), hence referring to the evident lack of close cooperation with existing market and affected actors. As it turns out, authority officials even argue that the Board has been using incorrect arguments while trying to establish the benefits of the solution.
In general, the Board’s communication is non-transparent and unclear hence the Board can benefit from being more transparent and communicate about current issues. For example, since 2012 the Board reports that the negotiations with affected actors are progressing and that outstanding issues will soon be solved (Information Security Strategist Agency#3 19/03/2015). Thus, several different messages have been sent to affected actors; that it is mandatory to join, that eGov eID is going to be forced by laws, that authorities cannot procure future eID services on their own as well as authorities not being able to sign agreements with multiple IdPs. However, several of these aspects used to get authorities to accept and sign have turned to be incorrect (Information Security Manager Agency#1 12/06/2014) since the Board later reveals that for instance bilateral agreements are still an option and joining the solution is voluntary. The dialogue is also described as clear problem based (Information Security Manager Agency#1 12/06/2014) and far from optimal: “I’ve seldom seen such an isolationistic project that should be based on cooperation and an active dialogue.” (Information Security Manager Agency#1 12/06/2014).

As described above the Board has a significantly different view of the cooperation offering, for example, several different forums of dialogue and cooperation as well as bilateral discussions. However, one can manage reference groups in various ways to support different purposes and agendas. Depending on the Board’s agenda and members’ competence these groups can, in fact, be used to facilitate a productive dialogue or just to push information (Information Security Manager Agency#1 12/06/2014). When the Board started out the dialogue between the SPs and IdPs had historically been positive hence, the Board had the chance to benefit from these positive relations, but unfortunately, they did not manage this well at all (IT Architect Agency#2 17/03/2015). So it is clear that the Board had a job to do and the plan is set, so they started talking to the banks only after the foundation is developed (Business Developer Agency#2 17/03/2015). One authority even describes that they had nothing to do with the Board until this authority being among the ones approaching MSB with a request for an external security analysis (Information Security Strategist Agency#3 19/03/2015). There is also an evident lack of communication and support regarding the process of actually connecting to eGov eID as an SP; “There are no guidelines one could read about the process of connecting. Even though the extensive and complex framework of regulations is available; there’s hardly any one that will bother reading it all and trying to understand what to do” (Infrastructure and Security Specialist 20/04/2015).

Although the Board announces such guidelines, they are not presented which in a way is strange with the deadline of joining eGov eID fast approaching. Without any proper guidelines and information other than related to the regulations and trust framework it is very difficult for affected authorities without the proper competence, especially local government, to understand its consequences (Infrastructure and Security Specialist 20/04/2015). Since most of the security risks put forth by leading authorities are in fact
initially identified by the bank consortium (CA), one could argue that these should be issues to be solved between the consortium (the banks) and the Board than rather with authorities having to act as mediators in the middle (IT Security Manager Agency#1 14/02/2014). This problematic relation between the Board and the banks is also described as a possible reason for other problems in the process: "The authorities are stuck in the middle between the Board and the banks – maybe that is why some authorities are dissatisfied, they feel they are stuck in the middle" (Information Security Strategist Agency#3 19/03/2015).

5.4.4 Acceptance and trust

So far I argue that the perspectives and views of SPs presented do not provide the best opportunities for building acceptance and trust in the eGov eID. The diverging translations and extended controversies are clear indications of the lack of grounding the eGov eID in practice, i.e. among affected actors. Acceptance and trust are therefore maybe the most critical aspects related to the success or possible failure of eGov eID. One authority describes this dilemma as directly related to the perceived benefits of the solution. If the benefits are substantial and clear for affected actors, the higher the possibility of acceptance and success of such inter-organizational initiatives. Hence, a solution forced upon authorities without clear benefits will most likely negatively affect the process of gaining acceptance (Security Specialist Agency#1 19/11/2013). However, the initial work of focusing on and coordinating the eID area made sense since a move towards a standardized solution instead of having different proprietary solutions would potentially result in decreasing management costs and a decent competitive market; both regarding prices and how competitive markets tend to work (IT Architect Agency#2 17/03/2015).

These also being some of the main incentives for the support and acceptance of the eGov eID from the beginning (IT Architect Agency#2 17/03/2015). Further, there are also examples of major authorities taking a greater responsibility: “We have to believe in this – as a major agency we must show that’s our intention. Otherwise, no one will accept it, and that’s when this will most definitely fail.” (IT Architect Agency#2 17/03/2015). Hence, this authority, in fact, describes the support of the eGov eID as a decision of principle from the beginning (Business Developer Agency#2 17/03/2015). This stance can also be linked to what another authority describes as some kind of unspoken ‘duty of loyalty’ towards the government which in turn has chosen this solution (Information Security Strategist Agency#3 19/03/2015). Meanwhile, authorities are free to act independently and must attend to their operations as well as their customers in a clearly business driven way.

Taking the events described in this chapter into consideration, it comes as no surprise that several officials report that they have serious shortcomings in their trust towards the Board. Moreover, this can be linked to perceptions of the Board on repeated occasions refraining from meeting agreements such as regarding the identified security risks. Thus, this lack of trust has serious negative implications on the introduction process since it
results in statements such as “It is always with scepticism we attend meetings with the Board.” (IT Security Manager Agency#1 14/02/2014). Another aspect affecting trust and confidence as well as acceptance are the numerous revised deadlines and time schedules (Security Specialist Agency#3 19/03/2015). One official even reports that the time schedule is revised on eight occasions (Infrastructure and Security Specialist 20/04/2015). One authority even argues that what the Board is trying to sell is actually an amount of trust (IT Security Manager Agency#1 14/02/2014) hence this amount drastically decreases when the Board does not live up to the expectations as translated by authorities.

The inherent duty of being loyal to the government described above is clearly not shared among authorities, for example, stating: “The Board wants all agencies to come together, accept the eGov eID and join but we perceive this as any service and want to know what the risks are.” (IT Security Manager Agency#1 14/02/2014). Thus, this authority does not share this kind of ethical standpoint to support the eGov eID for the greater good of the public sector as a whole but rather perceives it like any other ICT or security related effort. However, as soon as the outstanding security risks are solved this particular authority will accept the eGov eID (IT Security Manager Agency#1 14/02/2014). Hence, trust in this sense relates to this particular actor’s requirements on the solution, identified security risks and in turn, how the Board had handled these issues: “We will not join a solution with clear risks and deficiencies regarding security. You have to show us, as the customer, that we can trust this.” (Security Specialist Agency#1 14/02/2014).

5.5 Identity Providers’ perspective

5.5.1 The Market eID

When asked to describe their view of eGov eID, one bank official immediately responds: “There is no way we would have done something like this ourselves!” (Product and Process Manager Bank#2 19/03/2015). In a sense, these words indicate the challenges ahead when trying to gain acceptance from the current dominating IdPs (the banks). Similar to SPs, the IdPs think the convergence model of the Market eID works very well. Although it is possible to question the historical decision to let market supply the eID for the public sector, the government still made this decision, and the current solution has developed positively, and it has worked very well: "The silly thing is that we already have a working national solution. That’s why BankID was created in the first place." (Product Manager Bank#3 June 17 2015). The IdP describes the development of the joint BankID as a successful strategy, i.e. to consolidate competence and technology into a separate business unit appointing the banks as selling parties towards authorities. The government’s outspoken need of a working eID solution procured from market providers initiates this development with one success factor described as forming a joint effort while focusing on cost efficiency and coordination.
The fact that all major banks have come together and used the same eID for their own eBanking services has drastically strengthened and improved the BankID solution (Product Manager Bank#3 17/06/2015). According to IdPs, the critique against this oligopoly is therefore also a confirmation of this successful development. Further, bank officials describe the importance of having a significant diffusion and use of eIDs in order to succeed as an IdP on the market. Hence at present, it is very difficult to identify any new potential IdPs. Moreover, due to very low costs, very high transaction volumes must be reached in order to make this business case worth investing in (Product Manager Bank#1 17/03/2015). One must also have in mind that the providing eIDs to the public sector is not part of the core business of commercial banks. With financial incentives in the margin, the continued support of the banking sector is still based on loyalty towards the public sector and the willingness to provide eID services to authorities as a societal service (Product and Process Manager Bank#2 19/03/2015). Responding to the identified security risks, IdPs state that the banking sector will never accept an eID solution with inferior security, i.e. introduction of new risks, than the current solution.

Even if the entire public sector is completely shut off from the BankID solution in case of an incident, bad will and harm of trust could still spill over onto the BankID and the banking sector (Product Manager Bank#1 17/03/2015). Without a clear understanding of the eID process and chain of trust, customers could easily blame the BankID and perceive it as insecure (Product and Process Manager Bank#2 19/03/2015). Thus, these IdPs are extremely cautious about not introducing any new security risks in the eID model. In addition, questions about why the security perspectives on the eID should be different between the sectors stating: “Why should the public sector have other requirements regarding the eID than the banking sector regarding its security?” (Product Manager Bank#3 17/06/2015). Thus, implying that the highest possible security level should apply in both sectors.

5.5.2 The eGov eID

Although the banks have been openly positive towards supporting and possibly joining the eGov eID, the process as governed by the Board is far from unproblematic from the IdPs point of view. Nevertheless, they are, as well as the Board, still confident and committed to trying to solve the outstanding issues leading up to the acceptance and joining of the banks. Nevertheless, the IdPs still acknowledge several negative consequences of the solution and also state that the current problems seem to be a result of the eGov eID not being officially discussed among affected actors (Product Manager Bank#3 17/06/2015). This as exemplified by increased costs for SPs and IdP as well as the inferior business model from a banking sector perspective. The positive incentives of the eGov eID as translated by IdP’s are the current solution being associated with high costs, procurement problems and the need of improved development and competition as well as promoting more eID suppliers (Product Manager Bank#1 17/03/2015).
This view corresponds well with the official incentives motivating the eGov eID. However, the single most important motive is the required changes in procurement described to the IdPs as having no other option than to accept and join the eGov eID if they want to continue to support the convergence model by providing eID services (Product Manager Bank#1 17/03/2015). Thus, in the earlier stages of the introduction, the Board pressures the banks to accept the eGov eID without any objections. However, not all share this view and banks argue that BankID can, in fact, be used in the public sector without considering neither an updated procurement model nor the final deadline of the eGov eID in mid-2016 (Product Manager Bank#3 17/06/2015). Hence, this is clearly a result of the very strong development of the BankID resulting in agreement with one BankID bank covering almost the entire eID market. Accordingly, IdPs have strong objections against this semi-fixed business model of the eGov eID.

On this point, the eGov eID is clearly diverging from the current Market eIDs transaction based agreements (Product Manager Bank#3 17/06/2015). A point of view that exists as a shared consensus among IdPs (Product Manager Bank#1 17/03/2015) is the positive development of the Market eID being a result of increasing transaction volumes combined with decreasing transaction fees (Product Manager Bank#3 17/06/2015). Thus, the semi fixed pricing model of the eGov eID is by several affected actors described as associated with significantly higher costs for eID services. This is described as unfortunate since high costs are normally associated with the development of the digital service itself (Product Manager Bank#3 17/06/2015). Extensive negotiations regarding the business model are held on a strictly bilateral basis between the Board and the banks as a result of the laws on competition (Product and Process Manager Bank#2 19/03/2015). Still not fully accepting the eGov eID due to outstanding issues from the IdPs perspective such as security risks and lack of flexibility the IdPs are fully aware that there could be other means of pressure put the banks to join e.g. from ministry level (Product Manager Bank#3 17/06/2015) and/or political level (Product and Process Manager Bank#2 19/03/2015). Thus, the security analysis presented by MSB is perceived as a response to their concerns and in turn as evidence of the lack of security competence in the Board (Product Manager Bank#3 17/06/2015). Although the imminent need of new IdPs, from the banks’ perspective, the only other realistic provider would be telecom companies. However, so far only one\(^{83}\), as previously owned by the state, has shown any interest in issuing eIDs (Product Manager Bank#3 June 17 2015). When asked to describe any positive incentives of the eGov eID, IdPs put forth the potential decrease in the number of agreements and customer relations to be managed with the Board acting as an agreement proxy between the IdPs and SPs (Product and Process Manager Bank#2 19/03/2015).

\(^{83}\) Telia
Thus, potentially only one agreement between the Board and an IdP providing BankID will be needed to cover the entire public sector. Since the banks have their own regulations regarding the BankID, adding an additional level of regulations related to the eGov eID is perceived as potentially negatively affecting the much needed flexibility of the eID solution (Product Manager Bank#3 17/06/2015). Hence, to be able to continue and develop the BankID in a proactive way to prevent online threats and cybercrime, the IdPs are not willing the risk facing negative consequences of rigid regulative frameworks of the eGov eID. Therefore, IdPs argue that the Board has not taken current external threats and the flexibility needed to handle future threats into sufficient consideration hence the intention put forth by the Board to launch the solution and improve it gradually does not work from the banking sector’s perspective. In addition, the IdPs also share MSB’s perspective of the Board in need of increased competence in specific areas such as security (Product Manager Bank#1 17/03/2015).

5.5.3 Cooperation and dialogue

Several IdPs describe that from their point of view, the cooperation with the Board during the eGov eID introduction as almost non-existent (Product Manager Bank#1 17/03/2015; Product Manager Bank#3 17/06/2015). Without the exception of one official describing it as positive since it had indeed existed via different forums and working groups (Product and Process Manager Bank#2 19/03/2015). Hence, the Board follows the plan of eGov eID and only presents it for affected actors without them having any opportunity to affect it. This perspective is also confirmed when the Board fails to take improvements as suggested by the banks into consideration (Product Manager Bank#3 17/06/2015). Thus, IdPs describe that the Board actively tries to prevent market actors from influencing the eGov eID which in turn results in a solution that does not consider best practice existing on the market (Product Manager Bank#3 17/06/2015). “The fact that they [the Board] haven’t been receptive to our views from the beginning is a serious shortage. That they have listened but not taken to heart what we have said; this is absolutely a criticism of this work.” (Product Manager Bank#1 17/03/2015). Hence, the Board seems to have listened but not responded to any of the banking sector’s requirements, e.g. regarding the business and pricing model described above. Hence IdPs describe that they translate this behaviour of the Board as being forced to accept the eGov eID (Product Manager Bank#1 17/03/2015).

Another criticism perceives the Board as presenting the eGov in an incremental way. Hence, little by little the Board reveals the details of the eGov eID and as a result affected actors have a very hard time to assess the solution in its whole (Product Manager Bank#3 17/06/2015). Thus, being perceived as far from optimal, the cooperation and dialogue are also described as: “If one should change something that is already working just fine and you must talk to the actors that were there from the beginning; that is the biggest mistake they made.” (Product Manager Bank#3 17/06/2015). After the security analysis is performed in the fall of 2014, the IdPs perceive that the Board really seems to listen more to the arguments and critique forth (Product and Process Manager Bank#2
19/03/2015). Confirming the pressures put upon IdPs to accept and join the solution (Product Manager Bank#1 17/03/2015) the banks confirm that the Board exerted an increased pressure before summer 2015 to later be followed by the signing of final agreements to join the solution in September of 2015. However, any signing by the banks at this point in time would require conditions regarding the current outstanding issues (Product Manager Bank#1 17/03/2015). Diffusion and trust where put forth as extremely important aspects of the introduction of a successful eID solution and these aspects had not been handled in an optimal way (Product Manager Bank#3 17/06/2015).

5.5.4 Acceptance and trust

At the annual eID Day in 2015, a Chief Information Security Office (CISO) representing all seven banks of the consortium describes that member banks are very dependent of the eBanking eID (BankID) in their delivery of reliable and available digital services. The secure and cost efficient eID being one of the basic tenets of the BankID cooperation with ensuring identity as a central aspect. The rapid online development, as well as constantly changing threats, are important incentives for being both rapid and flexible in the continuous development of online security solutions. Further, the CISO states: “So, to preserve this confidence and our high level of security are crucial for us. It is essential for our business and a prerequisite for how we use [the eID]” (CISO February 4 2015). Hence, the perceived high level of confidence, trust and security of the BankID is a result of a positive diffusion and use as well as maintaining security at an appropriate level. The cooperation between the banks and the public sector is described as positive but any changes to it, as related to the eGov eID, will require thoughtfulness as well as thoroughness from the banking sector since the eID is seen as an extremely critical aspect of modern eBanking: “If something fails, it will have very serious consequences for us” (CISO February 4 2015). The banking sector still has a positive attitude towards a continued convergence with the public sector but emphasizes the importance of trust and confidence between the sectors. Further, IdPs have identified several shortcomings of the eGov eID not meeting their requirements such as user-friendliness and high levels of flexibility and security: “We are in favour of broadening the use of BankID to the [eGov eID] under conditions that it is done in a user-friendly way, we can have high flexibility and of course that it is secure.” (CISO February 4 2015). The dialogue between the Board and the banking sector is described as more intensified in 2014 but IdPs still not perceive the eGov eID as meeting their requirements (CISO February 4 2015).

However, the common perspective of a continued convergence between the private and public sector is still positive: “We want to continue to collaborate with the public sector to find good and working solutions that are developed continuously” (CISO February 4 2015, 2015). Hence, the aims is to solve all outstanding issues during 2015: “We are confident that we can find these solutions so we can join. It is our shared ambition that this will take place during the current year.” (CISO February 4 2015). The Chairperson of the Board continues to emphasize the positive aspects of this positive progress in the dialogue with the banking sector (Chairperson February 4 2015). Unfortunately, this
positive contribution to the eGov eID dialogue, describing the banks’ clear intention and willingness to continue the delivery of eID services to the public sector got misinterpreted and media reports that “The banks are joining the eID train” (IDG.se, 2015a). However, this media channel is immediately pushed to publish an official denial of this statement where the banking sector’s requirements for joining the eGov eID is clearly described (IDG.se, 2015b).

5.6 Concluding remarks

Besides presenting important empirical findings in the eGov case, this chapter provides the background and detailed problem context to serve as input to the coming actor and institutional analyses in Chapter 7 to 9. Based on the findings described it is clear that the indications of the challenges during the eGov eID introduction is confirmed. On the government level, the plan was set when the Board became operative in 2011 with the aim of an improved coordination, increased transparency and standardization of the new public sector eGov eID. Breaking the current oligopoly of banking sector IdPs and updating the expiring procurement model also being clear incentives. However, I argue that there are several crucial aspects of the eGov eID introduction severely underestimated by the governing (SOU 2010:104, 2010) as well as the Board. For example, underestimates several important aspects and takes establishing the eGov eID in practice and gaining acceptance from affected actors such as SPs and IdPs for granted. Since this is acknowledged much later during the introduction, these aspects turn out to be problematic to handle.

Moreover, the government starts to criticise its own legacy since the current convergence model is a result of a decision of principle taken by the government in the early 2000’s. Hence, with a positive development based on the synergy of aims and needs in the public and private sector as well as a strong diffusion and use among citizens and customers, the replacement of the Market eID posed a significant challenge in itself. In addition, the Board also faces a multitude of new obstacles along the introduction, and I argue that a significant part of these are clearly related to different existing and even contradictory views and translations of key aspects and consequences of the eGov eID as bound to specific organizational and actor based contexts. For example, the Board states that it is mandatory to join the eGov eID and that there is no possibility that the current IdPs (the banks) can continue to provide eID services to the public sector.

It later turns out that the accepting and joining the eGov eID is voluntary and bilateral agreements still being an option. As a first step towards analysing the eGov eID introduction from the socio-institutional perspective (see Section 4.4), Table 17 presents a summary of the comparison between the challenges of the eGov eID and the actual outcome of this process. These challenges are in turn based on the assessment of (SOU 2010:104, 2010) presented in Appendix 3. The challenge of failing to deliver an appro-
appropriate level of information security and personal integrity (1) as exemplified by the identification of the security risks that are acknowledged and results in the Board being given the assignment of performing a security analysis of the eGov eID. This also results in a number of recommendations put forth by MSB that forms the basis of the action plan to solve these issues as formulated by the Board. However, the outcome of the handling of this challenge clearly affects the introduction process in a negative way. Thus several SPs and IdPs translate this as a reason for not accepting and joining the eGov eID, in turn, use the security risks.

Table 17. Challenges and examples of outcomes of the eGov eID introduction

<table>
<thead>
<tr>
<th>#</th>
<th>Challenge</th>
<th>Outcome</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>The need of an appropriate level of information security and personal integrity</td>
<td>Security risks are identified by SPs and IdPs and acknowledged by the Board. A security analysis is performed resulting in an action plan as formulated by the Board</td>
</tr>
<tr>
<td>2</td>
<td>The need of establishing the eID model in current practice</td>
<td>The lack of local business perspectives indicated that the eGov eID is not sufficiently established in practice</td>
</tr>
<tr>
<td>3</td>
<td>The importance of cooperation and dialogue with affected actors</td>
<td>Several activities for cooperation and dialogue are initiated by the Board but still SPs, and IdPs reported a lack thereof</td>
</tr>
<tr>
<td>4</td>
<td>The identity providers will need to accept and join</td>
<td>The eGov eID is clearly not accepted by IdPs despite extensive dialogues with the Board</td>
</tr>
<tr>
<td>5</td>
<td>The service providers will need to accept and join</td>
<td>A very limited number of SPs accept and join the eGov eID</td>
</tr>
<tr>
<td>6</td>
<td>The incentives of the eGov eID model need to be accepted</td>
<td>Incentives of the eGov eID as acknowledged but not accepted by a majority of affected actors</td>
</tr>
<tr>
<td>7</td>
<td>The need for legal amendments to support the eGov eID procurement model</td>
<td>The System of Choice is successfully implemented in law</td>
</tr>
</tbody>
</table>
The outcome of the apparent lack of local business perspectives of SPs and IdPs took into consideration confirms the challenge of the lack of properly establishing or grounding the eGov eID in current practice (2). This in turn motivated by the lack of a broad acceptance and the critique put forth by SPs as well as IdPs hence, the main incentives of the eGov eID are not fully accepted. Even though the Board initiates several activities aiming at an increased cooperation and dialogue (3), several SPs and IdPs reports a lack of such initiatives in order to be able to influence the eGov eID as well as its introduction. As an example, the Board initiates the Governance Forum but exclusively for authorities that have already joined the eGov eID. In addition, several actors describe the existing dialogue with the Board as highly problematic.

The challenge of getting the IdPs as well as SPs to accept and join the solution (4 and 5) is confirmed by a majority of potential SPs still, have not joined the eGov eID. The major IdPs are not willing to consider the eGov eID as long as it does not meet their requirements regarding aspects such as security and flexibility. In fact, the majority of SPs joining have received clear instructions to investigate and consider joining the eGov eID in their government directions. Thus, among actors joining on a strictly voluntary basis, the uptake in the public sector is almost non-existent. This confirms the challenge of the incentives of the eGov eID not being fully accepted (6) by affected actors in public as well as private sector. Next, the Board successfully implements the needed amendment to public procurement law (7) with the System of Choice for the eGov eID hence, there are no longer any legal obstacles regarding eID procurement in the solution.

The challenge of failing to realize the eGov eID within the private market (8) is not handled by the Board at all. Moreover, this summary of challenges and outcomes is not only based on the plans or blueprint of the eGov eID but also on the actual work as performed by the Board under their awarded mandate. So based on the findings an additional challenge is identified as external directives (9) to represent any external regulations and directives directly or indirectly affecting the introduction of the eGov eID model. Exemplified by the EU-level eIDAS regulation and being a result of an increased interest in the eID within the EU. However, since still in its early stages the amendment
of this challenge is noted with the outcome of the need of the eGov eID to support the eIDAS regulation to facilitate cross border authentication.

Based on these findings, I argue that to be able to better understand the complex context of the eGov eID introduction, i.e. the inherent contradictions as well as the outcomes of identified challenges, a focus must first be put on the affected actors’ translations since the challenges and obstacles obstructing the introduction process are related to different actors’ perspectives of the eGov eID. Institutionalised aspects clearly affected this introduction as exemplified by the barriers of active resistance formed against the eGov eID, which in turn facilitates the coming analysis from the socio-institutional perspective. Further, one central finding from this introduction is the different constellations of actors translating and responding to the eGov eID in different ways which in turn strengthens the first stage of analysis as focused on actor networks. The central challenges presented above will serve as input to the translation analysis of the eGov case presented in Chapter 7 where they transform into central problem areas associated and negotiated by a selection of actors in a network.
6. The eHealth eID

This chapter presents the findings from the eHealth case focusing on the introduction of the eHealth eID. The background and context of this introduction are covered followed by a general description of this project. Next, two different perspectives on the introduction and its implications will be provided, and the chapter is concluded with identified challenges and examples of outcomes. Assessments are integrated throughout the chapter as an initial stage of analysis. Related to the first and second research question, this chapter describes the intra-organizational level introduction and resistance to the eHealth eID with clear relations to different actors involved or affected by this process. Identifying and describing the resistance and its implications during the introduction (RQ-1) as well as relating this resistance to different actors’ perspectives of the eHealth eID (RQ-2).

6.1 The Swedish health sector eID

6.1.1 The intra- and inter-organizational level

In contrast to the inter-organizational level of the eGov case presented in Chapter 5, the eHealth case provides the intra-organizational perspective on public sector eID introductions to this work. The described purpose of adding the health care domain as well as the intra-organizational level into this study is to benefit from any variations and similarities as provided by these different public sector domains and organizational levels (see Section 2.4.3). Although both cases focus on the introduction of eIDs in a public sector context, there are significant differences and a generative variation to consider regarding the eID contexts of these cases. First, aimed at authorities as service providers in the public sector, the eGov eID facilitates secure digital services (e-services) for citizens and businesses. This is contrasted by the eHealth eID aimed at health care staff to be used in their professional role to ensure patient security. The eGov eID safeguards an external digital service context for private use while the eHealth eID safeguards sensitive data in an internal digital service context. Second, the eGov eID turns out to be a voluntary solution for the public sector while the eHealth eID is strictly mandatory as enforced by law and regulations. Thus, accepting and joining the eGov eID can be subject to problematization while the eHealth eID leaves no room for objections or alternatives. Hence, the external pressure to introduce the eHealth eID put on organizations in the health care sector is undisputable and therefore to a significant extent left unproblematized in this work. Third, there are several clear differences between these two eID contexts for example regarding the concepts of acceptance versus resistance and use versus non-use. The acceptance and use of the eGov eID result in an authority integrating the eGov eID in secure digital services. Hence resistance and non-use results in an authority seeking other means and measures to fulfil its need of eID services. Regarding
the eHealth eID, acceptance and use correspond to more traditional concepts of ICT acceptance and use where acceptance will facilitate the proper use of the eID in a professional health care work context. In detail, use of the eHealth eID provides secure authentication to be able to access systems used in health care, medical as well as administrative. Non-use of the eHealth eID, on the other hand, therefore refers to not adhering to prescribed instructions with the result of the eHealth eID not serving its aim and purpose potentially risking patient security as well as individual users and the organization as a whole actively violating the law. Forth, security is an important factor and closely related to the eID. In the eGov case, security is predominantly described in relation to the level of security delivered by the eGov eID for example how it ensures non-repudiation, information security as well as handles online threats. In the eHealth case, it is assumed that the eHealth eID solution in itself is secure when meeting regulations hence, security is, therefore, focused on how different translations and resistance to the eHealth eID affects its prescribed security levels. Despite or rather thanks to their differences, I argue that these two public sector eID contexts supplement each other in a positive way providing valuable findings and new insights in the focused area of resistance to eID introductions in the public sector. Hence, together these two cases provide the empirical evidence needed in order to address the research questions (see Section 1.2).

6.1.2 Swedish health care

To be able to better understand the eHealth eID case, basic knowledge about the Swedish health care sector is required. Hence, this and the following sections will provide a brief overview of the health care model in Sweden, the emergence and current efforts in electronic health care (eHealth), relevant governing law and regulations as well as an overview of the eHealth eID solution. This background will, therefore, provide the basic incentives behind the eHealth eID introduction described in the remainder of this chapter. The responsibility of providing healthcare in the Swedish health care system is divided into the state, county councils or regions and municipalities. Health care in Sweden is regulated by the Health Care Act (Hälso- och sjukvårdslag) (1982:763) as well as specific regulations issued by the National Board of Health and Welfare (Socialstyrelsen) under the Ministry of Health and Social Affairs (Socialdepartementet). The state is responsible for health care on the political level; the county councils provide health care to citizens and municipalities have special areas of responsibility such as elderly care. Thus, health care in Sweden is provided to all citizens by a decentralized system mainly financed by taxes (SKL, 2015). However, for many years there has been a trend of privatization of the public sector also including health care. There are 20 county councils and regions responsible for health and social care, dental care and public transportation in their area of uptake (SKL, 2013a). These councils are governed by politicians, directly elected by the citizens of the county. The executive board manages and coordinates the work within the county and is financially responsible. There are usually a number of committees with different areas of responsibility responsible for the daily work within the county (SKL, 2013b). County councils, as well as the municipalities, are governed
by the Local Government Act (Kommunallag) (1991:900) but councils are also controlled by specific laws such as the Health Care Act (1982:763).

6.1.3 National eHealth

In 2005, a national executive committee for Information Technology (IT) in health and social care is appointed with members from Socialdepartementet, Swedish Association of Local Authorities and Regions (Sveriges Kommuner och Landsting, SKL), Socialstyrelsen, The Medical Products Agency, (Läkemedelsverket) and Carelink. The aim of this committee is to improve national cooperation regarding the use of IT in innovation and improvement of health and social care activities. While developed, the National ICT-strategy for health and social care (Nationell IT-strategi för vård och omsorg) has been well established with both SKL as well as the government offices. This strategy presents a common view of how to use ICT in the health and social care to meet current and future challenges acting as a support for business development on regional as well as local levels. Forming the committee and developing the strategy are therefore the first steps towards an improved nationwide cooperation regarding these aspects and issues (Regeringens skrivelse 2005/06:139).

This strategy is accepted and adopted by all country councils and regions as an important step for the further development of eHealth. To be able to further progress with the joint development of eHealth, an organization called Center for eHealth in Sweden (Center för eHälsa i samverkan, CeHis) is created to act as central ordering function with the company Inera AB acting as the provider (CeHis, 2006). Inera being a company with the aim of coordinating and supporting eHealth development is co-owned by county councils and regions (Inera, 2014a). In 2010 a new strategy is presented called National eHealth – the strategy for available and secure information in health and social care (Nationell eHälsa - strategin för tillgänglig och säker information inom vård och omsorg), hence the focus shifts from the creation of the basic eHealth infrastructure to the realization of eHealth (CeHis, 2010).

In 2013, two major organizational changes take place. First, the merger of Inera is a result of the partnership between CeHis acting as the customer and Inera acting as the provider needed to be changed resulting in these two organizations merged into Inera – County Councils and Regions in Partnership for eHealth (Inera, 2014b). Second, the eHealth Agency (eHälsomyndighetten) is created as suggested by an investigation focusing on the opportunities and obstacles in the health care sector. The investigation also puts forth the need suggests the need for stronger national initiatives managed by an appointed agency for coordination and development of the health sector ICT infrastructure (SOU 2012:33). Next, the government presents a proposal regarding the creation of this central coordinator with the aim of turning The Pharmacies Services Ltd (Apotekens Service AB) into a new authority for eHealth infrastructure (2012/13:128). Next,

84 A central organization for procurement of IT and related services in the health sector (later part of Inera)
regulations are issued by government further describing the role and function of this eHealth Agency (SFS 2013:1031). In the national eHealth area there are therefore currently two main coordinating actors responsible for delivering the eHealth infrastructure; Inera and the eHealth Agency.

6.1.4 *The Patient Data Act*

In 2003, it is decided that the relation between personal integrity and societal interests regarding sensitive information in health care should be investigated and regulated. The presented directive suggested the appointment of a special investigator to develop a proposal for a statutory regulation of national quality directories in the health and social care. Possible aspects are described as the type of information to be kept in the directories, the purpose of use of such information, control of access to the information as well as informed consent from affected parties. The appointed investigator will also take into account related aspects such as the Personal Data Act (Personuppgiftslag) (SFS 1998:204) and the European Parliament directive 95/46/EG ‘on the protection of individuals regarding handling of personal data and the free movement of such data’ or more commonly referred to as the Data Protection Directive (Dataskyddsdirektivet) (Dir. 95/46/EC)\(^{85}\).

This investigation is called the Quality Directory Investigation (Kvalitetsregisterutredningen) but the name later changes to the Patient Data Investigation (Patientdatautredningen) (S 2003:03). In 2004, the investigation’s mission is expanded to also include the handling of personal data in health and social care, and the proposal for an adequate and coherent regulation of that area is put forth (Dir. 2004:95). The investigation presents the Patient Data Act (Patientdatalagen) in 2006 (SOU 2006:82) and the final Patient Data Act (Patientdatalag, PDL) comes into effect in 2008 with an explicit aim of providing patient integrity, high quality and cost efficiency with respect to the patient’s integrity and restriction of unauthorized access to patient information (SFS 2008:355). Since 2008, measures to ensure the security of patient data in an ICT related context are required by law.

6.1.5 *National Board of Health and Welfare regulations*

The Regulations on Information Management and Record Keeping in the Health Care Sector\(^ {86}\) (SOFS 2008:14) are, together with the Patient Data Act, important parts when realizing the national eHealth strategy. These regulations are developed to clarify the responsibilities regarding the handling and journaling of patient information to caregivers, managers, health care staff and other executives. According to these regulations, the caregiver has a responsibility of keeping management systems to ensure quality and patient security by having a well-documented information security policy. The caregiver

\(^{85}\) A new EU data protection reform is currently being developed with strict consent requirements backed-up by huge fines and stronger enforcement.

\(^{86}\) Sv. Socialstyrelsens föreskrifter om informationshantering och journalföring i hälso- och sjukvården
must also ensure that the management system includes the processes needed to comply with the information security requirements. In compliance with the PDL, the National Board of Health and Welfare issues requirements for strong authentication when patient data is handled over open networks and in this context, strong authentication requires a minimum of identity control by two factors, by something you have (e.g. a certificate, smart card etc) and by something you know (e.g. with a password or a PIN-code) (SOFS 2008:14). These regulations thereby prescribe that strong authentication should be used in the health sector in accordance with current law.

6.1.6 The eHealth eID

Secure IT in Health and Social care (Säker IT i Hälso- och Sjukvård, SITHS) is a national solution for secure authentication of employees and contractors based on eIDs for secure authentication and encryption of sensitive information in a professional health sector context. The SITHS solution henceforth referred to as the eHealth eID, is a smart card based solution that provides a secure login to all national eHealth services. The eHealth eID serves as a professional identification for electronic as well as physical authentication by providing the prerequisites for a health organisation to adhere to the PDL regarding strong authentication to access national services like the National Patient Overview (Nationell Patientöversikt, NPÖ), pharmaceutical services and quality records (CeHis, 2013). By 2012, all county councils, regions and municipalities are connected together in this infrastructure (National eHealth, 2012). From the beginning of 2014, Inera is the sole coordinating organization of the SITHS solution due to the previously described organizational merger (Inera, 2013).

The eHealth eID consists of an eID certificate for private use and a SITHS-certificate related to the individual’s professional role. Strong authentication consists of the eHealth eID card and a personal PIN-code thus fulfilling the requirement for two factor authentication. Common forms of the eHealth eID are the company card and the SIS-card. In addition, there are several other forms of the eID for specific uses such as for protected identities and temporary cards. Depending on its introduction, the eHealth eID can be used in the following areas: system login, physical identification and electronic authentication for professional as well as private use, electronic signing, encrypted signing of emails, access control and secure printing (Inera, 2013). Hence, the eHealth eID (SITHS) is the only option offered to health sector organizations to be able to comply with laws and regulations regarding the use of strong authentication ensuring the appropriate level of information security for patient data.

---

87 Issued by Telia – a telecom company
88 A personal identification certified by the Swedish Standards Institute (SIS)
6.2 The project

6.2.1 Background

In this county council, the project to introduce the eHealth eID is initiated in 2012 and motivated by a decision by the county council director after pressure from the information security manager. This is seen as a positive decision to achieve the required security level when accessing patient data via the Electronic Patient Records (EPR) system in accordance with current regulations and law (Business specialist Central IT 08/10/2012, 2012). This top-level decision is also described as an effective means of legitimizing the eHealth eID introduction (Infrastructure specialist Central IT 17/09/2012). The aim of this project is to introduce the eHealth eID card across the organization to every potential user and at this time approximately 14,000 have been issued. The project team is acting on behalf of an appointed steering committee. Prior to this introduction, about 500-600 cards had already been issued to users. However, at this time the eID cards do not have any actual functionality (Infrastructure specialist Central IT 17/09/2012, 2012). The initial deadline for the project is set to February 2013 but the project deadline is later postponed on several occasions and finally set to mid-fall 2014 (Figure 20).

Figure 20. Introduction timeline

The introduction project has a very strong focus on time with the detailed track of the number of eIDs issued as well as health units covered during the process (Business specialist Central IT 08/10/2012, 2012). On a detailed level, the introduction is managed on health unit level with a stepwise progression across the organization. The strategy is also to address less critical units first which in turn results in more critical units such as

---

89 The county council provides community healthcare via local health care centres and specialist healthcare hospital clinics located in three different cities with national dental care. The hospitals are: the central hospital with, the county hospital and the smaller local hospital.
emergency clinics still awaiting introduction (Business specialist Central IT 08/10/2012, 2012). This decision is based on the extremely high requirements of emergency clinics. The introduction timeline presented in Figure 20 above covers the overall timespan of the eHealth eID introduction project is illustrated together with important national eHealth strategy milestones as well as the timeframe of this case study. Central IT, predicts the number of ICT systems being authenticated with the eID will increase in the near future together with a newly distributed Single-Sign-On (SSO)\(^90\) solution. However, in a longer time perspective, the use of a physical smart card for the eHealth eID may be challenged by it, as will be described, also introduces several problematic aspects that are specific to the health care sector. While the eHealth eID card facilitates authentication, it also introduces several new challenges and obstacles on technical as well as organizational levels that have to be handled to avoid any negative consequences. Further, the organization also anticipates that the eHealth eID will be a requirement for new ICT introductions hopefully acting as a lever and result in a less problematic use of the eHealth eID (Infrastructure and Security Specialist April 14 2015).

Nevertheless, there is still a positive attitude towards the future of the eHealth eID at Central IT and the continued development of the eID will hopefully improve the way it is used. As an example, a system for dose prescriptions of pharmaceuticals\(^91\) (PASCAL) has an explicit requirement for the eHealth eID and hence further facilitates and motivates the eHealth eID introduction (Infrastructure specialist Central IT 17/09/2012). The background and motivation of the eID as prescribed in laws and regulations is clear and will thus be left unproblematized. In 2012, CeHis, Apotekens Service and .SE\(^92\) form a joint initiative to design an identity- and authority federation for health care called SAMBI. A final report of this work is presented (Sambi, 2012), but according to this county council, this report is created without any significant grounding in practice. Further, with this kind of national eHealth identity infrastructure, there is also an inherent risk of introducing significant challenges regarding redundant solutions (Infrastructure specialist Central IT 17/09/2012). Being related to upcoming federated identity solutions in the public sector as well as the eHealth sector, some actors will have to will have to be members of both federations. Further, the health sector is planning to become an Identity Provider (IdP) as well as a Certificate Authority (CA). According to the county council, no one showed any significant interest in these types of issues a couple of years ago, but the significant increase in eHealth eID use has raised the awareness and interest in these matters (Infrastructure specialist Central IT 17/09/2012).

\(^90\) Controlling access to multiple ICT systems, the Single-Sign-On provides the single point of authentication and security attributes are then propagate among several systems.

\(^91\) Providing patients with medication in pre-packed bags

\(^92\) The Swedish Internet Infrastructure Foundation later The Internet Foundation In Sweden (Internetstiftelsen i Sverige, IIS)
6.2.2 Adhering to the law

The eHealth eID has been on this organization’s agenda for a considerable time. Prior to the eHealth eID introduction, the organization faces a Catch-22 problem. Previously, due to the lack of systems using authentication provided by the eID, no eHealth eIDs are issued. However, with no issued eIDs, systems cannot be adapted to the eID. Nevertheless, the organization decides to start issuing eIDs however in limited numbers in the mid 2000’s. Consequently, at this point, the issued eID cards lack any significant functionality due to the absence of system integration. This decision is therefore described as simply being a preparatory action in order to try and positively influence a continued introduction process (Infrastructure specialist Central IT 17/09/2012, 2012). However, it will take until spring 2012 before the work of introducing the eID across the organization is initiated. In this empirical context, there is also a clear distinction between issuing and introducing eIDs. The eID, as in this case, can be issued without being introduced, hence put to use for authentication purposes in an ICT-related context. Of course, another way around is not possible since this is a physical artefact. Thus, you cannot introduce an eID card that has not yet been physically issued. Two-factor authentication as provided by the eHealth eID as enforced by the PDL since 2008 hence this results in the organization violating the law for some four years.

This is also confirmed by Central IT with one official stating: “Well, we are actually breaking the law since the first of July in 2008. That applies to every county council and municipality and the private care givers too.” (Business specialist Central IT 08/10/2012). Accordingly, this rather late compliance with the current law regarding patient security and integrity seems to be a general problem in the Swedish health sector context with this particular organization being far from unique (Business specialist Central IT 08/10/2012). Although requirements and regulations for the eHealth eID are clear and undisputable, I argue that it is notable that there are only a limited number or larger health care organizations actively introducing the eHealth eID. Thus, the conformance regarding the eGov eID in the health sector as a whole must be seen as being far from optimal. Even if the final deadline for the introduction is met, this county council is therefore partially violating the PDL for over half a decade, in turn, risking patient’s security as well as integrity. Thus, on a general level, including the early preparatory work of issuing eID cards, the introduction of the eHealth eID will take approximately a decade to complete.

6.2.3 Preparatory work

When preparing for the eHealth eIDs, the issues at hand is mostly related to the setup of the technical infrastructure and procedures as regulated by the SITHS framework. Hence, at this time work is focused on following the national guidelines regarding the technical framework and setting up the necessary routines rather than introducing and gaining any real benefits from the eHealth eID itself. As a member of the national SITHS Management Team, the county council gets information and stays updated with other
county councils eHealth eID introduction efforts, although on an overall national level this development is described as being rather slow (Business specialist Central IT 08/10/2012, 2012). The intention of being part of this team also offers the opportunity of learning from other county councils in their development of related routines, but as it turns out: “Actually, we were the ones developing the routines at that time! We have been there from the start, but only one region and one county council have made more progress than us in their roll-outs.” (Business Specialist, 08-10-2012). This county council is a part of the national eHealth efforts for a considerable time, starting with the development of the eHealth strategy and later followed by being an early adopter of the eHealth eID. On one side there are positive aspects of being at the forefront of this new development in the health sector: “It is rather interesting being at the frontier of development and you experience all new problems as they occur.” (Business Specialist, 08-10-2012) However, on the other side, there is a clear downside of not being a follower with the missed opportunity to learn from the leaders and avoid mistakes: “You can not turn to anyone to ask: How did you solve this? We have to handle all the tricky issues – the others can just follow when we have the solutions.” (Business Specialist, 08-10-2012).

I argue that it is notable that there seems to be a recurring lack of inter-organizational communication and cooperation on the national level regarding SITHS-based eHealth eID solutions. This is also confirmed by the county council describing that this strategy is not managed centrally in an optimal way. There is, for example, a clear lack of a long term strategy and an open dialogue with actors introducing the solution which in turn causes a significant level of frustration; "It is crazy; we are all reinventing the wheel!” (Business Specialist, 08-10-2012). Hence, there are clearly missed opportunities and benefits that can be gained from mutual discussions of the outcome of the eHealth eID in practice. Examples of such topics brought forth are the added functionality of the eID card as well as specific support routines needed. With a rather weak central governance, it is mostly up to the individual county councils and regions themselves to decide about the introduction as well as the possible areas of application for their eHealth eIDs. Moreover, this lack of national strategy regarding the eHealth eID can also pose to be an obstacle in finding new and alternative ways and technology to facilitate electronic identification; i.e. the possibility of identifying eHealth eID solutions that go beyond the physical artefact of the eHealth eID smart card.

6.2.4 A rather unproblematic security solution

From an information security perspective, the eHealth eID seems like a straightforward way to adhere to the law. The information security specialist informs top management about these requirements which in turn results in the initiation of the project (Security Specialist Central IT 01/10/2012, 2012). One could then assume that security aspects would be a significant factor and strong driving force behind security solutions like the eHealth eID. However, this is not the case since these aspects seem to play a minor role
and only act as facilitators for initiating the eID introduction. Hence, from an information security perspective, the organization has no objections regarding the security aspects of the eHealth eID solution as long as the relevant law and regulations are met by the solution. Regarding the eHealth eID in practice, on the operational level, there are internal audits of the process of issuing eHealth eID cards and temporary cards (Security Specialist Central IT 01/10/2012, 2012). Hence, any other type of information security supervision, monitoring and audits are evidently lacking. The organization has an overall general security policy instead of an explicit information security policy. There are also very specific security guidelines regulating the different areas that exist in the organization. Hence, from an information security perspective, the eHealth eID is perceived as a security enhancing activity with its mandatory use and anticipated improvement in the protection of patient data (Security Specialist Central IT 01/10/2012, 2012).

To increase the security awareness across the organization, training sessions are held with a focus on the consequences of incorrect security behaviour. However, it is described that the county council faces major challenges to reach out across the entire organization with this kind of information. Nevertheless, it is deemed as very important to get the staff to really understand the importance of the security risks for example when one leaves their workstation without removing the eHealth eID card. However, the examples brought forth on these training sessions are mainly focused on consequences for colleagues when security is compromised rather than consequences and risks from a patient’s perspective (Security Specialist Central IT 01/10/2012). Therefore, I argue that the examples used in this context seems rather weak with regards to facilitating an increase in security awareness and behaviour among staff. Not by any means neglecting or downsizing the importance of avoiding negative consequences among colleagues but in this context, the benefits of emphasizing information security would be from the patient’s perspective since the eHealth eID is supposed to protect patient data. The use of these rather weak examples is symptomatic since there is no reported misuse of the eHealth eID card that has caused any significant harm or injury to patients (Security Specialist Central IT 01/10/2012, 2012). Thus, a view of the need of clear incidents and national publicity regarding the risks of neglecting security is also put forth. There is awareness of the need for stronger incentives to prevent the misuse of eIDs, from a legal as well as an information security point of view. Nevertheless, the organization more or less takes for granted that the eHealth eID will deliver on security when introduced in local health care practice.

6.2.5 An exploratory approach

Described in later sections, the introduction project shows several signs of having a very limited knowledge about the actual implications and consequences of the eHealth eID in health care practice. The identified challenges ranging from critical problems to the need for new and updated routines related to the eID are handled and solved on a case by case basis (Infrastructure specialist Central IT 17/09/2012) hence problem solving
during the introduction is made in an ad hoc or reactive manner rather than being based on a structured, proactive strategy. As first adopters, the organisation is not able to foresee these issues, and the handling of these challenges can also be seen as an exploratory approach. However, I argue that this strategy is quite noteworthy based on the significant size and limited timeframe of this project. Thus, I argue that the strategy of introducing the eHealth eID across the organization as quickly as possible does not fully comply with the applied exploratory reactive approach. Consequently, the introduction project faces several challenges that affect the timeframe negatively. Being an early adopter in a rather new field potentially adding to these challenges. In line with the eGov eID, the introduction of the eHealth eID seems to clearly underestimate the implications of the eID in practice. In addition, this introduction also faces the challenges of dealing with technical challenges of the eID and as first time adopters, experiences and knowledge about this process are described as limited.

6.3 The introduction

6.3.1 Purpose and aim

As it turns out, there are quite different perceptions and translations of the purpose and aim of the eHealth eID even in the project team at Central IT. With translations ranging from the eID as a secure identification: “Primarily, it means a secure identification. The focus of the SITHS solution is the certificate located on the eHealth eID card.” (Infrastructure specialist Central IT 17/09/2012) to mainly a means for fulfilling the legal demands: “[I]t has been a way to meet the Socialstyrelsen’s requirements for strong authentication.” (Security Specialist Central IT 01/10/2012). Although not likely affecting the introduction in any significant way, I still argue that the apparent absence of a shared official description of the basic incentives of the eHealth eID is still worth noting. However, there are clear benefits from having a more clearly defined common central project view of the eID to reduce or minimize the further spread of multiple translations of the eID in the organization. Moreover, as will be described in later sections, different translations of the purpose and aim of the eID are a recurring theme throughout this study. Hence, there is an imminent risk of clearly diverging translations existing on practice level that in turn potentially can affect the introduction in a negative way.

6.3.2 Communication strategy

As this case clearly indicates, communication is a very important aspect of an eID introduction. Regarding the eHealth eID, there are several formal roles assigned at the local level to facilitate the communication between the coordinating Central IT function and local practice at health care units such as health centres or clinics. As will later be described, one of these local roles is also assigned with a responsibility to facilitate the proper handling and use of the eID on an operational level. The Local Authorization Administrators (LAAs) are responsible for managing system related authorization at the local level, the local IT coordinators and IT Responsible persons (ITRs) are a resource facilitating ICT related issues as well as acting as a first line support towards the local
staff in health care units (Business specialist Central IT 08/10/2012). The communication regarding the eHealth eID between Central IT and the local practice of the organization has historically gone through the LAAs with several scheduled meetings a year. However, during the eHealth eID introduction, the communication channel shifts to be mainly between Central IT and the ITRs with the responsibility of forwarding the information to the local level. Still, this communication model is not entirely unproblematic since a lot of questions are raised locally and then forwarded by the ITRs (Business specialist Central IT 08/10/2012). Thus, weekly meetings are arranged to handle issues and problems deemed as critical but due to a number of reported issues; there is also a strategy of referring to the organization’s Intranet, asking users to find the answers themselves. However, this strategy is also affected by the extensive of information available through this information channel and acknowledged by Central IT stating: “There is almost too much information [on the intranet site], so there is a risk of not bothering to read at all instead.” (Business specialist Central IT 08/10/2012)

6.3.3 Multi-level complexity

Complexity seems to be a recurring theme when it comes to the introduction of the eHealth eID. It is described on several levels in organizational as well as technical contexts of the introduction. Given the fact that the organization has a high degree of heterogeneity, ranging from general to highly specialized health care and from stationary to highly flexible work situations, combined with the technical complexity of the infrastructure, the regulatory prerequisites (SITHS), technical as well as informational aspects of security and the eHealth eID solution itself (Infrastructure specialist Central IT 17/09/2012). This very high level of actual as well as perceived complexity is far from surprising since the eID needs to be integrated or interwoven into technical as well as organizational and social contexts to fulfil its purpose. Furthermore, the future development of the eHealth eID will most likely even result in an increase in the complexity of the infrastructure surrounding the eHealth eID with the new required supporting routines, referred to as an ecosystem (Infrastructure specialist Central IT 17/09/2012).

It is also a clear indication that this ecosystem will increase both in size, volume, diversity as well as complexity: “In a few years we will do the same things as today but with an increased volume. As long as we have the eHealth eID card, we will continue to develop services related to it.” (Infrastructure specialist Central IT 17/09/2012). Despite the clear possibilities and benefits of further development of the eHealth eID solution, the experiences from the introduction project so far also raise concerns about the increasing technical complexity affecting the overall maintainability of the solution in a negative way (Infrastructure specialist Central IT 17/09/2012). From an introduction perspective, the complexity has a direct impact on the progression of the introduction since unforeseen technical problems directly affect or even stops the entire introduction project on several occasions. These problems also directly affect users in a negative way.
and in some cases result in specific actions such as setting up dedicated servers for specific health care units to be able to trace and investigate the problems in a more controlled environment.

One could argue that these problems, as a result of high complexity, could have been predicted by proper investigations prior to the introduction but based on the sheer diversity of health care in general and this county council in particular, such a pre-introduction investigation would have been extremely time-consuming, costly and virtually impossible to carry out. Instead, the project team chose a strategy where the organization is divided into the following two categories based on their health care operations character: (1) the simpler units and (2) the more difficult units with the level of difficulty directly related to the level health care provided and the staff requirements of flexibility (Business specialist Central IT 08/10/2012, 2012). Accordingly, ambulatory health care such as local health centres, are put in the first category and emergency rooms in the second while inpatient health care such as hospital clinics are put somewhere in between.

6.3.4 The Estimated Benefits Strategy

The strategy of adding value to the eHealth eID is something described as central to the eHealth eID introduction in order to be able to gain an increased acceptance of the eID card in practice. This added value presents the users with opportunities of using the eID in other contexts and for other purposes than the primary ICT related authentication in their professional role (Infrastructure specialist Central IT 17/09/2012). Examples of such added benefits in professional use are the ability to use the eID for physical access, such as door and parking area access, secure printouts and physical identification, i.e. to use it as a traditional ID card. For private use, the ability to use the identity certificate on the eID in a private, public digital service context is emphasized. By using these added values as a selling point, Central IT is hoping to gain an increased acceptance and increase of the perceived value of the eHealth eID resulting in a more cautious and correct handling of the eID card in order to minimize security risks (Infrastructure specialist Central IT 17/09/2012). This is, in turn, indicating that incentives of adhering to laws and regulations as well as ensuring patient security have failed in terms of developing a common awareness among staff about these aspects. Nonetheless, Central IT is fully aware of existing workarounds for example when the eID card is left in the card reader resulting in, for example, the same eID being shared among several users and threatening security and integrity by exposing patient data (Business specialist Central IT 08/10/2012). Hence, this strategy for getting users to use and handle the eHealth eID correctly can be described as an Estimated Benefits Strategy (EBS), since these benefits are not based on any actual grounding in practice but are rather estimated and added to the smart card. Instead of trying to enforce strict compliance, the EBS is based on the creation of estimated benefits and value to transform how the eHealth eID is translated and handled in practice thus also linked to the institutional level of behaviours and actions. By Central IT, the outcome of the EBS is described as: “I think it is good because
it makes staff keep track of their cards and codes. They keep it safe and do not leave it. Soon they can not even park their car without the [eHealth eID, writer’s note] card. It is a good thing that it can be used for a lot of purposes.” (Business specialist Central IT 08/10/2012). However, despite being quite optimistic about this approach, Central IT also acknowledges potential risks such as an increased level of technical complexity and interdependency when integrating multiple uses and benefits onto one single eID card (Infrastructure specialist Central IT 17/09/2012). From a local users’ perspective, there are also clear negative aspects and risks when the eHealth eID becomes a carrier of a multitude of different functionality and uses. The most evident one being described as the ‘who is to blame’ dilemma. Thus referring to the difficulties in finding the responsible party for the specific functionality if the eHealth eID in some way malfunctions or fails (Business specialist Central IT 08/10/2012; Infrastructure specialist Central IT 17/09/2012).

However, I argue that this is far from surprising since the integration of multiple functions into one single physical artefact as the eID card tends to result in a hiding or black-boxing of the underlying functionality in favour of the physical item or carrier held in ones’ hand especially if it is presented in such a neutral way as a smart card. Central IT describes this as clearly related to a lack of understanding of the underlying technology such as the different certificates integrated on the card (Infrastructure specialist Central IT 17/09/2012). Moreover, I argue that this in fact results in the following intricate dilemma to be handled in the eHealth eID context; the organization strives for an increase in awareness of eHealth eID, but it is not realistic to assume that the practice will ever understand the purpose and significance of its constituent technical parts, different layers of certificates (cf. the hermeneutic principle in Chapter 2). The development of an understanding of the whole must by approached in a different way as exemplified by the EBS. One can also argue that all these added benefits described above are purely artificial since they are in turn based on pure estimates rather than performed investigations of existing needs.

6.3.5 Missed opportunities and reflections

Further, Central IT is fully aware of several missed opportunities related the introduction process of the eHealth eID. One being the missed opportunity of a positive project synergy with an organization-wide upgrade of hardware as well as software, workstations and operating systems (OS), henceforth referred to as the HoS-project (Hardware and Software project). According to tests, this upgrade would have significantly minimized several critical problems such as user session reconnection delays. Accordingly, an active coordination of these projects would, in fact, have had a significant positive impact on the eHealth eID introduction project (Business specialist Central IT 08/10/2012). Yet another missed opportunity between these projects is put forth describing the possible increase in user acceptance that could have been gained if the eHealth eID had been introduced in the wake of the HoS-project. With this approach, the new artefact, the
eHealth eID, could have been motivated and articulated to the users as strictly required by the OS upgrade (Business specialist Central IT 08/10/2012). However, not completely true, this could have been an effective lever in gaining the much needed increase in both compliance and acceptance towards the eHealth eID solution. Unfortunately, the HoS-project operates on a completely different timeframe and is progressing at a much slower pace. Hence, this potential synergy between the projects is not possible to gain in practice. When asked to reflect upon the introduction, an aspect brought forth by Central IT is the previously described downside of being an early adopter. Although it is interesting to break new ground and lead the way it would, in fact, have been much easier to follow and gain benefits from other county council’s experiences regarding introductions of the eHealth eID (Business specialist Central IT 08/10/2012).

As described above, the organization identifies different ways of handling the eHealth eID card issues, but one fact still remains; the technology involved is rather complex and expensive. As a result, technical as well as financial aspects influence the introduction of the eHealth eID which in turn is perceived as an aggravating factor: “It could have been much easier with more money and a different IT-infrastructure.” (Business specialist Central IT 08/10/2012). Another topic described is the project’s clear focus on time that results in a very stressful work situation for the project team members at Central IT. By progressing at a slower pace, the eHealth eID project could also have had better chances to realize the benefits of the HoS-project synergy described above (Business specialist Central IT 08/10/2012). When reflecting upon the incentives and motivators of the eHealth eID introduction, the following interesting view of the real cost of information security is described: “How much is the security worth? If you, for example, can not access patient data records; when it costs too much.” (Infrastructure specialist Central IT 17/09/2012) To me, this statement actually pinpoints one of the major challenges of introducing eHealth eIDs in the health sector; when the value of information security is set against the value of medical care and human health. Thus, existing workarounds are used to bridge the gap when the eHealth eID does not support medical operations in an optimal way. This can be a matter of the quality of health care provided suffering negative consequences as a result of the correct handling and use of the eID.

6.3.6 Known implications

According to Central IT, there are no technical issues with the eHealth eID cards per se (Business specialist Central IT 08/10/2012). The occurring problems encountered throughout the introduction process are therefore seen as strictly related to other technical parts in the described complex eID infrastructure as well as implications of the eID in practice (Infrastructure specialist Central IT 17/09/2012). For the average user, the eHealth eID setup is perceived as complex and most likely difficult to understand with the black boxed added functionality also being a part of this problem as previously described. When problems occur, the user often lacks the ability to identify the direct cause
of the problem and symptomatically lacks the knowledge of which part to hold accountable. This inherent complexity on the eID then becomes critical since the complex chain of technology must work together to avoid any further spread of misconceptions and dissatisfaction among the users: “Otherwise, they will throw away the card! I am not going to use this crap! It is too difficult!” (Infrastructure specialist Central IT 17/09/2012). Nevertheless, according to Central IT, there is a broad acceptance of the eHealth eID in general but if problems occur this can very easily turn into an increase in negative attitudes against it (Infrastructure specialist Central IT 17/09/2012).

Hence, Central IT is aware of user comments being very positive: “Some think it is great – they say - it is like having the EPR system around the neck.” (Business specialist Central IT 08/10/2012). However, there are also clearly negative perspectives: “Then there are those who think this is really complicated and very stupid.” (Business specialist Central IT 08/10/2012). There are even users that believe that the sole purpose of the eHealth eID card is to make things even more complicated for them (Business specialist Central IT 08/10/2012). Finally, one significant effect of the eHealth eID not working properly is described as an immediate impact on how users handle their eID cards. As an example, the recurring problem with long delays upon session reconnection (latency) has a direct impact on the users’ willingness to follow the instructions and remove their cards when they leave the workstation. With such an immediate impact, these kinds of cases are handled with a high level of attention at Central IT: “This must be resolved quickly since it results in users not removing their cards.” (Business specialist Central IT 08/10/2012).

6.4 The implications

6.4.1 Purpose and aim

In the previous section covering the project and introduction of the eHealth eID, it is described as a rather unproblematicized means for ensuring patient security in adherence to current laws and regulations. However, as the focus shifts from the introduction project to implications in practice of the eID, it becomes apparent that these two perspectives are clearly diverging. This, in turn, serves as an indication that translations of the purpose and aim of the eID from the project perspective (Central IT) are not successfully being transferred across the organization. As an example of these different translations of the eID existing in parallel on a different level in this organization, the following information conversation about the eHealth eID among staff at a local health centre as recounted by the Manager Health Centre#2 19/11/2012 (2012) is rather illustrating.
Although raised in an informal context, I still argue that this conversation clearly indicates how the information about the purpose of the introduced eHealth eID results in different translations by affected actors in the organization. To exemplify further, some typical statements characterized as different levels of views of the eHealth eID are compiled in Table 18. These can be placed on a scale between the polarities of ‘utter confusion’ to signify a complete lack of understanding of eID incentives and the state of fully understanding the purpose of ensuring ‘patient security’. Hence, the latter being fully in line with the official incentives of the eID as communicated by Central IT and in turn related to laws and regulations. Placed in between these two, the translation of the eID as related to ‘quality assurance’ is based on the notion that authentication and authorization, in turn, facilitates the correct high quality input to the systems. Finally, ‘authorize access’ is solely focused on the authorization process and ability to access the computer. Hence, it is worth noting that only one of these translations relates the eID to the aim of providing security of patients. Moreover, I argue that the eID does not on its own reach this goal but is merely one of several aspects, technical as well as non-technical such as the described conformance to prescribed use, working together to facilitate the positive outcome of securing patient data. This confirmed existing divergence among existing translations of the eID further strengthens the applied approach of focusing on actors’ translations and how these can be related to resistance appearing as institutional barriers with a potential negative impact on the introduction process.

Table 18. Different views of the eHealth eID

<table>
<thead>
<tr>
<th>Translation</th>
<th>Typical statement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Utter confusion</td>
<td>“I haven’t understood this yet. What’s the purpose? Why do we have it?” (Manager Health Centre#2 19/11/2012)</td>
</tr>
</tbody>
</table>
## 6.4.2 The introduction

The first health centre describes that are two key factors facilitating the eHealth eID introduction at the local level: (1) being an early adopter or pilot and (2) the ITRs. In addition, this particular unit receives the full attention from IT Center during the introduction (Manager Health Centre#1 05/12/2012). The first day of the introduction, a person from the project team is on site to help out which in turn is perceived as a very positive (Medical secretary Health Centre#1 17/12/2012). The crucial role of the ITRs is described as being able to actively inform the staff about why and how they shall use the eHealth eID, and the experience of being a pilot unit is described as overall positive. For example, the unit gains access to direct phone lines and the ITRs can identify possible problematic issues at an early stage (Manager Health Centre#1 05/12/2012). Since the ITRs know the local staff very well, on a professional as well as personal level, they can easily identify users in need of extra support. Moreover, this particular health centre is of a seemingly manageable size, with 20-25 persons, for this type of introduction (Manager Health Centre#1 05/12/2012). Describing problems at the time of the introduction, the significant time from the eID cards are issued until the actual introduction is put forth. As it turns out, this also results in all eID certificates becoming outdated and in need of updating (Medical secretary Health Centre#1 17/12/2012). One of the ITRs summarizes the introduction in the following way: “I think people thought it would be more difficult than it actually is. It seems like people really take responsibility for their cards.” (Medical secretary Health Centre#1 17/12/2012). The second health centre; a significantly larger unit with a work force of over twice the size of the first one, describes a more cumbersome introduction process primarily related to the size of the unit and an unfortunate coincidence in the project context: “You had to run around a lot the first week and show users how to use it, and there were a lot of emails. Most people learn, but some never do.” (ITR Health Centre#2 14/02/2013).
The unfortunate coincidence at the time of the introduction is related the described HoS-project that puts a very high level of strain on the ITRs. As it turns out, these two different ICT related projects actually result in no less than a threefold hardware inventory done completely manually. Thus, it comes as no surprise that these repeated tasks are described as extremely tedious and time consuming. From this health centre’s perspective, the main problem is the fact that they only receive information about one task per project at a time. Hence, these two projects are clearly not coordinated at all (ITR Health Centre#2 14/02/2013). As it turns out, a fourth hardware inventory is just being made related to an upcoming software upgrade (ITR Health Centre#2 14/02/2013) which in turn can act as a clear indication of a potential improvement in central ICT project coordination to possibly ease the stress and repetitive workload on local practice. This also motivated by one of the ITRs giving the following quite alarming statement about the working situation: “You do not have time to manage your normal job – these things take up too much time.” (ITR Health Centre#2 14/02/2013).

As a result, the workload on the ITRs resulted in difficulties in having the time to support local staff: “Usually, they [the ITRs] do not have the time, so you end up calling IT-support instead.” (Registered nurse Health Centre#2 07/06/2013). At the hospital clinic, from the manager’s perspective, the outcome of the eID introduction seems positive: “It went well, as I understand it. However, I’m very tolerant. I have heard of problems being investigated by the ITR, but for me personally, it works well.” (Manager Hospital Clinic 07/05/2013). However, this person is also aware of the risk of not having the complete picture of the introduction: “When you don’t hear anything you assume that everything is okay. So I haven’t even asked how it works, just assuming that it does.” (Manager Hospital Clinic 07/05/2013). However, from the ITRs perspective, there is a significant focus of the events that occurred in fall 2012 when severe access problems are reported associated with the eHealth eID in combination with access to the EPR-system.

The Operating Officer at the clinic urgently contacts the Chief Medical Officer at the hospital regarding these problems and very short after, the clinic receives the full attention of the support and IT Center: “The very next day a guy from IT showed up at the clinic, and they stopped the entire project.” (ITR Hospital Clinic 07/05/2013). As a result of this incident, the entire eHealth eID introduction project is temporarily stopped until these issues can be investigated further. By using powerful lines of communication, the problems at the clinic are able to affect the entire introduction project. The clinic then receives the full attention of Central IT and a dedicated server with updates and fixes rolled out in a very controlled environment (ITR Hospital Clinic 07/05/2013). The understanding among staff when facing similar problems is described as: “I understand that it has to be tested; that these things have to be tested in practice. It’s only then you’ll find out how everything works together and what’s affected. Is it affected when all users are logged in? However, at the same time, these issues really affect my working situation.” (Registered nurse Hospital Clinic 07/05/2013).
Other groups of professionals at this clinic, such as the nurses, also experience problems but seem to have been far more diplomatic in reporting about it, as opposed to the more urgent incident previously described: “It was a lot of error messages, and some had it worse than others. You had to try and login again and again and again because of these messages. Such things get really frustrating.” (Registered Nurse, 07-05-2013) At the time of the interviews, the Single-Sign-On (SSO) solution is being rolled out to simplify the login procedure mainly related to the EPR. Hence, the aim is to make the login procedure less cumbersome and improve the performance of reconnecting when re-inserting the card or switching between workstations. Accordingly, the SSO is introduced to solve problems but is actually caused new ones: “That’s when it got even worse! But they did something the other day, and it worked. Now I haven’t worked there in a while so I sure hope it works next time.” (Medical secretary Hospital Clinic 07/05/2013). Hence, the SSO solution is introduced to solve the most critical problems but also causes new problems as well as frustration at the hospital clinic. The testing of the SSO at the clinic is done in a similar way as the eHealth eID, by rolling out to what can be seen as a less critical part of operations: “It was tested at the clinic, and we tend to work normal office hours. However, it was not tested at the medical department, and they have very flexible working hours.” (Registered nurse Hospital Clinic 07/05/2013). However, the staff at the hospital clinic show a great deal of understanding of the eHealth eID related problems although a certain degree of dissatisfaction is still shining through: “You lose a lot of time when problems occur all the time, and one gets annoyed, and you think: ‘Why do they release these things when they aren’t working?’ I understand the cause, alright, but it doesn’t mean I like it.” (Registered nurse Hospital Clinic 07/05/2013).

6.4.3 Information security in practice

As previously described, the eHealth eID is seen as a straightforward security solution. Hence, it is interesting to find out how this unproblematic view of Central ID translates in practice. However, when it comes to the task of empirically investigating information security in practice, this is not the easiest of tasks since the practice itself can have difficulties in understanding the concept of information security, or as one respondent puts it; “It is very difficult to understand and grasp information security since you do not see the actual result of it” (ITR Health Centre#2 14/02/2013). Therefore, in this case, I chose to focus on the actions or non-actions that directly affect information security rather than the outspoken awareness and knowledge about it. With a multitude of ways to login into systems, facilitated by traditional logins or eHealth eID, voices are raised stating that it does not seem to exist any consistent strategy regarding the security measures taken (Manager Health Centre#2 19/11/2012). This being an effect of the preferred incremental approach of the eID introduction regarding ICT systems supporting the eID. Starting off with the EPR-system, there are still remaining systems that contain what staff perceives as very sensitive information but not requiring the eID (Manager Health Centre#2
Hence, this is translated as a divergence of how sensitive information in systems is protected. The importance of consistency is thereby emphasized in order to improve understanding and raise awareness about measures taken to ensure information security. For example by the eID card as required for all systems containing sensitive information instead of only a few. The use of the eHealth eID is closely related to the safeguarding of sensitive patient data as governed by law and regulations but nevertheless this inconsistency causes confusion and even a lack of understanding of security levels: “I’m receptive to information and want to learn, but right now it feels like we have a belt, seat belts and maybe one of those safety pins too.” (Manager Health Centre#2 19/11/2012). Thus, the main question being if an information security approach perceived as fragmented and inconsistent in practice can result in an over-confidence in security measures? Further, the consequences and risks related to the eHealth eID put forth by the respondents in local health care tend to focus on the negative consequences of the eHealth eID on a personal, professional level.

Aspects such as not being able to work without the eID card, having to report it to the police if lost or the extra fuzz of ordering and issuing a spare eID card is put forth (Medical secretary Health Centre#2 14/02/2013). This even creates a fear of misplacing it: “And I’m really scared of losing the card. When I did not remove it and arrived back at work in the morning, I thought; oh shit it’s still there! [sighs]” (Medical secretary Hospital Clinic 07/05/2013). Another effect of this fear of losing or misplacing the eHealth eID is related to where staff tend to store the card when not on duty. Since they are anxious about forgetting the eHealth eID, they often leave the card at work in some kind of a locked room. Even though the prescribed use is to keep the eID close at all times, this tendency is not seen as more problematic or less secure than keeping the eHealth eID at home (ITR Health Centre#1 13/03/2013). Hence, the intended handling of the eHealth eID, to treat it as a valuable and bring it home is a much rarer behaviour since this, in turn, introduces a new fear of leaving for work without it (Assistant nurse Health Centre#2 05/06/2013).

Regarding the problematic tendency of not adhering to the correct use of the eID and leave it unattended, one possible explanation can be traced to the two factor authentication since there is a tendency of perceiving the eHealth eID card as useless without having the proper PIN-code. Hence, this, in turn, assumes that this code is kept safe and not written down on paper or a Post-IT note (Manager Health Centre#2 19/11/2012). This is described by one respondent as: "Even though the [eHealth eID] card is still there, no one can access the computer in my name.” (Assistant nurse Health Centre#2 05/06/2013). As opposed to the fear of leaving the eHealth eID in the wrong place at the wrong time, such as at home when you leave for work, the single most problematic area is the wide spread and incorrect behaviour of leaving the eHealth eID in the right place at the wrong time. With this, I mean the neglect of keeping the eID close at hand at all times when at work, such as leaving it unattended in the card reader when you leave the
room. As it turns out, this behaviour is quite common; users tend to lock their workstations and leave the eHealth eID in the card reader. Talking to respondents about this behaviour is soon becomes clear that it can be interpreted as a norm developed and shared among colleagues. For example, one respondent shows a clear awareness of the risks but still leaves the card: reader: “Someone can take my card and use it for something else, but you don’t think about the consequences that way.” (Assistant nurse Health Centre#2 05/06/2013) and another said that just talking about it raised the awareness: “Anyone can go into my room and take it! When you put it that way, it’s a clear risk!” (Assistant nurse Health Centre#2 05/06/2013). During interviews, it also becomes clear that a tendency of neglecting instructions has developed through different phases over time: “At the beginning, there was a habit of trying to cover the card when left in the reader - it was like you tried to hide it. But now, if you take a look around you will find many cards lying around in unattended rooms. We are quite careless.” (Assistant nurse Health Centre#2 05/06/2013).

Even if leaving the eID card in the reader is a risk in itself, this behaviour can, in turn, pose an even greater risk if physical security to the health care facilities is low. Staff argue that if the eID card is left unattended in a locked room, there is a physical security factor minimizing the exposure to unauthorized persons. However, if the door is left unlocked or even open the risk becomes imminent. Nevertheless, it is reported that this really is the reality at several studied locations where the staff is accustomed to leave the room with an open door and the eHealth eID fully visible and accessible to anyone passing by (ITR Health Centre#2 14/02/2013). There are several potential reasons behind this very risky behaviour. First, the eHealth eID can be translated as strictly related to systems access (ITR Health Centre#2 14/02/2013) with the user lacking knowledge about the potential security risks. Second, there seems to be a correlation between the time you are away from your workstation and the tendency to leave the eID, hence the shorter the time away the higher the chance of leaving it: “One and a half, up to two hours; that’s too long to leave the card [unattended].” (Assistant nurse Health Centre#2 05/06/2013).

When asked about the difference between leaving the eHealth eID unattended for two minutes compared to two hours, one respondent said: “Then it’s unattended for too long, but that’s quite stupid – talking about it like that.” (Assistant nurse Health Centre#2 05/06/2013). Therefore, I argue that this clearly can be interpreted as a based on a current existing norm in the workplace resulting in unreflective behaviour. Negative consequences for the individual user thus seem to override the risk of not adhering to the information security guidelines and in turn risking patient data. On the one hand, this confirms existing norm among staff to neglect the prescribed handling and use of the eHealth eID if it results in negative consequences in the work situation. On the other hand, this behaviour also shows that an information security solution that lacks support for the work situation can never override the provision of health care. Thus, there are
clear challenges in introducing the eHealth eID as a means of increasing information security at practice level since staff seems unaware of the risks caused by misusing the eID card; a misuse that is silently accepted: “We don’t manage it properly from a patient security point of view.” (ITR Health Centre#2 14/02/2013).

6.4.4 Communication strategy

At the health care units, appropriate information is described as a key factor: “Good information is really the key here!” (Manager Health Centre#1 05/12/2012). However, communication about the eHealth eID is described as being a pure top down character and often having a very high degree of urgency (Manager Health Centre#2 19/11/2012, 2012). Thus, central directives regarding the eHealth eID are pushed out vertically across management levels of the organization mainly via mail. Regarding information about the eID introduction, one respondent recounts this information as: “From now on, everybody should have an eHealth eID.” (Manager Health Centre#1 05/12/2012). Another says: “I suppose this has been decided on a management level that this is the way it should be and we have no say about it.” (Medical secretary Health Centre#2 14/02/2013). Hence, these are clear indications of the information distributed by Central IT being focused on ‘what to do’ rather than ‘why it should be done’: “It’s always like that. This is how it should be done! From now on you should use this!” (Registered nurse Hospital Clinic 07/05/2013). Therefore, from Central IT’s perspective, all is well; the dedicated communication channels are used, mail and intranet, and the local ITRs have a key role in disseminating the information at local level. However, I still argue that local management, in fact, should also has a responsibility of getting the information correctly disseminated on the local operational level.

Moreover, this case shows several examples of local management having difficulties in translating the incentives of the eHealth eID as well as a lack of interest in the introduction. Therefore, I argue that this can be translated as lack of support on local management level having a potentially negative effect on how the eID is translated in general by staff. In addition, there is also a general tendency of being ‘negative by default’ to top management decisions in the organization (Manager Health Centre#2 19/11/2012) and this, in turn, can be an indication of some kind of existing norm or antagonism between local practice and top management. Further, there are also examples when an individual has the responsibility of pulling the information from different sources such as the intranet (Registered nurse Hospital Clinic 07/05/2013). This, in turn, being an indication of a strategy of delegating information retrieval at the local level: “But how shall we do this? That’s more or less up to you to figure out.” (Registered nurse Hospital Clinic 07/05/2013). Although this being a part of the described communication strategy formulated by Central IT to cope with the high communication levels during the introduction, with the responsibility of local information retrieval, or rather users informing themselves, comes an inherent risk of information not reaching the intended recipients (Registered nurse Health Centre#2 07/06/2013). As a result of the sheer amount and constant flow of information in the organisation, this is also a problem acknowledged
by Central IT. As a result, several respondents are uncertain of the information received about the eHealth eID (e.g. Manager Health Centre#2 19/11/2012) which in turn indicates that it should be taken seriously. Another important aspect when it comes to communication is the aspect of time since there seems to be a ubiquitous shortage of time between receiving the information about a particular change and the actual point in time from when this change will be in effect: “Because this tends to come quickly, you sense that something’s going on and then one day you have that mail in your inbox.” (Manager Health Centre#2 19/11/2012). Further, this strategy clearly counteracts with arguments put forth stating that actually takes considerable time between being informed about a specific change and actually accept and integrate it into the daily work (Manager Health Centre#2 19/11/2012); it is a process of progressive integration, understanding and acceptance taking place in the social context of a considerable amount of time. In combination with the tendency of forcing the timeframe thus results in an introduction that in fact leaves no room for the eHealth eID to be properly introduced and integrated on social and organizational levels. Since the introduction focuses on technical aspects, individual health care units are left to handle the social and organizational introduction of the eID. Further, due to its highly interwoven character in the technical as well as organizational and social context, the eID might be even harder to integrate compared to ordinary ICT related artefacts, information systems in general. In addition, the close relation to information security can also prove to be a barrier to diffusion of information. Nevertheless, there are examples of local practice in some cases acting responsibly and taking the time to inform staff in face to face meetings: “It was the ITR who informed about the introduction and made it very clear. The information was great, and it was presented in a very clear way. This is the way we have to do it.” (Assistant nurse Health Centre#2 05/06/2013).

6.4.5 An inflexible artefact in a flexible context

As previously described, the eHealth eID offers a very limited flexibility since it must be handled according to the instructions to fulfil its purpose. Hence, health care organizations tend to be very heterogeneous often requiring a high level of flexibility in order to provide the best possible health care. However, at the same time, these organizations are also professional bureaucracies bound to strong structures such as rules, hierarchies and authorities. Thus, the challenges of introducing this kind of inflexible artefact in a flexible, heterogeneous and bureaucratic organizational context become apparent. As it turns out, the single most reported negative aspect of the eHealth eID card, in this case, is the requirement of removing the eHealth eID from the card reader when leaving the workplace. However, the reported obstacles of adhering to this requirement can also be related to technical problems occurring at the beginning of the introduction when reinsertion of the eID card into the card reader resulted eID resulted in considerable reconnection delays. This in turn causing negative consequences for medical as well as administrative staff (Manager Health Centre#2 19/11/2012). This behaviour, previously described as linked to an unawareness of information security aspects of the eID is also described as: “With a full schedule and a lot of patients to handle every day, you can not
The eHealth eID

spare the extra time of removing the eHealth eID card every time you leave your workplace.” (Assistant nurse Health Center#2 05/06/2013). Another aspect motivating the notion of perceiving the eHealth eID as an inflexible artefact is the introduction strategy chosen by Central IT. Hence, by focusing on introducing the eID at less critical health care units with lower demands of flexibility, with a higher degree of stationary work, this problem is acknowledged by Central IT but not addressed until later with the introduction of the SSO solution. Nonetheless, I argue that it is fully logical to assume that these significant delays associated with the card removal in fact initially sparks, or even evokes, the existing workaround of not removing the card; a quite risky deliberate non-action with negative implications on information and patient security. As previously described, this accepted normative behaviour proves to be difficult to manage and possibly change in a health care organization since it in a way has a significant different objective: “You have your own dedicated workstation but nevertheless you have to move around a lot, and the priority is taking care of the patients.” (Assistant nurse Health Centre#2 05/06/2013). Therefore, I argue that the aspect of flexibility is just one of several potential challenges that occur when trying to introduce a standardized ICT artefact, such as the eID, in a critical and flexible organizational context such as the health care.

Especially when the prescribed use of this artefact counteracts with the aims and goals of this organization. Moreover, since it negatively affects the flexible working situation, users are very alert regarding eID problems and especially the ITR noticed even the slightest differences in reconnection times of the SSO solution (ITR Health Centre#1 13/03/2013). Therefore, this is a very critical factor that immediately can affect the use and attitudes towards the eHealth eID as well as the reported support cases relating to the eHealth eID solution. A current trend across the entire health care sector indicates that about 50 percent of the staffs’ working time is spent on technology and administration leaving only 50 percent of the time to spend on patients and medical care. Hence there should be a great potential for time saving innovative solutions in this sector that also would be of great socio-economic value (Manager Health Centre#2 19/11/2012). On the other hand, this tendency can also explain some of the staffs’ negative attitudes towards the eHealth eID; it is an additional thing, a new thing that increases the already too high level of administrative tasks: “The only downside is that it’s an additional step that decreases the patient’s contact time. You’ll get less time for patient related work.” (Physician Health Centre#1 17/12/2012). Hence, one of the key issues here is how the eHealth eID solution can be developed further to offer a better fit for the special characteristics of the health care organization or as one respondent puts it: “You must be able to use it as swiftly as you do at the supermarket.” (Manager Health Centre#1 05/12/2012).

6.4.6 The Estimated Benefits Strategy

The efforts of creating an added value associated with the eHealth eID that in turn is based on estimates about the practice are previously described from Central IT’s perspective. Since Central IT seems very confident and convinced that this is an appropriate
approach facilitating the correct handling and use of the eID. However, I argue that the main question regarding this effort still remains; how did these estimates about creating a valuable eHealth eID really hold up when scrutinized by local practice? As pointed out by Central IT, the identity certificate for private use integrated on the eHealth eID should be perceived as beneficial for users as well as the opportunity of using it as a physical id-card. However, one of the respondents almost immediately questions this approach by saying: “I suppose it’s good, but I won’t bring it when I’m not working. It’s strictly related to my professional access in an IT environment!” (Manager Health Centre#2 19/11/2012). This being a typical example of one of the possible dilemmas of this chosen approach; why try to integrate the professional and private domain in this specific context when these two are clearly separated in other contexts? In confirmation one respondent also stated: “You can use it privately but it’s not okay – the card belongs to my work.” (Assistant nurse Health Centre#2 05/06/2013).

As it turns out, only one of all respondents (19) actually uses this feature of the eHealth eID: “It was great because I’ve not gotten around to testing those digital services. So I thought to myself, I have to test it, and it turned out great!” (Medical secretary Health Centre#1 17/12/2012). Another development of the eHealth eID discussed when it comes to integrating additional functionality is physical door access. This functionality of acting as a key to restricted areas will obviously have different kinds of impact on the studied health units where the two local health centres still use normal keys and the hospital clinic has a separate door access card. However, the respondents’ views of this added benefit of the eID card seem to vary quite a lot ranging from highly positive: “That would be great. Then you would only have to keep track on one card.” (Assistant nurse Health Centre#1 17/12/2012) to very negative: “No, no, and enough! I run around all the time, and a specific room must always be locked. Then I’ll have to remove my damn card as soon as I have to access another room. I actually don’t know how many times an hour. I have a stationary work, but I’m always running around.” (Medical secretary Hospital Clinic 07/05/2013). Meanwhile, ITRs struggling with users not removing their eIDs, in general, welcomed this development (e.g. ITR Hospital Clinic 07/05/2013). However, according to one of the ITRs, this strategy of pairing the eHealth eID with physical access to locked areas is seen as a quite drastic but at the same time effective approach: “They will be locked out of their rooms. They will leave the room as well as the card in the reader but hopefully, they will adapt quickly.” (ITR Hospital Clinic 07/05/2013). However, since these things always tend to obvious and unproblematic on a conceptual level judging from some of the respondents; people almost always find their own ways around things that are considered to be too cumbersome or time consuming or as a medical secretary put it: “But then there will be many doors left open instead. I don’t know if that’s actually better. All doors will be left open!” (Medical secretary Hospital Clinic 07/05/2013). Hence, this person argues that if the door access is introduced on the eHealth eID, this will most likely result in staff leaving the eHealth eID in the reader as well as leaving their doors open which in turn will be a significant
decrease in security levels. Nevertheless, there are still respondents who say that they are positive towards a higher level of integration of functionality on the eHealth eID (e.g. Assistant nurse Health Centre#1 17/12/2012) and there are even ones saying that they have an interest in the private use of the eHealth eID but also points out that this topic has not been focused on the information (Registered nurse Health Centre#2 07/06/2013). Hence, the approach of trying to add value to the eHealth eID card seems to be a relevant approach but in this case I argue that the process of trying to create this value suffers from a clear discrepancy in perspectives since the estimated value, e.g. the private use, differs from the actually preferred value as translated and perceived by local practice, the professional use. Hence, with the ESB, Central IT has to work backwards by actively trying to convince local practice to accept the pre-formulated added value.

6.5 Concluding remarks

A similar approach as in the eGov case (see Chapter 5) is applied where a number of challenges are identified and related to examples of the actual outcome of the eID introduction are summarized and in turn, will be used as an input to translation analysis performed on the eHealth case in Chapter 8. However, unlike the ones related to the eGov, these challenges are numbered in sequence for practical reasons hence not based on any kind of structured assessment. A summary of these challenges is presented in Table 19. Local health centres turned out to be a better fit for the eHealth eID due to less complexity and fewer demands for flexibility (1). This indicates organizational heterogeneity and special requirements, for example, regarding flexibility to be important factors that affect the introduction. Further, introduction at critical care units such as the emergency unit are postponed indicating the Central IT wanted all possible problems to be identified and solved until critical units are approached. Thus complexity also refers to the technological challenges (2) encountered during the introduction such as reconnection delays that in turn negatively affects the process on several levels, e.g. by postponing project deadlines and introducing additional obstacles in medical staff daily work routines. Management has also introduced a clear challenge in the form of the estimated benefits strategy that did not turn out as expected (3). Thus there are indications that these challenges, in turn, result in a development of resistance to the eHealth eID itself (4) since hardware and software problems put negative stress on users on several occasions. In addition, this case shows that there are examples of current medical practice conflicting with the prescribed use of the eHealth eID that resulted in a misuse, e.g. by leaving the eHealth eID unattended that in turn also is evidence of affected actors not accepting it (5). Finally, there is a lack of knowledge and understanding of the motives and purpose of the eHealth eID that in turn could be seen as a result of these issues not being communicated in an optimal way (6). Although some affected actors are fully informed, others perceive the eHealth eID as a problem thus did not acknowledge its purposes as related to an increased security level.
Table 19. Summary of identified challenges and examples of outcomes

<table>
<thead>
<tr>
<th>#</th>
<th>Challenge</th>
<th>Outcome</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>The organizational complexity and heterogeneity will prevent the eHealth eID from being successfully introduced</td>
<td>Medical units with a higher request for flexibility report that the eID negatively affects their working routines</td>
</tr>
<tr>
<td>2</td>
<td>Technological complexity will present challenges and problems</td>
<td>Technical problems such as reconnection delays (latency) affect the eHealth eID introduction negatively on several occasions</td>
</tr>
<tr>
<td>3</td>
<td>Management may affect the eHealth eID introduction in a negative way</td>
<td>The estimated benefits strategy of the eHealth eID did not work as expected and in turn negatively affected the attitudes towards the eHealth eID</td>
</tr>
<tr>
<td>4</td>
<td>If the introduction becomes problematic the eHealth eID itself might negatively affect the introduction</td>
<td>Technical problems of the eHealth eID such as outdated certificates put stress on staff during daily work and in turn create negative attitudes to the eID</td>
</tr>
<tr>
<td>5</td>
<td>Current practice at operational level might prevent the eHealth eID from being accepted and used</td>
<td>Medical staff did not handle the eHealth eID according to instructions</td>
</tr>
<tr>
<td>6</td>
<td>Lack of knowledge and communication will affect the introduction negatively</td>
<td>There is a clear lack of understanding and knowledge of the motives behind the eID</td>
</tr>
</tbody>
</table>
7. Translating the eGov eID

This chapter presents the translation analysis of the eGov eID introduction as motivated by the applied theoretical and analytical perspectives (see further Chapter 3 and 4). By perceiving the introduction as a network of actors, this analysis focuses on the perspectives of these actors as well as relationships between them. This brings an increased level of understanding of actors’ translations, their causes and originating contexts, as well as implications for the network as a whole. The previously described different stages of the analysis (see Section 4.3.4), will be covered with important findings presented throughout the path. The chapter ends with a summary of the outcome of these stages to be further synthesized with the institutional perspective in Chapter 9. This chapter addresses the first part of the second research question (RQ-2) where actors’ translations are related to resistance by applying the approach of translation analysis on the national level eGov eID case.

7.1 Problematization

The problematization (Callon, 1986) focuses on the identified challenges and obstacles of the introduction of the eGov eID. As first presented in the report (SOU 2010:104), the assessment of this plan shows eight potential challenges with different levels of probability and potential impact on the introduction process (see Appendix 3). The outcome of the introduction, as described and grounded in empirical findings presented in Chapter 5, confirms these challenges as having a significant negative effect on the eGov eID introduction (see Section 5.6). Thus, I consider these validated challenges as the result of the first stage in problematization. As a result of the outcome of the introduction, an additional challenge (external directives and regulations) is added motivated by the fact that this aspect is not been emphasized to any greater extent neither by the report (SOU 2010:104) nor by the Board, but still seen as very relevant as exemplified by the eIDAS regulation prescribed with a mandatory conformance. To integrate these identified challenges into the translation analysis to be used as the starting point for the problematization, these challenges has to be transformed into problem areas. This will enable the identified network’s general aims and obstacles to be further elaborated and problematized. Furthermore, in a later stage of this process, each participating actor will be assigned with the appropriate set of obstacles or problem areas as well as aims and incentives for participating. Hence, this will enable the identification of each actor’s own path as related to opportunities as well as obstacles along the path of the introduction. The challenge of delivering an appropriate level of information security and personal integrity (1) is categorized as clearly related to the problem area of Security and trust. Thus, being based on the notion that providing appropriate security and trust levels will in turn minimize risks as well as facilitate the correct handling of sensitive information.
The need of establishing the eGov eID in current public sector practice (2) is, together with consequences preventing IdPs as well as SPs from accepting and joining the eGov eID (4, 5), categorized as a problem area clearly related to Current practice. The importance of cooperation and keeping an active dialogue during the introduction (3) is categorized as Cooperation and dialogue and the incentives of the solution as related to acceptance (6) is categorized as a problem area related to the eGov eID itself. Finally, the challenge of amendments to public procurement law (7) and external directives (9) are left unchanged, i.e. categorized as Public procurement and External directives. Therefore, based on the empirical findings in Chapter 5 indicating that the introduction had not focused on the private market eID, the realization of the eGov eID within the private market (8) is removed from any further analysis since it lacks any efforts in practice. The following six problem areas\textsuperscript{93} are categorized as based on the outcome of challenges in practice:

\begin{itemize}
\item Security and trust
\item Current practice
\item Cooperation and dialogue
\item eGov eID
\item Public procurement
\item External directives
\end{itemize}

7.2 Interdefinition of actors

The interdefinition of actors (Callon, 1986) (see Section 4.3.4) starts with identifying the main actor of the network being formed hence in the eGov eID case this role is assigned to the Board coordinating and leading the introduction. Based on empirical findings regarding the Board’s efforts and the outcome of the eGov eID introduction, the following three actors are considered as strong candidates to be added to the network of this translation analysis: the eGov eID, the Service Provider (SP) and the Identity Provider (IdP). Motivated by their key roles during the introduction in turn validated by empirical findings. Needless to say, the eGov eID is the first of the three key actors selected due to its key role and intended impact on the public as well as private eID area. This also facilitated by opportunity to treat human as well as non-human actors as equals during the analysis. Second, the Service Provider (SP) is selected as represented by a major Swedish authority often described as being a leading example of a successful eGov actor with a significant share of the total volume of public sector eID authentications in a digital service context. Hence, the assumption is that without the support of

\textsuperscript{93} The ordering of these problem areas has no significance regarding priority but is a result of the order these challenges are identified in (SOU 2010:104).
leading authorities in their roles of providers of digital services using the eGov eID for authentication, the solution will lack a digital service context thus most likely be a failure. Third, the Identity Provider (IdP) has an equal critical role to play in the network that in turn is quite straightforward: without any IdPs there will be no eID services for the SPs to integrate and use in their digital services. Given the fact that there is currently only one dominating eID in the Market eID solution, BankID, the acceptance and joining of related IdPs becomes extremely crucial. Since this actor empirically is represented by respondents from several banks, the IdP featured in this network is not a unique actor or organizational body per se but rather becomes the spokesperson for the three leading commercial banks providing BankID. Without the acceptance and support of the SP and the IdP, the network with the aim of successfully introducing the eGov eID will most likely not succeed due to the lack of digital services as well as eID services. Therefore, the success of the eGov eID depends on keeping the SP and IdP within the network together with the non-human actor of the eGov eID and successfully negotiating towards its common goal. This formed network around these selected actors will be the focus of the following analysis but first these identified actors will need to be further elaborated.

7.2.1 eGov eID

The eGov eID is described as the next step in further developing the highly successful existing Market eID for use in the public sector. The new version will provide a setup where the Board is responsible for coordination and the future development of the eGov eID infrastructure consisting of different frameworks regarding technology and regulations. This also resulting in a new way of procuring eID related services in the public sector with the Board acting as a central signing party for agreements with the IdPs which in turn will have to be approved by the Board to be able to join the solution. The SPs, i.e. public authorities using the eID in their digital services, will be signing central agreements with the Board acting as a proxy. On a general level, this solution is motivated by incentives such as simplifying agreements and the technical integration and management of eID services in public sector digital services as well as creating an identity federation coordinated by the Board to manage common registers and central functions. Hence, the main argument is that the eGov eID will make the use of eID services in public digital services much easier and in turn hopefully have a positive effect on the development of public digital services. However, as it turned out, there are clear indications of these basic tenets not fully converging with the perspectives of current SPs and IdPs as exemplified by a reported lack of grounding in practice and identified security risks. This makes the eID as an actor very crucial for the potential success of the network with its inscribed opportunities as well as identified challenges.

7.2.2 Service provider

The Service Provider (SP) is represented by an authority described as a major public sector digital service provider in Sweden. Representing the largest target group of actors in the eGov eID solution also consisting of smaller actors such as municipalities as well
as county councils and health care regions. In terms of resources for digital service development, the major authorities are way ahead, but in terms of numbers, these smaller actors are in the majority with over 300 individual actors. Hence, in the translation analysis, the selected SP can also be seen as a spokesperson for other public sector actors acting in a similar role. However, there are several differences between this actor and other types of public sector actors in terms of resources and competence. Apart from being a leading public sector digital service provider, this actor is selected based on the fact that this authority is one of the strongest advocates of the eGov eID delivering a sufficient level of security as well as not negatively affecting the authority’s development and provision of digital services. Hence, I argue that this authority in its role of actively resisting to accept the solution, stressing that it should at least deliver the same level of security as the current Market eID, makes this actor an ideal candidate due to the engagement and persistence in ensuring that the new solution delivers in terms of security; a rather obvious aspect in a security solution such as the eGov eID. From the Board’s point of view, in order to succeed in introducing the eGov eID among public sector actors, it is not only about making it easier for potential and new SPs but to keep the current and knowledgeable ones satisfied, confident and aligned within the eGov eID network. The report (SOU 2010:104) also clearly states that the introduction shall be done in close cooperation with affected actors but empirical findings indicate otherwise. Hence, I argue that bringing one typical example of an affected as well as a concerned and knowledgeable actor into the network will be crucial to reflect the existing obstacles and controversies in practice.

7.2.3 Identity provider

The new infrastructure and setup for the eGov eID will not be operative without the support and participation of external market actors in their role of Identity Providers (IdPs). This is acknowledged by the report (SOU 2010:104) as well as the Board itself. In an effort to break the monopoly or oligopoly of the banks as IdPs, the Board reassures that the eGov eID will be fully available for any new IdPs aiming at becoming a part of the new solution. In addition, the Board will also take on the role of approving and sign agreements with new IdPs. However, during the introduction of the eGov eID, it is very difficult to see any new IdPs entering the market reaching the same level of acceptance, trust as well as diffusion and use as the dominating eID as provided by the banks. So, the choice of bringing the IdP into the network, as a representative of the three leading commercial banks providing the BankID, is based on this actor’s very crucial role in realizing the goal of reaching a fully operative and working eGov eID solution. As acknowledged in the report (SOU 2010:104) as well as by the Board, empirical findings of the current problematic state show that getting this actor to accept and join the eGov eID is, in fact, a serious undertaking. Hence, I argue that this outcome clearly diverges from the rather unproblematized plan of getting current IdPs to join the eGov eID which in turn highly motivates bringing the IdP into the formed network. This actor then acts as a spokesperson for the commercial banks, as members of the consortium, providing current Market eID services (BankID). So, at this time, if the Board will not manage to
convince this actor to accept and join the solution, the eGov eID will end up being an eID solution without any eID services to offer.

### 7.3 Obligatory Passage Point

#### 7.3.1 Formulating the OPP

Based on empirical findings, it is clear that the Board is highly dependent on keeping the eGov eID, SP and IdP within the network with the common goal of successfully introducing the solution. The aim of the network is formulated as an Obligatory Passage Point (OPP) (Callon, 1986) (see Section 4.3.4). This OPP must be successfully negotiated in order to achieve the goal of the network, the successful introduction of the eGov eID across the public sector. Thus, the process of managing and delivering the eGov eID programme is highly dependent on the successful introduction of the eGov eID and its related aspects as well as the SP’s and the IdP’s acceptance and willingness to join the solution. From the Board’s perspective, the central governing question is therefore formulated as:

| Is the eGov eID going to be successfully introduced? |

Illustrated in Figure 21, considering this question to form the OPP of the network, it also becomes clear that to be able to successfully navigate through this passage point and reach success. There are also clear individual relationships between each of the partaking actors and the OPP which in turn means that each of these actors’ individual perspectives must be acknowledged and negotiated by the Board with a successful result. These actors are also clearly interdependent; individually they cannot accomplish this alone. For example, the Board can not introduce the eGov eID without considering the eGov eID itself and the affected actors and without the participation of the SP and IdP the solution will lack usage in digital services as well as eID services altogether (Figure 21).
So, it will be highly unlikely for the Board to be able to gain acceptance for the eGov eID from current and future SPs as well as the current and future IdPs without some kind of acknowledgement of these actors’ perspectives, communication and negotiation. Figure 21 also clearly illustrates that each of the actors within the network has its own path to follow as illustrated by the arrows linking each actor to the OPP. However, each actor is in turn surrounded by its own translations and beliefs of the eGov eID as forming the basis for their individual perspective of the route leading to the OPP as well as how the OPP itself should be negotiated successfully from their perspective.

7.3.2 Problematizing the OPP

If reality would be as straightforward as illustrated above there are no obstacles or problems on the road towards the OPP. Needless to say, this is not the case in the eGov eID case. The OPP paths of each actor, therefore, needs to be further problematized. Based on the previous problematization, each of the formulated problem areas is associated with an actor and placed along the corresponding OPP path. Hence, this is also the act of mapping problem areas to relevant actors while still perceiving the network from the main actor’s perspective. The problematization of the OPP is also expanded with individual goals for each actor to further emphasize the need of taking each individual actor’s perspective into consideration. For the eGov eID, the goal is formulated as aiming at an operational eGov eID in line with the main goal of the network as a whole. However, for the SP and IdP, the goals are formulated as continuing doing business, as usual, to be able to continue to provide secure digital services for citizens and businesses and provide eID services for the public sector. So, in a way, one already senses significant challenges ahead since the eGov eID should be introduced while keeping eID business as usual for the SP and IdP. The problematized OPP is illustrated in Figure 22 where each of the three actors’ paths is further problematized by associating the each with
relevant problem areas as derived from the identified potential challenges of the eGov eID. These further problematized OPP paths will be further described in the following sections.

![Diagram of OPP problematization - Obstacles and goals of actors (adapted from Callon, 1986)]

7.3.3 eGov eID

Since the eGov eID is a security solution, it has to deliver on security and trust (1) at least on an equal or preferably higher level than the current Market eID. Information security is also put forth in the report (SOU 2010:104) as one of the critical aspects of the eGov eID, and empirical findings confirmed that this indeed is a very critical aspect of the eGov eID introduction. Trust, in different forms and on different levels, is an equally critical and central aspect of the security solution. For example, the trust in the issued identity and service providers to supply services for the eID to be used in. The trust of citizens and businesses to actually use the eID in their online actions also being important. Regarding eIDs, trust is most commonly referred to as identity assurance, the assurance or trust in the correctness of the identity, and categorized by different level of assurance (LoA) levels. According to the report (SOU 2010:104), the eGov eID will
follow common information security guidelines together with the need for a detailed information security analysis performed in cooperation with relevant actors. Hence, the Board will need to emphasize, prioritize and analyse information security aspects in close dialogue with relevant actors in this area. With the previous framework agreement being phased out without any option of renewal, the eGov eID introduces a new **public procurement** (5) model. Due to changes to public procurement law prohibiting agreements with multiple providers supplying similar services (eID) (SFS 2007:1091) new amendments to law is required. Accordingly, the System of Choice (SoC) will enable SPs to access eID services of multiple signed IdPs with the Board acting as a proxy hence amending the SoC to public procurement law is considered a significant challenge to handle during the eGov eID introduction.

This also motivated by aspects such as delegating the awarding of contracts to a central signing party (the Board) being described as in need of further investigation regarding specific public sector actors such as municipalities and if the SoC can be considered to be a service concession (Prop. 2008/09:29). Hence, as previously only applied to health and social care, a SoC for eID services implies a transfer to a completely different service context that in turn should be seen as a significant challenge in itself. The **external directives** (6) affecting the eGov eID are clearly related to the eIDAS regulation aiming at a more strict regulation of the eID area in order to facilitate the cross-border use of eIDs among member states (EU 910/2014, 2014). So after the regulation is formally adopted in 2014, the Government of Sweden must start developing the related implementation acts. However, since the eID landscape within the EU is very heterogeneous with various kinds of eID solutions fulfilling different levels of trust, the complexity of this undertaking should not be underestimated. External directives regarding eIDs such as eIDAS clearly qualify as obstacle/problems along the path of the eGov eIDs actor – especially when operated on a very tight timeframe such as the eIDAS that should be accomplished between 2014 and 2019.

### 7.3.4 Service provider & Identity provider

The need of establishing the eGov eID in **current practice** (2) is described as a very important aspect of the Boards work (SOU 2010:104). However, the Board struggles very hard to convince certain actors of the benefits of the eGov eID hence current practice in the public as well as private sector become a significant obstacle/problem to negotiate. Since the eGov eID aims at replacing the current Market eID in turn perceived as successful, this poses a significant challenge especially since several actors perceive the eGov eID as a significantly inferior eID model. In addition, specific aspects of the eGov eID may even be in direct conflict with current practice as exemplified by increasing costs for SPs and the inferior business model for IdPs. Thus, this clearly contradicts with the aim of the eGov eID described in the report as not preventing any existing eID solutions while creating opportunities for the use of existing as well as future eID solutions (SOU 2010:104). Further, the financial aspects of the eID model will change quite
Translating the eGov eID

... drastically if compared to the transaction based framework or bilateral agreements between SPs and IdPs in current practice. Since the eGov eID will introduce annual fees for SPs as well as IdPs there is a clear risk that these affected actors will suffer negative financial consequences. So, although the total cost for eID services within the public sector will remain on an equal or even lower level, individual actors’ might be negatively affected in financial terms. IdPs will also have to bear the financial risks of the agreements with the Board and adhering to these regulations may in turn potentially require costly adjustments. The report clearly stated that an active dialogue between the Board and affected actors must be initiated where outstanding issues of the model need to be discussed. Thus, cooperation and dialogue (3) with the aim of establishing the eGov eID in current practice is described as very important.

The Board will facilitate several forums for such activities to ensure participation and minimize negative aspects for actors. These efforts need to be launched at an early stage of the introduction process, and a special need for cooperation with SKL is described to be able to address the significant part of the public sector this particular actor represents (SOU 2010:104). The eGov eID is therefore seen as totally dependent on the support of affected actors such as SPs and IdPs, but at the same time, it introduces several obstacles potentially challenging this support hence becoming a contradiction. To be able to transfer to the eGov eID model, SPs will also need to have access to specific skills and competence hence the term of simplifying the access to eID services for actors in the public sector can be questioned. Hence, the eGov eID incentive of reduced dependence on specific skills can potentially turn out to become an increased dependence on such skills instead. Although the Board is prescribed to inform about the important stages of the transfer to the eGov eID, it will be up to SPs and IdPs to translate them and act in accordance. The Board being mainly financed by SPs fees, any profitability of this model will never be reached without the participation of IdPs bringing a significant existing diffusion and use of eIDs to boost the eGov eID transaction volumes. In accord, positive incentives for IdPs are crucial.

So, the participation of SPs with a current high volume of eID service use becomes a prerequisite for IdPs to join but at the same time the eGov eID model might introduce negative aspects that cause the SPs to maintain their current eID agreements and setup, hence there is a significant risk that the eGov eID introduction turns into a Catch-22 like state where SPs refuse to join because no IdPs are joining and the IdPs are awaiting for SPs to join. In addition, any additional adjustments or other potential risks related to the transfer to the eGov eID solution will have to be assessed by SPs and IdPs respectively. This concerns issues such as the need of having parallel eID systems or allocating resources for preparatory work and transfer projects. This will also require dedicated resources and competence on the SP’s side to be able to assess and possibly transfer to the solution that in turn can turn out to be a severe challenge or obstacle for smaller public sector actors with very limited resources such as municipalities. According to the report
(SOU 2010:104), there is a need for a common public sector eID infrastructure to facilitate and simplify the development of secure digital services in the public sector as well as create opportunities for new IdPs to enter the market. Hence, the eGov eID (4) will provide a more simplified and coordinated public sector eID infrastructure fulfilling the needs of eID services in the entire public sector. In the report (SOU 2010:104), the eGov eID is clearly described from a central coordinating business perspective based and regulations and legal aspects, however, this plan also contains a very detailed technical blueprint of the solution as based on the SAML v2.0 architecture. So there is a potential risk of affected actors having difficulties in translating and understanding this plan since it is predominately formulated from the Board’s point of view as governed by coordination of the area. Even though the entire eGov eID depends on the creation of clear positive incentives for SPs and IdPs, the report presents a rather narrow view of the solution that lacks grounding in practice among affected SPs and IdPs. The eGov eID will most likely indeed make it easier for SPs to implement the eID in secure digital services and the agreement model will eliminate the need for multiple agreements between SPs and IdPs as prohibited by law. However, these incentives are clearly aimed at potential or small scale SPs. Hence there is an inherent risk that these incentives are not translated as positive by major authorities based on their significant experience and knowledge of digital service development thus in turn challenging existing practice.

The Board will be financed through annual fees paid by SPs in turn based on a number of estimated users, and the main part of these fees will then be paid to the IdPs as based on their market share in the eID area. Thus, on a general level, the financing model will remain the same with SPs financing the eID services and the IdPs will get financial compensation. However, in detail the new model marks a significant move from the existing transaction based model to a semi-fixed pricing model based on factors such as estimated users or employees for SPs and the estimated market share of IdPs thus the existing transaction model is another aspect of the current Market eID that will, in fact, be challenged by the eGov eID. Since there are no prior existing agreements or regulations on a central Government level in the public sector eID area, the eGov eID frameworks have to be created from the ground. Accordingly, there is a need for constructing and establishing a complex hierarchy of rules and regulations to be applied in the area. This close relationship between the SP and IdP sharing a similar translation of the goal of the introduction resulted in locating a similar setup of obstacles/problems along the OPP paths of these two actors (Figure 22 above).

7.4 Interessement

Still focused on the main actor’s perspective, the stage of interessement (Callon, 1986) (see Section 4.3.4) focuses on how the Board acknowledges the different identities of the actors and how these actors are handled in order to keep them committed and aligned within the network. In the context of the eGov eID, a typical example of interessement
would be actions performed by the Board in order to prevent a potentially doubting external influences from influencing the introduction in a negative way. If for example, the SP for some reason considers opting out of the eGov eID, this will be a potential risk to the entire network. The same goes for the IdP; if the Board fails to convince the IdP to accept and join the network will lose the actor issuing the eIDs. Hence, even though the Board introduces a potentially working framework and solution and reaches the individual goal of the eGov eID actor (an operational eGov eID), the network as a whole will not be considered a success since due to the lack of eID services. This also emphasizes the close interdependency between the participating actors within this network. The interessement process for the three identified actors will be described below with an interessement device; the efforts launched by the main actor in order to eliminate or minimize any negative consequences. Formulated for each actor and set in a context with a triangle of interessement showing potential external influences potentially able to prevent the interessement from succeeding. Hence, this stage of the translation analysis takes us one step further towards finding out what actually happened during the introduction in a highly structured way by showing how the Board acted during the introduction in relation when trying to keep these actors committed to the network as supporters of the eGov eID.

### 7.4.1 eGov eID

For the eGov eID actor, this triangle of interessement (Callon, 1986) as illustrated in Figure 23 shows the identified external influences of **Security and trust**, **Public procurement** and **External directives**. As derived from the previous problematization, these are identified as obstacles and problems located along the path of the eGov eID that can have a potentially negative influence on this actor. Thus, the arched arrow in this illustration represents the interessement efforts of the main actor to try and avoid these external influences from affecting the eGov eID as a member of the network in a negative way. **Security and trust** have, for several reasons, been a very important aspect of the eGov eID during the introduction. First and foremost, the solution itself is to be considered a security solution. Second, the security aspects are described as very important to handle in the governing report (SOU 2010:104) and third, since the eGov eID aims at replacing the existing Market eID, there are already existing views among affected actors regarding appropriate levels of security and trust in this kind of solution. Hence, these three aspects of security and trust have to be addressed and negotiated in a successful way by the main actor to avoid any negative influence on the eGov eID.
The Board will have to convince affected actors in public as well as the private sector about the benefits of joining the eGov eID by getting them to accept and support the solution, to remain in the network and in cooperation towards its common as well as their individual goals. If we focus on the fact that the security level of the eGov eID is questioned by the identification of security risks - what interessement devices, communication and actions, does the Board use in order to try and keep these outside forces from affecting the network in a negative way? Initially, the Board has an active dialogue with representatives from the public (SP) as well as the private sector (IdP) and the mutual outcome is to act duly to hopefully solve these issues as soon as possible. The interessement device here is the acknowledgement and following mutual agreement where the Board seems to acknowledge the risks with the aim of quickly minimizing the potential negative impact of the external influence of security and trust.

However, at the beginning of 2014, the Board uses the Letter of Intent (LoI) as another interessement device for the eGov eID approaching top level management of some selected public sector authorities to hopefully gain a quick acceptance. Based on the outcome of this effort, all general director representatives of E-Delegationen finally accept and sign the LoI it seems to be a success even though several authorities having clear concerns regarding how this document to be signed is formulated resulting in revisions. However, translating the LoI as the interessement device for preventing security and trust from negatively affecting the eGov eID it should be noted that this effort is not aimed at the identified security risks per see but at the top management level of the leading authorities as members of E-delegationen. Later during the spring of 2014, the Board is awarded the mandate to lead a detailed security analysis of the eGov eID which in turn also results in cooperative efforts with MSB acting in a supporting role during this analysis. Thus, the security analysis performed in fall 2014 becomes another interessement device to potentially minimize the negative effects of actors questioning the security levels of the solution. This is seen as a very important step in assessing and
improving the security of the eGov eID and in turn as an interessement device completely adhering to different voices raised questioning its level of security. The Board, as well as MSB, reports their results of this analysis and the Board, in turn, uses these findings as a basis for formulating their action plan in late 2014 with the aim of solving all outstanding issues regarding the eGov eID. In addition, several major agencies such as the Tax Agency joins the solution and there is also a clear focus on cooperative efforts an improved dialogue by forming the Governance Forum of representatives of eGov eID members’ authorities. During 2015, the Board works very actively in different constellations and forums to solve the outstanding issues on the action list hence this being the latest example of an interessement device formed to ensure that the Board acknowledges the work left to be done before the eGov eID can be fully operational. During 2011 to 2012, the System of Choice (SoC) and the needed amendments to public procurement law is one of the most critical parts of the eGov eID along with the need to develop the needed frameworks of regulations and trust.

This narrow focus results in a forced development and introduction process strictly focusing on these aspects for a considerable time. The SoC, therefore, becomes the interessement device regarding the outstanding procurement issues to be solved. The extensive work preparing for the amendment to law requires a considerable effort, and the SoC is finally implemented into law in mid 2013 (SFS 2013:311). Hence, the SoC is also described as a significant obstacle that in turn results in the first revision of the eGov eID timeframe. Although the finalization and operationalization of the SoC being described as a significant success, the Board ends up being severely tied up in this process for a considerable time. Although, a possible influence on a national level eID of future external directives for example in the form of EU initiatives are mentioned only very briefly in previous government investigations and reports focusing on eID services such as (VERVAR 2007:13).

Not described in detail in the report governing the eGov eID (SOU 2010:104), this area has a clear potential for a greater interest on the EU level. Motivated by several EU initiatives investigating potential interoperability among member states (IDABC, 2009), specifically focusing on eID services (PEGS, 2010) and piloting cross border eID services for simplified access to public digital services such as the STORK-project (e.g. STORK, 2014b), it is just a matter of time before the EU will initiate coordinating and regulating efforts within this area since the benefits and key role of the eID as a cross border digital service enabler has been identified and the successful results of these pilot project starts to show. Therefore, the eIDAS regulation focusing on cross border use of eIDs among member states (EU 910/2014, 2014) is used as an interessement device in a later stage of the eGov eID introduction to potentially bring clear positive incentives to join the solution. Hence, if the aim of EU level conformance regarding eIDs is to be realized actors have to accept and join the eGov eID. However, external directives are still located outside the triangle of interessement as an outside actor with a potentially
negative influence motivated by factors such as government still being in a very early stage of investigating the consequences of the eIDAS regulation as operating on a very tight timeframe itself. Based on the scope of this effort, the coordination and control of eID services in all member states, I argue that this should be considered as a high risk effort in itself thus any potential challenges in adapting to eIDAS will easily spill over and negatively influence the eGov eID. Thus, if coordinating efforts on a national level face obstacles and challenges, coordination of eIDs on a European level will probably be even more challenging.

7.4.2 Service provider and identity provider

As described above, a similar approach is used when problematizing the OPP paths of the SP and IdP since these two actors share several points of departure and perspectives on the eGov eID during the introduction. This results in the forming of two similar triangles of interessement as illustrated in Figure 24. Hence, this is the outcome of identifying clearly recurring patterns regarding perspectives and implications of the eGov eID for these two actors. To keep the SP and the IdP content in the network, there has to be an active cooperation and dialogue; their current eID practice should not be risked to any larger extent, and the eGov eID itself must be associated with positive incentives in order to accept and join the solution. Moreover, these recurring patterns or overlap also provides insights of eGov eID implications not being bound to a particular sector since these potential obstacles have been identified as relevant to public as well as private sector actors. This also provides a more unified view of a limited number of aspects significantly affecting the eGov eID network and introduction process. Accordingly, how these external influences of cooperation and dialogue, current practice and the eGov eID can potentially affect the SP and IdP will be described along with the Board’s efforts of avoiding any negative influence.

Figure 24. Interessement - service provider and identity provider (adapted from Callon, 1986)
One of the previously main concerns and potential obstacles regarding the introduction is the fact that this solution aims at challenging *current practice* by replacing the fully operative and widely used Market eID with the banks acting as dominating IdPs. Hence, the Board is up for quite a challenge when trying to introducing a new solution that will affect all public sector current and potential SPs as well as current and potential IdPs. Therefore, the positive incentives of the eGov eID become of great importance for the entire introduction process acting as the interessement device when trying to prevent the current practice from affecting the network in a negative way, by resistance and lack of acceptance. Prior to the introduction, the main incentives are described as simplifying the process of accessing and developing eID enabled digital services and to provide a standardized sustainable solution that will allow for new IdPs to enter the market.

However, this interessement device is clearly aimed at one specific segment of SPs in the public sector; SPs that struggle with the development and delivery of eID enabled secure digital services or potential SPs without current digital services. It should come as no surprise when major SPs starts to question these basic eGov eID incentives since their aims and goals of the eGov eID are clearly diverging; to keep their eID business as usual to continue the development and provision of digital services. The current practice of such established SPs becomes a strong influence on a potential negative impact on the SP as an actor in the network. However, for other authorities, the incentives of the eGov eID seem to work since authorities, although a small number, start to sign and join the solution in 2014. The main motive of trying to increase the momentum in the development of secure eID enabled digital service is also focused by the IT-minister in 2012 stating that a secure eID is an important prerequisite for the much needed increase in digital service development.

However, it would be safe to say that established SPs and IdPs did not share this urgency regarding these matters since they had been developing such digital services for a considerable time hence only wants to continue this development. This is, therefore, a significant obstacle for the main actor to handle during the introduction process that will be further elaborated below. Since affected actors have the opportunity of influencing the eGov eID network in several ways of forms makes efforts regarding *cooperation and dialogue* very crucial for the network or introduction to succeed. One clear example being the IdP influencing the SPs regarding the identified security risks in fall 2013. As an interessement device, a mutual agreement is made between the Board and several authorities taking part in these discussions but later, from the SP’s perspective it is described that his agreement is not met when the Board instead launches a new interessement device (the LoI) aimed at a higher management levels for seeking acceptance for the eGov eID among authorities as members of E-Delegationen. The neglect of the main actor to directly act upon this agreement, in fact, allowed external influences are putting forth the security risks to grow even stronger. This is an example of a failure of the LoI working as an interessement device in the context of cooperation and dialogue.
to handle the identified risks hence the lack of cooperation and dialogue becomes the negative external influence causing the SP to seriously doubt the main actor’s competence in handling these security issues in turn resulting in the call for an external independent security assessment of the eGov eID sent to MSB. From the IdP’s perspective, aspects of current practice potentially negatively affecting this actor’s participation in the network is predominantly related to the perceived inferior business model of the eGov eID from a banking sector perspective and the issues of lack of flexibility and security from a technical eID perspective. Throughout the introduction, the Board used the statement ‘positive negotiations with the banks’ as a standard phrase to show that the Board and the banks as SPs are actively discussing these issues hence this phrase, in turn, becomes the interessement device regarding cooperation and dialogue.

Along the path of the introduction, the IdP also clearly stated that their intention is to continue to support the public sector with eID services hence the IdP is also showing a willingness to offer continued support to be public sector as soon as the requirements of the eGov eID from the IdP’s perspective are met. Despite the efforts of the Board trying to keep an open dialogue in different forums such as reference groups and bilateral dialogues, affected actors still report the lack of a constructive dialogue as one of the main concerns and problematic aspects of the introduction. The reason for locating the eGov eID itself as an external influence with a potentially negative influence on the SP and IdP needs to be further explained and will in turn address the question of how and why the eGov introduction process influences itself. In fact, there are aspects and actions performed by the Board that affects the introduction negatively hence the eGov eID then becomes the external influence with a potentially negative influence on the SP as well as the IdP. As previously described, there are at least two clear examples of the eGov eID introduction process turning on itself in this way.

First, the most obvious example is the security risks first identified by the IdP, acknowledged by the SP and later also acknowledged and confirmed by the Board as well as relevant authorities in the security area. At an early stage, the Board reassures that relevant security risks have been assessed and handled accordingly referring to a previous security analysis. However, this strategy evidently fails when MSB and FRA acknowledge the security risks. Although these actors did not have regulative roles, they strongly emphasized the need for addressing the identified risks. The Board finally acknowledges these arguments and creates the action plan as a new interessement device to handle these issues. Second, increasing costs and adjustments needed by the SP and IdP will possibly prevent them from accepting the eGov eID and transfer from the current Market eID solution. However, these consequences are clearly underestimated from the Boards perspective and are not addressed until 2014. However, in 2015 the Board finally addresses the financial consequences of joining the eGov eID by stating that the total cost of eID services for the entire public sector should remain the same hence
touched upon the financial aspect but showed an unwillingness to respond to any specific questions. Needless to say, this strategy did not work very well hence the argument stating that joining the eGov eID will result in significantly increased costs became a well-known fact among affected actors and also freely translated by each affected actor’s own organizational perspective. Regarding any additional adjustments needed for the joining party such as the SP and IdP, these aspects are also up to the individual actor to assess thus I argue that the Board clearly did not try to bridge these potential gaps between different organizational perspectives and the eGov eID.

7.4.3 Additional remarks

So, after analysing how external influences affect the introduction and in turn how the Board as the main actor handles and negotiates these influences by launching different kinds of interessement devices, it becomes clear that the presented triangles of interessement above are clearly related to each other. Based on the fact that the eGov eID is identified as a potential external influence with a potential influence on the interessement of the SP as well as the IdP, for example, the security risks of the eGov eID as well as negative financial aspects. Hence, the three triangles can be successfully combined into one as illustrated in Figure 25. This in turn clearly illustrating the reciprocity of the eGov eID actor; both in its role as the important actor as well as the goal of the introduction but also in its role as a potential negative external influencer of the SP and IdP.

During interessement, the main actor has full control of the devices used towards the different actors, i.e. the curved arrows, but has little or no knowledge about the negative influence emanating from introduction process itself as shown by the two emphasized arrows in Figure 25. Therefore, whenever the Board faces a challenge or obstacle along the introduction, it has not only to deal with solving this issue itself but also with the fact that there is a potentially negative influence on the SP and the IdP emanating from the challenge and its handling itself. Thus, this can potentially develop into a double negative feedback loop when an event has negative effects on the eGov eID itself as well as the other two actors in the network. The most obvious example would be the identification of the security risks that caused the external influence of security and trust to negatively affect the eGov eID as well as the SP’s and IdP’s translations of the solution. For obvious reasons, the translations of these events are also clearly related to the amount of trust specific actors such as SP and IDP have towards the Board at this point in time. Therefore, this also proves that translations of the events taking place in the network will, in fact, have the power to affect the actors as well as their participation in the network.
7.5 Enrolment

The next stage of enrolment (Callon, 1986) (see Section 4.3.4) is focused on the outcome of the previous stage of interessement. Hence the guiding question here is how the main actor did success in keeping the actors enrolled in the network throughout the introduction process. The following sections will cover how the Board as the main actor negotiates and acts during the interessement and how the actors of the network respond; if in fact the efforts of interessement succeeded and keep the actors content and enrolled in the network or if they failed and make actors to consider their participation altogether? Accordingly, from the enrolment and onwards, the actual perspectives of the SP, as well as the IdP, are based on empirical findings which bring the opportunity to find out what actually happened during a selected number of events during the introduction as seen from each individual actor’s perspective. Therefore, I argue that this approach will provide unique insights on how the actors responded and in turn translated these events as well as the related actions launched by the Board and how this actor based translations in turn significantly affected the entire introduction process. So what I am referring to here is the confirmation of the perspective of perceiving the eGov eID introduction as on several occasions influenced by translations. Hence this power assigned to actors’ translations to affect the whole introduction process also being one of the central arguments put forth in this dissertation.
Translating the eGov eID

7.5.1 eGov eID

The enrolment of this non-human actor is of course managed by the Board governing its participation in the network. Although the interessement device of the agreement to act upon identified security risks in late 2013 seems very promising, with a swift acknowledgement and a dialogue and actions to minimize the potential consequences of these risks, empirical findings indicate otherwise. Initially, the Board did not seem to take these views seriously since they, according to the SP, did not act in accordance with the agreement. Hence, the interessement device of the LoI did in fact not eliminate negative influences of security and trust to affect the eGov eID, but rather sparked the other actors to form another constellation or network to continue to push for these security issues to be handled accordingly. As a result of Government awarding the Board with the mandate to lead the security assessment with MSB in an advisory role, the Board clearly changes its strategy. By accepting the risks, the Board now uses the security analysis as their main interessement device to counteract the negative consequences of these aspects. The result of the security analysis is used as a basis for formulating an action list on how these risks should be handled in late 2014 and early 2015.

Thus, this action list became the next interessement device to show that the Board takes these criticisms seriously and works actively to sort out any outstanding security issues. Further, the Governance forum is also formed in an effort to legitimize these efforts with the aim of solving these problems in cooperation with actors that had already joined the solution. Needless to say, the identification and rather late acknowledgement and handling of the security risks did not work entirely in favour of the Board in its efforts to gain acceptance and trust in the eGov eID during 2014 and 2015. Having settled for the SoC as the solution to solve the outstanding issues regarding public procurement of eID services, this new model receives positive comments in general. However, critique is put forth describing the risk of increased legal fragmentation bound to a specific technical context. The referral process focused on the SoC also confirms that as an interessement device seems to work quite well since a majority of comments supports it although the need for further investigations of its consequences is also put forth.

As an example of external directives, the eIDAS regulation aims at coordinating European eIDs, comes into effect in 2014. Hence the potential influence on the eGov eID should be deemed as significant. However, since the introduction of eIDAS on a national level only started out in 2015, at this point in time its consequences can only be predicted. While still in its early stages I argue that the main incentives of the making national public sector eIDs interoperable with other member states (MSs), at this stage are rather weak which in turn will affect the outcome of the interessement process as well as the following enrolment. As tightly bound to providing a cross-border interoperability per se rather than local benefits for authorities and in turn related to challenges such as how to map the unique individual identifiers of foreign eIDs to the Swedish model of unique personal identifiers I argue that eIDAS fails as an interessement device during
the eGov eID introduction. Moreover, if succeeded, the number of authorities signing and joining the eGov eID would have been significantly higher.

7.5.2 Service provider and identity provider

Clearly challenging the current practice and use of the current Market eID in the entire public sector, the eGov eID should be considered a significant challenge to manage in itself. The interessement and enrolment should, therefore, most likely focus on the positive incentives to join the eGov eID and to negotiate and handle any negative consequences. The initial incentives of the eGov eID are focused on aspects such as simplifying the development of eID enabled digital services for SPs and allowing for new IdPs to enter the market. Hence, the governing report (SOU 2010:104), as well as the Board, adapts a clear centralized, coordinated view on the incentives. So how successful are these incentives in keeping the current practice from influencing the actors in the network in a negative way and can the Board successfully convince the SP and IdP about the benefits of the eGov eID in order to get them to consider to join the solution?

At first, it sounds very promising since cooperation and grounding in practice are emphasised in the report (SOU 2010:104) along with the Board ensuring that they would facilitate an unproblematic transfer from the current eID solution to the eGov eID. However, one of the most important aspects that drives the SP’s strong development of secure eID enable digital services is the handling of financial transactions for example in the form of different kinds of financial support to citizens. This, in turn, requires a high level of security internally as well as externally towards customers thus the SP is to be considered a very competent in the security area. By challenging the current Market eID the Board in fact challenges one of the basic pillars of this authority, i.e. secure online communication. Further, the oligopoly of the IdPs (the banks) is not considered a problem from the SP’s perspective despite the Board’s efforts of convincing the public sector that the dependency of the banks as IdPs needs to be reduced.

Hence, the SP translates the private-public sector convergence as merely a result of the strategy dating back to the beginning of the 2000s when it is decided that the public sector should make use of eID services existing on the market. The SP, therefore, perceives the described benefits of the eGov eID as rather diffuse and difficult to translate from their business perspective. Without offering any significant advantages as compared to the Market eID, the purpose and aim of the eGov eID is questioned from an early stage. The disadvantages and potential risks of the eGov eID, such as the security risks and increased costs, receives considerable attention are also used as the strongest incentives not to accept and join the solution since it implicates the introduction of an inferior eID solution from a security perspective. This results in the SP initiating internal discussions in terms of not joining the eGov eID and hence totally opt out of the network altogether. Similar to the SP, the Market eID (BankID) has over time grown extremely important for the IdP and banking sector as a whole hence the IdP is extremely cautious in not risking any negative consequences regarding its current high levels of trust and
Translating the eGov eID

security. Also stating that any changes to the successful current eID model, such as introducing the eGov eID, should be approached with extreme caution since the consequences of any failures regarding security and trust will have very serious consequences for the IdP. Hence, from the IdPs perspective, the eGov eID got a rather bad start since this actor clearly questioned the technology used from the beginning, in turn, resulting in a negative translation of the architecture since it is described as building on old technology and not fitted for its purpose. Thus, the SP and IdP both share the similar translation of the Market eID as well functioning providing an appropriate level of security and trust at a reasonable cost.

In addition, the IdP puts forth the perspective of the Market eID as a fully functioning national eID solution hence the incentives to replace it are questioned. Although the introduction is translated as being highly problematic from the IdP’s point of view mainly regarding the lack of an open, constructive dialogue and cooperation, this actor is still convinced that the IdP eventually will accept and join the solution. The incentives and benefits of the eGov eID are translated as rather weak and in fact only resting on the need for a new procurement model. However, the IdP argues that from their perspective, SPs will have the ability to procure eID services directly and hence not via any centralized public sector procurement model. This also being a consequence of the extremely strong position and dominance of the eBanking eID. Hence, the main consequences of the eGov eID as translated by the IdP is described as an inferior business model and a change in the management of agreements going from a bilateral to a centralized agreement model.

The fact that the supply of eID services to the public sector should be considered as a non-core business done in the margin for the banking sector also clearly affects how the IdP translates the incentives and consequences of the eGov eID. The IdP urges for a continuance of the transaction based business model, but despite extended negotiations, the IdP is presented with facto of having to accept the semi-fixed pricing model as presented by the Board in turn translated as a clear setback by the IdP. The outset for the Board regarding the acknowledgement and grounding among affected actors looks promising since the report (SOU 2010:104) emphasizes the importance of cooperation and dialogue with affected actors. Thus, the dependency between the acceptance among affected actors and a successful introduction of the eGov eID is acknowledged at an early stage of the introduction. On a general level, the Board actually faces a major challenge when trying to balance the required high level of acceptance of the SP and IdP with the successful negotiation of potential negative consequences for affected actors that in turn potentially could threaten the entire network. Acceptance from and cooperation with affected actors must be considered crucial in order to minimize any potential negative influence on the network from these actors. Thus, the guiding question here being how the Board manages to handle the acceptance and cooperation in order to keep

239
actors enrolled within the network? During 2014, the Board focuses strongly on promoting the eGov eID in different forums such as workshops and public sector conferences, with the aim of increasing the levels of acceptance in the public sector.

In addition, during spring 2014 the Board allows the possibility for authorities to sign and join the eGov eID for the first time hence this could be considered a milestone of the introduction. It is also described that the Board’s dialogues with several banks as well as other potential IdPs are intensified in order to seek acceptance. During fall 2014 the Governance forum is initiated as a way to improve the dialogue and cooperation. However, this initiative is exclusive to the authorities that had already signed to join the solution while excluding the doubting ones. Based on these actions it seems that the Board clearly acknowledges the need for improved dialogue and cooperation. From the SPs perspective, it is described that the eGov eID is significantly different from how authorities normally tend to cooperate. Thus this introduction is translated as applying a perspective of compliance instead of being focused on mutual benefits for affected actors. This in turn also being a consequence of the strategy chosen by the Board by first laying the foundation of the eGov eID with the creation of different regulatory frameworks and technical infrastructure, before moving into the phase of actively seeking support and acceptance.

Unfortunately, the SP translates the communication about the eGov eID as fragmented and unclear and on some occasions even incorrect hence, this results in this actor perceiving the introduction as clearly non-transparent. Further, the dialogue with the Board is described as clear problem based as exemplified by the SP approaching the Board with identified security risks. The strategy of forming different forums for dialogue is not perceived as optimal but rather translated as a strategy chosen by the Board to seek acceptance without leaving any room for any influence. From the IdPs perspective, the dialogue is described as being almost non-existent, and the communication is described as being performed in one-way without any room for cooperation or dialogue in a real sense.

Hence, it is clear that the IdP translated this as the Board sticks to be a blueprint for the eGov eID without leaving any opportunities for market actors such as the IdP to actually influence it. As a result, the business model of the eGov eID is described as being a result of a non-cooperative effort since the IdP is forced to accept it. However, after the security risks are acknowledged, the IdP perceives that the Board does not ignore any critique of the eGov eID in the same way as before. However, since the efforts to solve the outstanding security risks pose an extensive challenge, the IdP can not speak in terms of accepting the eGov eID before these issues are actually solved by the Board. Further, the IdP describes not being able to assess the eGov eID solution in its whole since it is presented in a highly incremental and fragmented way by the Board. Although this most
likely being a result of how the Board works during the introduction, addressing upcoming challenges and obstacles on a case by case basis. However, this is clearly translated by the IdP as a planned strategy to prevent external influences from actually affecting it. The most significant shortcoming of the introduction as translated by the IdP is described as the missed opportunity of taking advantage of the existing knowledge and competence in the area among affected actors such as SPs and IdPs. The IdP also translates the Board’s effort to get the IdP to accept the solution as a way of trying to enforce an acceptance. Nevertheless, there is still a strong consensus among IdPs that all outstanding issues of the eGov eID have to be addressed and confirmed as solved prior to signing any agreements. In addition, the IdP emphasizes the need for acceptance, diffusion and trust as the most important aspects regarding the introduction of an eID solution.

In the previous stage of interessement, locating of the eGov eID itself as an external influence possibly affecting the network in a negative way is based on the notion of potential challenges and obstacles being translated in a negative way by affected actors hence negatively affecting the introduction itself. To try to ensure a high level of legitimacy trust, the Board focuses on activities such as the development of central regulatory and trust frameworks, but in reality, affected actors report a clear lack of legitimacy and trust in the Board as well as the eGov eID. Hence the guiding question here is why does not the Board succeed in gaining the needed acceptance and trust of the eGov eID among public and private sector actors? Despite having performed several security analyses, the Board still faces significant problems regarding the security of the solution and the eGov eID is continuously criticized for being associated with negative aspect such as increased eID costs. Hence, what will be focused here is how these described security risks are handled and in turn translated by the actors of the network. At the time of the security risks first being identified, the SP states that if a security solution, such as the eGov eID, fails to deliver on security it will never gain the needed acceptance and trust. Further, the way the Board handles this issue, i.e. by instead focusing on the distribution and signing of the LoI, is clearly translated as an act of neglect by the SP. In 2014, on the annual eID day, the chairman of the Board urges for public sector authorities to accept and join the solution but at the same time, several authorities alongside the SP are highly dissatisfied with the way the Board seems to refrain from accepting and acting upon the identified risks. The SP’s trust and confidence in the Board is seriously affected in a negative way and results in the SP approaching an external authority to perform an independent security analysis of the eGov eID; also joined by several other concerned authorities. Hoping for an impartial analysis, the government assigns the Board itself with the task of assessing its own solution from a security perspective. Although being positive about the acknowledgement of the security risks, the SP again negatively translates the coming security analysis with concerns that the Board will influence it and
present a result in its favour. MSB, the authority that the SP approaches for an independent analysis, is appointed as a consulting party to the Board during this analysis which is translated by the SP as a conscious strategy to place this competent authority (MSB) in a weaker position. When MSB presents its final report in the form of a list of recommendations for the Board to follow it is also reported that this authority has a classified version of the report as a result of the cooperation with external actors in the area of public sector information and cyber security. Thus, the SP is quite content of the analysis being performed with an independent approach but at the same time equally dissatisfied with the arguments put forth in the report.

Since MSB has no regulatory mandate, this authority can only issue recommendations with different levels of emphasis. However, this report describes some very serious shortcomings in the proposed eGov eID solution. Later, the Board also presents its final report of the analysis which in turn is translated as quite confusing, and several questions are raised such as – how should these two reports be measured and how would they affect the Board? So, with the report later released by FRA, these reports are translated and gives rise of a distrust of how the Board dealt with these risks; a translation that is clearly affected by how the Board previously hesitated to acknowledge and act upon these risks. It is clear that the events surrounding the identified security risks of the eGov eID are translated in a negative way by the private sector as well hence the IdP also questions how these risks are handled by the Board. Historically, the dialogue between the Board and the IdP has been almost non-existing which in turn is translated as the Board trying to enforce the eGov eID on the public as well as private sector without the possibility of influence. In 2014 the dialogue between the IdP and the Board becomes more active and in 2015 the IdP officially states that they are still supportive of the eGov eID solution.

Important aspects such as high levels of flexibility and security are clear prerequisites for considering to sign and join the solution. Nevertheless, the IdP is still confident that these outstanding issues will be solved during 2015 with the possibility of the IdP officially joining the eGov eID later in 2015. Being extremely cautious about the security of the eGov eID, the IdP translates the security analysis as positive, but the advisory role of MSB is described as very unfortunate. The IdP will therefore still urge for a detailed security analysis and assessment of the final version of the eGov eID. Further, the IdP puts forth flexibility as a very crucial aspect regarding eID solutions to be able to respond quickly to new online threats. Therefore, the IdP translates the different frameworks (regulatory, technical and trust) as introduced by the Board as potentially affecting the IdP’s much needed flexibility in a negative way. The IdP also acknowledges translating actions performed by the Board as trying to force them to sign agreements but maintains the demand that all outstanding issues from their perspective must be solved or at least have very clear conditions on how and when they would be solved. Even though the IdP translates the eGov eID introduction as far from optimal regarding
several aspects as well as potentially introducing new risks that could harm and spill over to their core business, i.e. banking services, the IdP is still positive regarding the continued support of eID services to the public sector in the context of the eGov eID.

7.6 Mobilization

Mobilization (Callon, 1986) (see Section 4.3.4) is the stage of the analysis that focuses on how the aims and goals of the identified network are transferred into actual practice i.e. how the organizations acted as represented by their spokespersons in the network. Since the representatives are featured in the network only allowed us to create a more or less generalized picture of previous actions, translations and negotiations, there will be no guarantees that the actual organizations as represented by these spokespersons will follow, i.e. all current and potential SPs as well as IdPs. So in this case, if mobilization will be successful it will mean that the eGov eID gets successfully introduced and accepted throughout existing and potential SPs across the public sector with the support of current and potential IdPs.

7.6.1 eGov eID

On a technical and regulative level, the eGov eID seems to have been successfully introduced since the service is operational in 2014 according to the Board. Hence, at first glance, it seems that the Board successfully reached its goal of the national eGov eID solution although with a significant delay. However, as it turns out, this success is reached only by successfully fulfilling the individual goal of the eGov eID actor in the network and reaching an operational eGov eID. Hence, the acceptance and use is put in the background since the full support of the SP as well as the IdP is still missing. This is also motivated by the very few authorities that have actually signed and joined the solution, and the IdPs are still waiting for several outstanding issues to be solved. As previously described, without the broad support of SPs and IdPs, the eGov eID will never reach significant success, i.e. be used in in public sector digital services as well as diffused and used by citizens and businesses.

Therefore, I argue that these are the requirements for the eGov eID to be able to replace the current Market eID. Based on the analysis so far, indications point towards the Board putting the technical and regulative aspects of the eGov eID introduction in the foreground (2011-2013). Hence, the important need of grounding the solution in practice as well as facilitate an open dialogue and active cooperation is acknowledged much later (2014-2015). This can also be the result of the Board counting on a higher level of loyalty towards the public sector as a whole; a perspective also motivated by the lack of problematization of these aspects in the report (SOU 2010:104).

Maybe the Board had counted on more loyalty towards the public sector as a whole among current and potential SPs, but as it turns out current practice and local business perspectives are predominant forces influencing the SP’s and IdP’s translations as well.
as institutional norms and values regarding the eGov eID. As the deadline for the last framework agreements is fast approaching (mid 2016), several authorities such as the SP starts to investigate alternative solutions to facilitate a continued supply of eID services. These backup plans include the following three scenarios: (A) to join the eGov eID, (B) to use the current Market eID solution via interim arrangements and (C) to procure services directly from the IdPs. Consequently, the Board responded to this need and presented an official transition service in mid 2015. This arrangement will, however, result in the Board signing with current IdPs hence the transition service is the result of the Board mobilizing in order to minimize the negative consequences of the majority of public sector actors not being signed to the eGov eID yet. If public sector SPs are to solve these issues by themselves, i.e. sign agreements with one IdP (bank) representing the BankID solution, this will also render the eGov eID as completely obsolete. Still, this transition service also introduces the risk of the eGov eID being put on hold for several years, i.e. until end 2017.

7.6.2 Service provider

The SP in the network is mainly represented by skilled officials in the information security area which in turn is motivated by the eGov eID being a security solution. This perspective is made very clear in the previous stage in the analysis. Hence, regarding the representativeness of these officials regarding their authority as a whole, it is reported that they have a very hard time convincing top management that they can neither consider nor accept the eGov eID as long as it is flawed with security risks. On several occasions, officials report there are close calls for example when an agreement with the Board is almost signed, but eventually these security advocates manage to get their message through, i.e. that the authority must await any signing until the Board delivers on security. With the end of the current agreement with IdPs fast approaching (mid 2016), there is also a considerable mobilization to investigate alternative ways of securing the access to the current Market eID services without signing any agreements with the Board. Regarding this SP’s representativeness with regards to other public sector authorities, I argue that this SP has a unique role.

At times of the introduction, there are only very few authorities actively resisting the eGov eID and really try to put pressure on the Board regarding the outstanding issues. However, as described in the enrolment stage, negative translations of the outcome results in a clear mistrust in the eGov eID solution in general and the Board in particular that influenced the later actions regarding these matters. So it is clear that the coordinating perspective of the Board quite dramatically conflicted with the security perspective of this SP. The transition service presented by the Board is in turn translated with a great deal of mistrust and perceived as a way for the Board to get authorities to join the eGov eID by signing up for the transition service. In the following discussions bilateral agreements are also confirmed as possible on legal grounds hence this alternative can result in the IdP continuing to support the SP with eID services in a similar way as in the current Market eID solution. So this would, in fact, provide a very interesting outcome.
of the network where the introduction of the new eGov eID, in fact, results in a reinforcement of the use of the Market eID.

7.6.3 Identity provider

Although the events and actions related to the eGov eID are translated in a slightly more positive way by the IdP, this actor is still extremely cautious signing any agreements with the Board as long as the banking sector’s requirement regarding specific aspects of the solution such as flexibility and security are met. However, the discussions held internally among banks are kept totally secret, but it is described that these discussions both internally and externally with the Board are entering another stage i.e. with a not too distant acceptance. However, discussions between IdPs and the Board are still held on a strictly bilateral basis due to laws on competition. Since there are no indications of the IdP accepting the eGov eID and signing with the Board yet one would assume that preparations and impact assessments are extremely thorough and/or the Board are not providing the necessary solutions for the critical outstanding issues as seen from the IdP’s perspective. In addition, the analysis presented above presents a rather relentless willingness from the banking sector in general and the IdP, in particular, to continue support eID services to be used by SPs in the public sector hence the outlook for current IdPs of accepting and joining the eGov eID in the near future is still positive. However, as long as no agreements are actually signed between IdPs and the Board there will always be a risk of SPs in parallel signing bilateral agreements with IdPs or existing intermediaries to provide their eID services. Thereby the eGov eID will, in fact, turn out to be a fully operative national public sector eID solution working in theory but not used in practice.

7.7 Closure

With the stage of closure (see Section 4.3.4), the final point of the analysis is reached hence a short description of the current status of the eGov eID introduction is in place. Hence, the events described below focuses on the events in fall 2015 thus actually takes place after the final interview is performed in June 2015. However, these are very briefly described to reach a level of the closure of this analysis. As previously described, by this time the eGov eID is described as fully introduced on a technical as well as regulatory and legal level. However, there are still outstanding issues in the action plan as formulated by the Board. The Board describes that discussions and negotiations with the IdPs are intensified and has just launched the transition service to provide a means to public authorities not planning or not having time to adjust their digital services to gain access to eID services. However, despite these efforts by the Board, the SP featured in the network above finally decides to opt out of the eGov eID in October 2015 as motivated by the security risks still not accounted for as translated to be “fundamental security risks” (Publkt, 2015a, 2015b). This means that one of the major Swedish SPs will in fact not be a member of the eID eGov solution. This decision is described as a major setback for the introduction in turn also being a result of the timeframe given by the
Board to prepare and transfer to the eGov eID translated as being non-realistic (Publikt, 2015c). However, at this time (late 2015) there are no reported signs of this unfortunate defection influencing the continued negotiations between the Board and the IdPs but I argue that losing the authority with one of the largest eID transaction volumes in the public sector most likely not works in favour of the much needed increased acceptance of the eGov eID. So this brings us to the conclusion that the network that features in this analysis, unfortunately, failed at this point in time since the SP chose one of the identified alternative strategies to ensure a continued support of eID services from the IdP. Further, the IdP is still within the network at this time but given this development; I argue that its participation still is rather uncertain.

7.8 Concluding remarks

Based on the translation analysis presented in this chapter, the following important findings have emerged. First, the importance and potential power of actor based translations are confirmed when it comes to trying to succeed and reach the common goal of successfully introducing the eGov eID in a network consisting of different actors. Second, the inability of successfully handle individual translations will present the main actor with very difficult challenges. For example, the Board clearly underestimated the power of actor level translations as based on different local business perspectives of the SP and IdP. The Board tries relentlessly to try and keep these actors enrolled in the network, but the SP finally chose to opt out of the network and the participation of the IdP, as well as the rest of the banks, still, hangs in the balance at the time of writing. Third, the competence and ability of the main actor to handle key aspects of the eID become very crucial during an eID introduction, as exemplified by the identified security risks of the eGov eID. Thus, there is a strong need to acknowledge and align the perspective of the main actor with other actors, e.g. the SP and IdP, when acting upon such critical issues as the security of a security solution.

This analysis also provides important insights regarding the introduction of public sector eIDs on a national level. Although the Board, operating on a very tight timeframe, succeeded in introducing the eGov eID, the acceptance and support among public sector actors are very limited. So this also touches upon one of the main challenges when it comes to ICT initiatives in general and eID initiatives in particular launched on a political level in a potentially too optimistic and deterministic way. In government documents, the eGov eID is described as the next step forward towards a standardized and coordinated public sector eID and would, in turn, eliminate the monopoly of the current private IdPs. Although the importance of establishing the eGov eID in practice is clearly stated as an important aspect of the report (SOU 2010:104) governing the introduction, the Board clearly underestimated the importance of these aspects since they initially focused on getting technical, regulatory and legal frameworks in place. Accordingly, acceptance and grounding in practice are left to be handled ex post of the introduction of the basic infrastructure by launching different interessement devices and hoping for
a continued enrolment within the network. However, in reality, trying to convince actors with already developed and potentially institutionalized negative translations of the eGov eID turned out to be very challenging and in some cases even impossible since the SP finally chose to opt out of the eGov eID network. It, therefore, becomes clear that to be able to succeed with inter-organizational coordinating efforts regarding eID services, the main actor must acknowledge and address different actors’ translations in the early stages of the process since the acceptance neither can be taken for granted nor forced upon the affected actors; also related to the Swedish model of the independent authorities.

In turn, I argue that the acknowledgement and understanding of translations will provide a positive basis to establish an active dialogue and participation that in turn if positive results are met with mutual benefits, will result in a much higher degree of acceptance. Further, several of the challenges regarding the eGov eID introduction have been identified in the introduction of the eIDAS regulation. For example, a seemingly overly optimistic timeframe and the fact that acceptance and participation are more or less taken for granted. So, based on the eGov eID, still struggling to gain acceptance, and paired with unknown consequences for public sector authorities, I argue that the odds are quite low that the eIDAS regulation will be the anticipated success at least not on such tight timeframe. Especially when it taps into and possibly affects the very basic parts of each MS’s government, e.g. regarding their national eIDs and history of personal identifiers. However, I strongly argue that these kinds of initiatives, i.e. regarding national eIDs, facing several challenges should be considered symptomatic rather than problematic since these are the first efforts of trying to coordinate public sector eIDs on national and European level respectively. Hence, this makes it very difficult to predict the potential challenges and obstacles ahead.

So based on the so far very limited acceptance rate of the eGov eID, I therefore argue that the challenges and obstacles faced during the introduction are not by any means a result of conscious oversights and neglects by the Board but rather a result of applying the perspective initially put forth in the governing reports and mandate as well as later during the introduction. In the eGov case, it is clear that the Board applies a coordinating perspective on the eGov eID and related aspects such as regulatory, trust framework and technical infrastructure hence the obstacles and challenges became symptomatic when this perspective came in conflict with the perspectives and translations of affected actors. However, during the process, despite the shortcomings of the introduction, lack of dialogue and acknowledgement of local perspectives, the Board still had a strong belief that the banking sector, in the end, would continue to support the public sector as IdPs.

In summary this chapter presents the translation analysis to investigate and uncover the different perspectives represented in the identified network and the next step in Chapter 9 will be to integrate the findings from the translation analysis performed on the eGov
case, the translation analysis of the eHealth case presented in Chapter 7 and the institutional perspective in the synthesised socio-institutional model. Moreover, a summary of important findings put forth in this chapter is presented in Table 20. In addition, this summary also provides an overview of the translation process from central problem areas (problematization), via how these problems are managed by the Board (intere-essement), translated by actors (enrolment) towards the outcome (mobilization). The final stage of closure is omitted from this summary since it is not part of the original approach as presented by (Callon, 1986).
<table>
<thead>
<tr>
<th>Actor</th>
<th>OPP</th>
<th>Problematization</th>
<th>Interessement</th>
<th>Enrolment</th>
<th>Mobilization</th>
</tr>
</thead>
<tbody>
<tr>
<td>eGov eID</td>
<td>Operational eGov eID</td>
<td>Security and trust</td>
<td>Agreement in 2013 LoI</td>
<td>Action list Governance forum</td>
<td>Approaching deadline</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Security analysis</td>
<td></td>
<td>Limited number of SPs</td>
</tr>
<tr>
<td></td>
<td>Public procurement</td>
<td>System of choice</td>
<td>SFS 2013:311</td>
<td></td>
<td>Lack of IDPs</td>
</tr>
<tr>
<td></td>
<td>External directives</td>
<td>eIDAS Investigation with PTS</td>
<td>Preparatory work</td>
<td></td>
<td>Alternative plans</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Board's report</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Service provider</td>
<td>Provide eID enabled digital services for citizens and businesses</td>
<td>Current practice</td>
<td>eGov eID</td>
<td>Specific requirements must be met</td>
<td>Not convinced to join</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cooperation and dialogue</td>
<td>Bilateral discussions Annual eID day Workshops Conferences Governance forum</td>
<td>Non-transparent Problem based Lack of active dialogue and influence Pushing for acceptance</td>
<td>Mistrust of the eGov eID and the Board</td>
<td></td>
<td></td>
</tr>
<tr>
<td>eGov eID</td>
<td>Security analysis M5B's report</td>
<td>Security risks Increased costs Inferior to Market eID</td>
<td>Additional security analysis to consider joining</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Identity provider</td>
<td>Provide eID services for public sector</td>
<td>Current practice</td>
<td>eGov eID</td>
<td>Specific requirements must be met</td>
<td>Intention to join</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cooperation and dialogue</td>
<td>Bilateral discussions</td>
<td>Lack of active dialogue and influence Fragmented view Not considering existing solutions Pushing for acceptance</td>
<td>COnnuing discussions Intention to join</td>
<td></td>
<td></td>
</tr>
<tr>
<td>eGov eID</td>
<td>Security analysis Business model</td>
<td>Security risks Lack of flexibility</td>
<td>Additional security analysis Internal preparations Intention to join</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Translating the eGov eID
8. Translating the eHealth eID

This chapter presents the translation analysis of the eHealth eID introduction presented in Chapter 6. In line with Chapter 7, the aim is to identify and analyse actors’ perspectives and relationships. The introduction process is seen as a network depending on the commitment and participation of a selection key actors which allows for further analysis of the resistance to the eHealth eID as based on these actors’ individual perspectives. The analysis will follow the prescribed stages of this approach with important findings integrated throughout the analysis. The chapter concludes with a summary of findings from the translation analysis to be further synthesised with the institutional perspective in Chapter 9. By applying translation analysis on the organizational level of the eHealth case, this chapter addresses the first part of the second research question (RQ-2).

8.1 Problematization

Focusing on the introduction of the eHealth eID, the stage of problematization (Callon, 1986) introduces challenges or obstacles on several levels of the network. This problematization focuses on the challenges faced during the organization-wide introduction of the eHealth eID. As a first step of problematization, the eHealth case described in Chapter 6 concludes with a summary of identified challenges of the introduction (see Section 6.5). Hence, these challenges will be further elaborated into more distinct problem areas for further problematizing actors’ paths in the network. This enables the development of a deeper understanding of these challenges and the possibility to relate them to individual actors’ translations. The challenges describing the inherent complexity and heterogeneity in the health care organization (1) as well as complexity as related to technology (2) as potential obstacles during the introduction process are categorized as Organization and Technology. The challenge of how management of the introduction process might affect it negatively (3) is of course related to Management, and the challenge of preventing the eHealth eID from negatively influencing the introduction (4) is consequently categorized as the eHealth eID. Finally, the finding that current practice (5), as well as a lack of knowledge and communication (6), have a negative effect on the introduction of the eID are categorized as Current practice and Knowledge and communication resulting in the following six problem areas:\footnote{These problem areas are listed in the order they are presented in Chapter 6.}
8.2  Interdefinition of actors

In eHealth case, Central IT is coordinating the introduction hence this actor is selected as the main actor in the first step of interdefinition of actors (Callon, 1986) (see Section 4.3.4). Further, based on findings regarding the efforts of Central IT during the eHealth eID introduction as well as the outcome of this introduction, the following three actors are considered as actors within the network of the translation analysis: the eHealth eID, the User and the ITR. These actors are motivated by their importance and key roles during the introduction since it is deemed highly unlikely for the eHealth eID introduction to succeed without a fully functional eHealth eID, acceptance of users as well as support from IT Responsible persons (ITRs). The User and the ITR as actors in this network, in turn, become spokespersons for the larger group of actors they represent.

8.2.1  eHealth eID

The eHealth eID is described as a solution for identification and digital authentication based on smart card technology and a technical infrastructure of standardized parts as prescribed by the SITHS framework. It provides strong authentication to meet the governing regulations for the protection of sensitive information regarding patients. On a technical level, the eHealth eID itself can be seen as unproblematic as issued to medical as well as administrative staff within the organization. The organization applies a strategy where professional, as well as functionality for private use, have been integrated on the same eHealth eID card. It should be treated as a strictly personal highly valuable item, kept near at all times by the user during working hours hence never be left unattended. Thus, the eHealth eID should be inserted into the assigned card reader upon systems authentication and access and removed from the card reader when the user leaves the workstation for other duties. It can be used on multiple workstations during the working day and ensures that the user’s active system session is restored independently of physical location systems access. The eHealth eID must be handled correctly by the user in order to serve its purpose of ensuring the correct level of information security. From the main actor’s perspective, the eHealth eID is assigned with the meaning of an increased security level within the organization. Thus it becomes crucial for affected users to translate it in a similar way for the eHealth eID to achieve its purpose.
8.2.2 User

This actor represents the users of the eHealth eID across the organization, in different roles and professions and on different organizational levels. According to the main actor, there is a broad acceptance of the eHealth eID, and for the majority, it works well. However, there is also an awareness of the lack of acceptance and existing workarounds for example when the eID card is left unattended in the reader and/or shared among several users. Findings point toward users perceiving the handling of the eHealth eID as a complex obstructive process and confirm a lack of understanding and knowledge of its purposes. Hence, the user is crucial for the potential success of the eHealth eID, but empirical findings have confirmed several cases of problematic translations.

8.2.3 ITR

Knowledge and communication are very important aspects of ICT related introductions in general and eID introductions in particular. This organization, therefore, uses specially assigned roles at local health unit level to facilitate communication and dissemination of information from Central IT. There are several of these roles such as Local Authorization Administrators (LAAs) and IT Responsible persons (ITR’s). Motivated by their key role during the eHealth eID introduction, the ITR is considered an important actor in this analysis. The ITR is generally technically skilled in the role of providing local level technical support as well as informing local practice about the eID. The ITR also serves as a feedback channel reporting issues and problems back to the Central IT through established communication channels such as scheduled meetings.

8.3 The Obligatory Passage Point

8.3.1 Formulating the OPP

The eHealth case shows that the main actor seems fully aware that the identified actors in the network (eHealth eID, User and ITR) are crucial for the success of the eID introduction as well as acceptance and use of the eHealth eID. Hence the introduction process is heavily depending on the eHealth eIDs successful transfer to a stage where it is actually used according to instructions, the users’ ability and willingness to accept the use of the eID card as an integrated part of the daily work routine and the ITR’s across the organization to provide the needed information and support of the eID. Thus, from the main actor’s perspective, the central governing question is formulated as:

Is the eHealth eID going to be successfully introduced?
However, as shown in Figure 26, considering this central critical question as the network’s Obligatory Passage Point (OPP) (Callon, 1986) (see Section 4.3.4) it becomes clear that to pass this point and achieve success, for the introduction project to reach its goal, there is a clear relationship between the three actors whose individual perspectives must be negotiated in a positive way.

Figure 26. The OPP of the organizational level eID introduction (adapted from Callon, 1986)

Accordingly, these actors cannot negotiate and pass the OPP by themselves since they are all dependent on each other in the identified network surrounding the eHealth eID introduction. For example, the User is dependent on the eHealth eID to be able to accept and use it, and the ITR is dependent of the eHealth eID as well as the User to successfully support the introduction. Figure 26 also illustrates that each actor has its own path to follow towards the OPP, a path possibly affected by social aspects such as norms, beliefs and translations based upon their own individual perspective of the eHealth eID. Moreover, there is always the risk of an actor refusing to accept and stay within the network which in turn will result in its failure due to the high interdependency between these actors. For example, if the eHealth eID fails to deliver due to technical problems or the User fails to accept and use it, the introduction as a whole will not become a success. So this becomes the overall view of the network featured in this analysis with the OPP to be negotiated successfully in order to achieve a positive outcome, in turn, depending on the commitment of the identified actors. However, this network needs to be further problematized as will be elaborated below.
8.3.2 Problematizing the OPP

The OPP presented above needs to be further investigated and problematized since there are no evident potential obstacles blocking the individual paths towards the OPP. Figure 27 further expands the view of the OPP with a description of each actor’s obstacles, or problem areas, and goals as perceived by the main actor. In this figure, the six problem areas previously described are assigned to the corresponding actor, hence considered as a significant obstacle on that particular actor’s path. These obstacles can overlap and refer to each other since they are all more or less interdependent of more than one of the corresponding problem areas and this also being a consequence of the problematization being based on one single actor’s point of view, the main actor, and the intertwined character of this network. In addition, the goals of the actors also need to be further elaborated to better represent their individual views and translations.

Accordingly, the eHealth eID is assigned with the goal of reaching the state of the operational eHealth eID indicating a successful introduction from a predominantly technological, regulatory and legal focus. Further, the User is assigned with the goal of
providing high quality medical care putting an emphasis on the main purpose of the organization including medical as well as administrative and supporting staff acting as facilitators. The ITR is assigned with the goal of providing ICT related information and support to indicate that the introduction of the eID is only a part of this actors assignment of supporting local operations (Figure 27 above). Each of the three identified actors’ paths is further problematized by associating the actors to the previously identified six problem areas as derived from the identified challenges in the eHealth case as will be described more in detail below.

8.3.3 eHealth eID

The organization is problematized mainly due to its high level of heterogeneity and complexity. In addition, based on findings indicating that the main actor emphasizes challenges related to the technical complexity of the eHealth eID introduction, there is a clear potential risk of underestimating the organizational complexity as related to different types of health care units having different requirements and demands. However, the challenges of getting the eHealth eID to support local operations with high requirements on flexibility resulted in the introduction strategy of assigning specific health care units with a higher level of stationary work as pilots. Hence, this also poses the risk of just delaying the required handling of these problems. Since the eHealth eID is described as being based on a very complex technical infrastructure, placing technology on the path of the eID seems obvious. This is also motivated by the number of unforeseen technical incidents and problems that pose significant challenges for the introduction and on some occasions even temporarily halt the entire introduction process altogether. The eHealth eID is also presented with the problem area of management motivated by several factors such as an introduction strategy clearly focused on timely progress and number of organizational units covered hence potentially underestimating any organizational factors affecting it. Further, the introduction is based on an unproblematized top government decision to comply with the current law, in turn, raising the question about how to establish this decision in current practice in order to raise awareness and acceptance of the eHealth eID.

8.3.4 User

The problem area of current practice is placed along the path of the user in the network motivated on indications as reported by Central IT that there are several cases where users do not comply with the correct use of the eHealth eID. Hence this in turn indicating a conflict between the eID and current practice that should be taken seriously. Knowledge and communication are also described as problematic since some users are clearly lacking understanding about the aim and purpose of the eID which in turn can be related to communication being a problematic area. In addition, the eHealth eID itself is placed as an obstacle on the user’s path in the network mainly due to its problematic character as described in the previous section. Hence, if affected negatively by its own problem areas or obstacles, this will most likely spill over onto the user’s translations of the eID.
8.3.5 ITR

If negative consequences regarding the management of the introduction occur these will most definitively affect the ITR acting as an intermediary between Central IT and the operational level. The similar relation applies to the eHealth eID hence it is also assigned to the ITR. Hence, if the introduction faces challenges that result in negative consequences, these will most likely affect this actor supporting the local level. If the eHealth eID suffers negative consequences during the introduction, this will most likely counteract against it via affected actors’ translations. The highly interdependent role of the ITR is also strengthened by the addition of current practice to its path based on this actor’s position faced with the challenging task of trying to manage, support and establish the introduction on the operational level thus in turn highly affected by current practice at the healthcare unit.

8.3.6 Additional remarks

The fact that this is the first time this organization introduces an eID solution could account for several of the open issues and unforeseen events that had to be handled, but I argue that this is also a direct effect on the clear technological emphasis put on the process by the main actor Central IT. Up to this point, analysis shows that the complex and interwoven character of this introduction poses a significant challenge to overcome in order to reach the aim of a fully introduced, accepted and used eHealth eID and the most significant challenges are clearly related to the organizational and social context of the eID. According to the case, the fact that several of these eHealth eID cards are issued a significant time before the introduction does not seem to have any significant positive implications on this introduction. Hence, without any use of a digital service contexts certificates become outdated. Hence this strategy also has clear negative consequences.

8.4 Interessement

The main actor’s perspective of the eHealth eID introduction is that the following goals have to be reached in order to achieve success: (1) it has to be introduced to the organization and fully working, (b) it must be accepted as well as used as intended by the users and (c) the users should treat it as a valuable item. This can be seen as the result of a process where different actors and their mutual relationships have an important role to play. In addition, there is also a need for a common consensus of translations of the purpose and aim of the eHealth eID. The result of the previous problematization must also be investigated with a clear focus on these actors’ individual relationships since they each can submit to the participation in the network or take their matters elsewhere; i.e. to opt out of the network. One clear example of this is the silent non-human actor - the eHealth eID. If for some reason the eID solution would fail completely, e.g. by a severe security flaw in technology or a data breach compromising the entire eID operations. With no chance of recovery, this would mean a fatal blow to the relationships in the network formed around the eID introduction and in turn quite instantly render the
whole network obsolete. In short; without a working eHealth eID solution there will be no working eID solution to introduce. The consequences of the other actors, the User and the ITR, not complying with the network will most likely be a bit less dramatic but as will be shown; far from less problematic. The actions of interessement (Callon, 1986), as performed by the main actor thus aim at locking the actors or allies into place within the network, to interest them. The network is formed as a result of the problematization and its interdefinition actors’ identities, roles and attributes as based on aspects such as tendencies and goals as translated by the main actor. The interessement, therefore, serves as the acknowledgement of the fact that the actors within the network can have identities that are defined in ways competitive to the network and during this process the main actor uses different kinds of interessement devices to try to get them to commit to the network and stabilize their identity within the same. The interessement consists of the actions or efforts, to keep possible outside actors from affecting the identity of the actor and keeping them aligned with the network. The aim of interessement is, therefore, to possibly disrupt or weaken any efforts of outside influences affecting the actors within the network to form a kind of barrier between the network and the possible negative influence of the outside world.

8.4.1 eHealth eID

In Figure 28 below, the triangle of interessement (Callon, 1986), is illustrated for eHealth eID with the introduction strategy being used as a means of handling potential problems and risks possibly affecting the introduction process, the outside influences represented by complexity, technology and management. Thus, the introduction strategy is identified as the interessement device, illustrated by the arched arrow, to keep these external influences from affecting the introduction in a negative way.

Empirical findings show that the organization for example in terms of its complexity is a recurring characteristic of the eHealth introduction. The organization has also been described as inhibiting a high level of heterogeneity ranging from general to highly specialized medical care and the existing working conditions for staff has been described as ranging from strictly stationary to very flexible. Accordingly, the case shows that the
more specific health care provided, the stronger the requirements to be able to use the eID in a more flexible way as related to the aspect of space and time. Central IT, therefore, tries to manage these aspects of the organization from negatively affecting the introduction of the eHealth eID by introducing it at less complex organizational units such as local health centres prior to the more complex and critical ones. In turn, a high level of flexibility also poses a considerable challenge to handle during the introduction, for example, related to considerable reconnection times when switching workstations. Therefore, the aim is to introduce the eHealth eID at less flexible health care units while these problems are hopefully solved prior to addressing more critical and complex units.

The technology involved in the eHealth eID introduction is clearly described as a challenge to handle by the main actor. Apart from the view describing that security solutions such as the eID tend to be very complex per se, it also becomes apparent that the introduction of the eID also requires an extensive integration between existing technology and the technology prescribed by the eHealth eID solution. Further, the outside influence of technology already showing its ability to influence the eID introduction in a negative way when the entire project is completely halted due to problems that occurred during the introduction. However, the strategy applied during the introduction is focused on solving any technical problems related to the eHealth eID on a case by case basis. A clear example being the Single-Sign-On (SSO) solution to simplify the login procedure and improve the performance of reconnecting user sessions.

Management is also a strong force affecting the introduction, and by management, I hereby mean strategic decisions and measures that counteract or negatively affects the eHealth eID introduction process. For example, the very tight timeframe upon which the introduction project is initially launched in turn sets the tone for the whole project, i.e. the introduction is rushed on time by a stepwise covering of health care units and counting the number of eHealth eID cards issued. However, as the timeframe is deemed too optimistic, it is later revised on repeated occasions which in turn confirms that the initial project incentives can be questioned. Further, the management and coordination of different projects affecting each other regarding local technical prerequisites are far from optimal. For example, the introduction of the eHealth eID would have been much smoother and unproblematic if the Hardware and Software (HoS) project would have taken the lead and the eID introduction had followed in its wake. Thus, instead of facilitating the introduction process several management decisions instead presented additional obstacles along the introduction process.

8.4.2 User

The next triangle of interessement focuses on the User with the identified interessement device of the Estimated Benefits Strategy (EBS) as illustrated in Figure 29. The main actor acknowledges that there are problems with the users when it comes to the acceptance, use and handling of the eHealth eID and the possible outside influences are
identified as current practice, knowledge and communication as well as the eHealth eID itself.

![Image of Triangle of interessement – User (adapted from Callon, 1986)]

Figure 29. Triangle of interessement – User (adapted from Callon, 1986)

As previously described, specific requirements from current practice regarding the flexible handling of the eHealth eID poses a significant risk of influencing the introduction process in a negative way. For example, since the prescribed handling of the eHealth eID describes that it should never be left unattended, the problems with significant re-connection times when re-inserting the card results in users not handling the eHealth eID according to instructions. The tendency of leaving the eID in the card reader while attending to other duties is a clear indication of how requirements of current practice in terms of flexibility influence the eID usage. Hence the eID does not seem to match duties that have a high demand for flexibility, and by focusing on less critical and less flexible health care units, there should be a clear risk of just pushing these problems ahead since they will most likely be more significant in the more critical units such as emergency care. Knowledge and communication appear to be a key aspect when it comes to the user’s attitudes towards and understanding of the eHealth eID. This assumption is also motivated by the reported consequences of a significant lack of knowledge and understanding of the purpose and aim of the eHealth eID. The user often lacks the knowledge and ability to identify and assess the direct cause of ICT related problems and with this lack of knowledge the tendency is to blame the last introduced solution such as the eID in this case. Further, there are users who clearly question the meaning of the eHealth eID altogether which in turn is a clear indication of an inherent lack of knowledge and understanding about its purpose, the safeguarding of patients’ sensitive data, and some even think it is introduced with the sole purpose of causing problems for users. From the user’s perspective, the eHealth eID itself is also identified as an external influence on the introduction. As Central IT reports that several users show a clear resistance to the eHealth eID that in turn can be a consequence based on several different reasons. For example, if the eHealth eID, in fact, introduces obstacles in current practice this
poses the risk of potentially affecting the user in such way that norms and values develop a resistance to the eHealth eID. Hence, these negative influences can turn into a resistance both on the individual level and also shared among actors as a socially established consensus. Further, if users have previously experienced problems as related to the introduction of new ICT systems or artefacts in the workplace, this can also affect actors’ norms and values in such a way that the eID meets users that are negative by default. Since Central IT reports that several users do not use the eID as intended for no obvious reasons, I argue that the eHealth eID as related to the assigned norms and values on actor level, should, in fact, be a matter of concern and a plausible cause for this unexplained behaviour that in turn could jeopardize the eHealth eID introduction by decreasing the information security level instead of increasing it.

8.4.3 ITR

The third triangle of interessement is focused on the ITR where the Communication strategy is been identified as the interessement device. Since this strategy is built upon the relation between Central IT and the ITR with the latter having the responsibility of forwarding information to local operations as well as supporting and reporting back eHealth eID related issues. It, therefore, becomes crucial for Central IT to keep the ITRs as allies within the network and the chosen communication strategy of using the ITR as a spokesperson as well as an informant on the local operational level. The potential external influences influencing the ITR have been defined as management, eHealth eID and current practice as illustrated in Figure 30.

![Figure 30. Triangle of interessement – ITR (adapted from Callon, 1986)](image)

Management in terms of the chosen introduction strategy is clearly indicated as having a negative influence on the ITR. The very tight timeframe and the strategy of solving technical problems as they occur can potentially put a strain on this actor since unforeseen technical problems, in turn, affects local operations in a negative way. As related to the external influence of the eHealth eID, with the organization having adopted a strategy where users are responsible themselves for staying informed e.g. by the active
use of the Intranet, the ITR is also presented with the challenge of disseminating information of the eHealth eID on local operational level for example regarding its aim and purpose. Hence, the ITR is responsible for the introduction at the local level but must also face any existing negative norms and values of the eHealth eID among staff. *Current practice* finally, is of course of significant concern when it comes to the ITR’s role and duties in the network.

The resistance to correct handling as well as any negative attitudes towards it should be a highly prioritized aspect for the local ITR to handle and one of the external influences most immediately affecting the eHealth eID introduction in a negative way besides technology. If users do not use the eID card according to instructions and stay negative towards it, the aim of increasing the security level across the entire health care organization will not be met. Based on these potential external influences the interessement device of the communication strategy clearly transfers the responsibility of informing and aligning operational practice with the eHealth eID from Central IT to the ITR. As an example, a large amount of reported issues at local level results in users being instructed to support themselves via the Intranet which in turn can be seen as a far from optimal solution.

### 8.4.4 Additional remarks

Since the eHealth eID is represented as an actor as well as a potential external negative influence, this indicates a clear relationship between the triangles of interessement presented above. Figure 31 below shows this dual role of the eHealth eID as illustrated by the emphasised arrows. The eHealth eID is an actor itself as crucial for Central IT during the introduction and in turn also an external influence of the ITR’s duties to support the introduction at a local operational level as well as the User. Therefore, the eHealth eID becomes a subject in the interessement device for the ITR’s communication strategy and also an extremely important prerequisite to the ITRs work of supporting the introduction at local operational level. If the eHealth eID in any way becomes negatively influenced, the role of the eHealth eID as an external influence possibly influencing the ITR as well as the user in a way that is not in line with the aim and goal of the network. Therefore, I argue that it is very important to keep this relationship in mind for the main actor when addressing the network.
To summarize, the stage of interessement of the translation analysis corresponds to the previously described problem areas identified during problematization. It becomes clear that Central IT has mainly focused on technical and management aspects during the introduction but nevertheless at the same time acknowledges the importance of the role played by the user and ITR. Thus, during the interessement stage, problem areas related to acceptance and use of the eID are further elaborated and categorized as related to current practice as well as existing norms and values of the eHealth eID. A new dimension is also brought into the scene by further studying the ITR and its possible external influence. Yet another interesting and important finding is the identified relationship between these three triangles of interessement as related to the user as well as the ITR via the eHealth eID as an external influence on these actors.

8.5 Enrolment

By now it should be clear that the road from interessement to actual enrolment is never a clear cut or deterministic one since the devices formed to serve the interessement do not necessarily lead to the keeping of the alliances and actual enrolment among the actors within the network. The focus of enrolment (Callon, 1986) (see Section 4.3.4) is thus on the definition of a set of interrelated roles and their attributes in the network and to what extent the actors accept them. A successful enrolment is, therefore, dependent on a successful interessement, but in addition to this, there is also the need for further negotiations to get the users enrolled in the network. As an example, from the main actor’s perspective; to be able to enrol the users, they must willingly accept and use the eHealth eID but judging from the case, this process seems far from straightforward. Up
to this point, the previous stages of the translation analysis, i.e. from problematization to interessement, have been based solely upon the perspective of the main actor, in this case, Central IT. However, the following stages of the analysis will be based on the actual outcome of the introduction of the eHealth eID as translated by the affected actors. This shift in perspective provides further insights and findings regarding the outcome of the previous stages of the translation analysis.

8.5.1 eHealth eID

One prerequisite for the identified network to reach its goal of a successful, accepted and used eHealth eID is, of course, the eID itself. Hence, the introduction of this artefact becomes a crucial part of the network. The focus here is how the external influences can possibly affect the introduction process from a project point of view. The organization in terms of its heterogeneity and complexity pose significant challenges as previously described. However, Central IT emphasizes the complexity in terms of technological and process related aspects rather than organizational heterogeneity. The introduction strategy with a focus on first approaching less problematic and less critical health care units and solving technical issues on a case by case basis therefore neither acknowledges nor addresses the fact that the characteristics of the organization diverge from the prerequisites of the eHealth eID. This reactive behaviour is also a recurring pattern of how technical as well as user related issues are handled with the exception of the EBS.

Despite the fact that the eHealth eID is perceived as an obstacle, Central IT tries to enforce compliance with estimated benefits added to the card. Technology, with an emphasis on technological challenges, is a significant influence during the introduction. For example, severe problems occurring during the rollout cause a complete halt to the entire introduction project. However, I argue that these technological problems and the difficulty of predicting them can, in turn, be traced back to the nature and characteristics of the project. When introducing this kind of solution across the entire organization which also has a high level of heterogeneity, it will be extremely hard to foresee and act proactively regarding potential technological challenges ahead. Not going into any specific details about the complex character of health care (see Section 1.5.2), this study nevertheless shows that this artefact is perceived differently from a clinical working context as compared to an administrative. So far, the eHealth eID is integrated with only a few systems such as the Electronic Patient Records (EPR) system, but according to future plans, this way of authentication will be integrated with a growing number of ICT systems. There will, therefore, be considerable challenges with technical integration ahead. However, the inability to test the eHealth eID with every single configuration and with a full service load also results in users severely doubting the quality of the software being rolled out. Although, some users show an understanding attitude towards these problems they are inevitably affected negatively in their working situation. Management has also influenced the eID introduction in the way that the project itself is based on a top management decision initiates the project; a decision that has not been questioned, problematized or negotiated at all. However, this probably due to the fact
that this decision is a clear way of finally adhering to the current laws requiring strong authentication. The main actor also states that the top management decision has been a positive way of motivating the project towards the organization, but this strategy has also caused problems. Users report that they have a hard time understanding the why’s of the of the eHealth eID when the how’s have only been communicated. Therefore I argue that basing an introduction solely on what should be done, i.e. that the eHealth eID must be used, poses a significant risk of the organization failing to understand the motives. Hence, local translations of the purpose of the eHealth eID are significantly different, and there are also users stating that “this is the way it’s done in this organization”, i.e. confirming the tendency of informing what to do while not emphasizing why it should be done.

Management also clearly influences the introduction project by setting the timeframe and a very clear focus. However, this timeframe seems not sufficiently grounded in practice since the project deadline is postponed on several occasions. The national management of the SITHS solution also affects the eHealth eID introduction via regulations and updates which result in additional activities such as renewal of certificates. All three external influences of organization, technology and management are confirmed as having a negative impact on the project despite the interessement device of the introduction strategy. Therefore, I argue that the main actor’s ability to act upon these organizational, technological and managerial obstacles becomes a key factor. The ability to adapt the introduction strategy also becomes a key issue since this project has to adapt to the contexts of these external influences.

8.5.2 User

The user is another key actor during the eHealth eID introduction acting as a spokesperson for users across the organization that need to accept and use the eID in order for the introduction to succeed. The focus here is how the user responds to with the interessement device of the EBS as the preferred way of the main actor to keep this actor committed to the network and keep any negative external influence at a distance. Current practice as exemplified by the requirements of flexibility is a clear example of an outside influence that has only been briefly considered and touched upon by the main actor. However, this aspect has significantly influenced how the eHealth eID is perceived by practice. Users performing mainly stationary work perceive the eID to be working quite well as opposed to staff at the hospital clinic who complains over the perceived obstacle of removing the eID when they have to leave their workstation for other duties. Other problematic aspects are also put forth such as the ability to swiftly switch between workstations. However, despite the interessement device (EBS) used for the enrolment, the users with the highest demand for flexibility seems to be significantly influenced by the flexibility, and it seems that the functionality of the eID still does not fully match their demands. Thus, regardless of estimated benefits added to the eHealth eID, the prescribed use of the eID still diverges from their daily working routines such as not providing the needed flexibility. This is therefore seen as an important factor
leading up to users not adhering to the correct use of the eID by leaving it unattended in the card reader. **Knowledge and communication**, an external influence characterized by how lack of knowledge, understanding and information of the aim and purpose of the eHealth eID can possibly negatively affect the user’s willingness or ability to enrol and stay within the network. Regarding the enrolment of the eHealth eID, there is a reported clear lack of information motivating why the eID should be used that in turn results in a lack of knowledge of the purpose of the eHealth eID. This argument is also strengthened by the fact that there are very clear differences in how the purpose of the eID is translated by users. The most evident example of the **eHealth eID** itself acting as a potentially negative influence on users is the reported contradiction between the mission to provide high quality health care and adhering to the use of the eID to increase the level of information security and meet prescribed standards.

Highly institutionalized norms and values of health care, in fact, poses a direct threat to the eID introduction. In addition, this creates the intricate dilemma at user level of how to act upon central directives if these, in fact, have a negative impact on the organization’s main mission. Despite this, Central IT tries to overrule these norms and values with the EBS hence not addressing the root cause of this problem, the divergence between the eHealth eID use and the focus on providing medical care. In addition, it is quite hard to see how these norms and values could be affected by trying to increase the perceived value of the eID card since the downplay of integrity and security in favour of providing the best possible medical care is no novelty in the health care sector; aspects of integrity and security have not been put in the foreground historically.

8.5.3 **ITR**

The ITR have a key role to play in the network since this actor represents highly IT-skilled staff with an operational background and a responsibility of acting as an intermediate between the main actor and the users on the local operational level. The ITR is assigned to tasks such as general IT support, informing local staff about IT related issues and reporting back critical issues to the main actor. Thus, in the network, the ITR has a role of acting as active facilitators regarding the introduction of the eHealth eID. Hence, in its key role the ITR becomes very important on the road to a successful eID introduction. **Management**, in the form of the introduction strategy, clearly puts stress on the ITR during the actual introduction at the health care unit and in some cases the focus on supporting the eID prevented this actor from managing the duty of supporting local operations. Further, the ITR is also faced with the task of trying to translate and disseminate the need of an increased security level as imposed by management in turn reported as a challenging task due to the abstract character of information security as related to the eHealth eID. As the introduction faces several technical problems and challenges, the role of the ITR is to negotiate and inform local operations about these disturbances. The **eHealth eID**, as introduced according to the introduction strategy, is an important prerequisite for the ability of the ITR to perform duties hence also forms the relationship
between triangles of interessement of the eID and the ITRs. Hence, in order to successfully support the eHealth eID introduction, the ITR is dependent on a successful introduction of the same. If there are problems with the eHealth eID, the users will report this immediately, and any disturbance regarding the eID at the local level will immediately affect and influence the ITR. Current practice is, therefore, a significant external influence on the ITR and users are depending on the ITR regarding IT support in general and eID related issues in particular. The ITR are fully aware of users not willing to comply but is left with no other means than to repeatedly inform about the misuse. Findings also point towards that there are examples of the ITR being quite resigned to the fact that it seems very difficult for a current practice to comply with the correct use of the eHealth eID.

8.6 Mobilization

In the problematization, the identity, relationships and goals of the different actors are formulated, and in the following stages of the analysis, a network of actors and relationships are created. However, the consensus within the network is never stable based on the fact that the network itself is based upon generalized translations and negotiations. The stage of mobilization (Callon, 1986) (see Section 4.3.4) addresses the fact that the network is formed based on a few representatives from each category of actors acting as spokespersons. The user is maybe the most significant one thus representing users of the eHealth eID within the organization. However, the question of how the group of actors will follow their representatives in the network. Thus, mobilization will indicate how this network will actually take effect in practice. If mobilization is successful it means that: the eHealth eID is introduced successfully, it is used according to the instructions and it is accepted and translated in line with instructions across the organization. Thus this makes the stage of mobilization very interesting since the main actor representing only a handful of people discusses the introduction that will directly affect the everyday working routines of some 14 000 individual users. The main actor forms relations with only a few actors within the organizations and relies on the interessement devices for successful introduction of the eID across the organization.

8.6.1 eHealth eID

As being a non-human actor, it seems reasonable that the eID in the introduction itself is rather easy to enrol and mobilize within the network. However, the eHealth eID has caused several problems during the introduction mostly due to the main actor’s difficulty to foresee consequences of organizational as well as technological complexity during the introduction. By piloting the eHealth eID at selected local health centres, Central IT pushes forward the handling of the eID at more flexible and critical locations. Thus the representativeness of these locations in terms of needs and demands becomes an important factor. Hence, from the main actor’s point of view, when the eHealth eID is introduced at a health unit, its users are considered as eID users regardless of the individual acceptance and potential negative translations of the eID. The users and units
covered by the introduction are transformed to numbers reported back to top management. This not being at all unique in IT related introduction projects but this particular project’s successes hangs in the balance if the users do not fully understand the purpose of the eID and adhere to its instructions and regulations. In a way, with the eHealth eID, the main actor is trying to change the working routines of the staff and how the eID is perceived and is doing this by treating the users as a relatively silent actor only represented by a few.

8.6.2 User

The main actor negotiates the interessement and enrolment of the user based upon how the eHealth eID is perceived by very few users as representatives bringing forth problems regarding the eID. Hence, the entire group of users becomes a rather silent actor for Central IT, but in practice, this group is far from silent. The users of the organization speak quite freely and open of how they perceive ICT related introductions in general and the eHealth eID introduction in particular. Further, a quantitative approach is applied since the introduction is measured and reported by the number of healthcare units and users covered. This instead of ensuring that the eHealth eID is properly introduced and accepted by concerned users. Negotiations revolve around the issue of not leaving the eID in the card reader, therefore, the act of removing, or rather not removing, the eID from the card reader becomes crucial. When the user removes it, this is the clear sign of adhering to the instructions and acknowledge the enrolment into the network. On the opposite, leaving the eID in the card reader when leaving your workstation is like saying ‘I’m not going to follow the instructions since they have a negative impact on my work’.

One additional aspect to keep in mind is that the introduction of the eHealth eID is neither based on any organizational benefit approach nor requested by staff. Hence, without bringing any clear benefit for users apart from increasing security levels and adhering to the law, there is a potential risk of perceiving the eHealth eID as solely a burden, especially if it is related to technical problems and does not converge with the daily work of users. In addition, from the main actor’s perspective, there also seems to be a lack of identifying and acknowledging different requirements and needs based on different professions and roles in this complex organization. Hence, it is up to local ITRs to facilitate that the local health centre or clinic confirms to the pressure of using the eID according to instructions. Thus, this becomes a significant challenge since there are administrative staff as well as different levels of clinical staff involved. Hence, the users are seen as more or less as one group of individuals becomes problematic when this group, in fact, can be divided into a number of very specific subgroups. The technological complexity is addressed, but the organizational requirements are left unproblematised to a significant extent.
8.6.3 ITR

The ITR has a crucial role in the network acting as an intermediary between Central IT, the eHealth eID and the user respectively. Hence, the ITR has the dual role as spokespersons for the main actor as well as the users. One relevant question here is what happens if that role could mean a clash of interests? Which side will the ITR take if there is a conflict of loyalty between the main actor and the solidarity towards colleagues? As indicated, the ITR shows signs of resignation when staff does not comply with eID instructions, in turn, being a result of not pushing its mandate awarded by the main actor too far. Further, it seems that the ITR is appointed based on personal interest in ICT rather than the managing skills required to convince and motivate staff. Communication wise, the ITR can speak for itself in the communication with the main actor, but users are treated as being quite silent. However as we know, this group can have strong opinions about the eID and in turn, can show their discontent by neglecting the instructions. Although the ITR should act as a first line support for local operations, in times of high pressures users look for other ways to get support.

8.7 Closure

Even though one could argue against using the term closure in a context of an introduction project especially when the case study did not follow the introduction of the eHealth eID to the end. However, I argue that this added final stage of the analysis is motivated since it also becomes the closing point for this analysis. Hence, this stage presents the outcome of the different stages of the translation analysis performed above as the potential outcome of the controversies caused by the representativeness and generalized negotiations as inherent in the constructed network. The introduction of the eHealth eID is governed by the interessement device of the introduction strategy. Clearly forced on time and progress and communicated in terms of health units covered. However, the timeframe has been revised several times and the most critical units still awaits introduction.

During interessement, the potentially negative influence of complexity, technology and management is identified, and during enrolment, it is concluded that all three of these aspects have already influenced the introduction process so far. Thus, hopefully, management will henceforth formulate a more realistic timeframe but still the complexity and technology are acknowledged by the main actor as significant obstacles to overcome during the continued introduction in turn confirmed by the translation analysis. The case study shows that as far as the main actor knows, with a few exceptions, users have mainly a positive attitude towards the eHealth eID. However, the behaviour of leaving the eID unattended in the card reader needs to be minimized and handled by increasing the perceived value of the eHealth eID. The top management decision to introduce the eHealth eID as a means of adhering to the law is seen as a powerful tool to support the introduction, but the main actor also acknowledges that the perceived value of the eID
Translating the eHealth eID

might have to be addressed to minimize the misuse. The interessement device of the EBS is seen as the proper way of increasing the perceived personal value by adding functionality such as private use that in turn will make users treat the eHealth eID card as they should. However, interessement and enrolment provide insights indicating that user’s translations of the eID have already been influenced in several negative ways by how the introduction is managed, technological problems and different specific requirements of this heterogeneous organization. For example, for the larger and the more flexible health care units, there are greater potential risks of obstacles since such characteristics of operations have been proven to be difficult to support with the eHealth eID solution. From a user perspective, there is a reported lack of knowledge of the purpose, aim and motivation for the eHealth eID which in turn significantly affects translations of the eID and in turn clearly affects how it is used in the workplace. Referring to a top management decision that the eHealth eID should be used for increase security levels does not seem enough to be able to ensure acceptance and adherence among users. The ITR is enrolled into the network with the use of the interessement device of the communication strategy. Hence, the main actor is depending on the ITR supporting the local practice during introduction, but at the same time, the ITR is given the dual role of acting as a spokesperson for the main actor as well as the users at the local health center. Hence the ITR is in turn influenced by the enrolment of the eHealth eID as well as the enrolment of users, and in the end, this can be seen as just one additional ICT related task for the ITR.

8.8 Concluding remarks

This translation analysis is based on the three principles of agnosticism, generalized symmetry and fee association (Callon, 1986). The first principle allows us to treat uncertainties about the eHealth eID, the users and the ITRs in the same way and the analysis is performed by avoiding preconceptions of these three perspectives put forth. For example, the main actor’s belief that the eHealth eID will be accepted and used across the organization and the users’ tendency to leave the eHealth eIDs in the card readers is never judged or questioned. In line with the second principle, the same vocabulary is used throughout the analysis regardless if dealing with technical or social aspects. Hence, all stages of the analysis are applied to the technical artefact (the eHealth eID) as well as the user and ITR. The third principle allowed us to describe all variations which affected the relations and alliances without locking them into fixed positions. Hence, this enables the identification of variations in the relationships between the actors. Further, unpredictable relationships between the actors and external influences are also taken into consideration. This is also made possible by not locking our position regarding any predefined roles. This provides the opportunity to show how different influences affected the actors within the network in ways that we hardly would have found by using other analytical approaches. Further, the identified actors are confronted with different obstacles and uncertainties as relevant from their respective perspectives. In the analysis, the main actor has spoken in the name of the eHealth eID, the user and
the ITR up to the stage of interessement. Thus, in the following stages of enrolment, mobilization and closure, the perspectives of the user and ITR are based on empirical findings. Further, there is a clear progression during negotiations from the initial problematization to mobilization, and the aim of the final stage of closure is to bring together findings from the previous stages of the translation analysis. This analysis also focuses on the power of relationships. The translation is not designed to identify symmetry but rather used as a way of describing a complex process that intertwines several aspects of social and technical aspects. This analysis is also an example of how a few representatives take on the role of being spokespersons for others more or less silent actors and how they are handled during the different stages of translations. To be able to introduce the eHealth eID across the organization, the main actor needs to identify important actors involved in the network and try to identify and understand their different agendas of needs and goals.

On the other hand, every actor related to this network has the ability to form their own translations which in turn might be in line with the overall goals and means of the network or possibly overthrow it completely. The aim of this analysis is therefore to show the importance of translations, relationships and possible influences among actors affected by the eHealth eID introduction. By perceiving and handling this introduction as mainly a technical and regulatory effort, I argue that there are clear potential risks of neglecting the importance of the direct influence of how the individual users translate the eHealth eID. Thus, for the eID to function in a positive way it must not only be introduced and used; the users need to understand its purpose and the possible consequences of misuse. In essence, this is about gaining knowledge about the fact that the user with the correct handling and use if the eHealth eID, safeguards sensitive information with their own existence and to communicate this across the organization should be considered a very important but at the same time significant challenge. The users should not only use their eHealth eIDs; they should use them on their own as well as the patients’ best interest.

Although this could also indicate a need for shift in existing health care paradigm; it is not only about delivering high quality health care; it about delivering high quality healthcare in the highest possible way concerning integrity and secrecy regarding the patients. With the increasing use of ICT in health care operations, more and more possible single points of failure is constructed regarding unauthorized access to sensitive information. This analysis also shows that to facilitate a correct conformance to the eHealth eID; information needs to be introduced and acknowledged in practice. However, judging by the findings, users tend to translate the eID based on their own working situation rather than acknowledging the eID as an artefact for increased patient security. The summarized findings from the translation analysis presented in Table 21 will serve as an important input to the upcoming final analysis and discussion in Chapter 9. In
detail, this summary provides an overview of the translation process from central problem areas (problematization), via how these problems are managed by the Board (interessement) as translated by actors (enrolment) towards the outcome (mobilization). However, in this summary, the final stage of closure is omitted since it is not part of the original process as suggested by Callon (1986).
<table>
<thead>
<tr>
<th>Actor</th>
<th>OPP</th>
<th>Problematization</th>
<th>Interessement</th>
<th>Enrolment</th>
<th>Mobilization</th>
</tr>
</thead>
<tbody>
<tr>
<td>eHealth eID</td>
<td>Operational eHealth eID</td>
<td>Organization</td>
<td>Introduction strategy</td>
<td>High levels of technological complexity and dependency</td>
<td>Problems due to complexity and technology must be addressed on occurrence.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Technology</td>
<td></td>
<td>Project stopped due to technical problems.</td>
<td>Project can be halted at any time, i.e. a stop/go progression.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Management</td>
<td></td>
<td>Non-optimal project management model.</td>
<td>Project plan will need to be re-revised.</td>
</tr>
<tr>
<td>User</td>
<td>Provide or facilitate provision of high quality medical care</td>
<td>Current practice</td>
<td>Estimated Benefits Strategy (EBS)</td>
<td>Lack of knowledge affects acceptance.</td>
<td>Users will question the eID and resist acceptance.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Knowledge and communication</td>
<td></td>
<td>Norms and values override correct handling.</td>
<td>Norms and values will not converge with use of eHealth eID.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>eHealth eID</td>
<td></td>
<td>Prioritized provision of health services.</td>
<td>Provision of health services will always override information security.</td>
</tr>
<tr>
<td>ITR</td>
<td>Provide ICT related information and support</td>
<td>Management</td>
<td>Communication strategy</td>
<td>Smaller more stationary units are more easily introduced and supported.</td>
<td>Health units with less optimal fit will continue to struggle with eHealth eID.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>eHealth eID</td>
<td></td>
<td>The eID problems immediately affect local operations.</td>
<td>eID problems will be an increasing burden for ITRs to handle.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Current practice</td>
<td></td>
<td>Users not adhering to instructions affect introduction and use.</td>
<td>There will always be users not adhering to the eID and risk information security.</td>
</tr>
</tbody>
</table>
Part IV – Discussion and conclusions

The fourth and final part brings together findings and insights from translation analysis (Chapter 7 and 8) with the theoretical and analytical perspectives to provide a final synthesised analysis and discussion in Chapter 9. This chapter also concludes with emerging concepts that are further elaborated in Chapter 10 and presented along with conclusions, implications and suggestions for future research.
9. Concluding analysis and discussion

This chapter is the part of the dissertation when the main areas of theoretical and analytical perspectives (Chapter 3 and 4), empirical evidence from the eGov and eHealth cases (Chapter 5 and 6), and translation analyses of these two cases (Chapter 7 and 8) are brought together for a final analysis and discussion. Also providing the described suggested synthesis of the sociological and institutional perspectives by applying the socio-institutional framework, the chapter will be structured according to the suggested four stages of this framework. This provides the theoretical and analytical concepts and insights as well as the structure to form and evaluate the proposed relationship between actors’ translations and institutional barriers. To conclude this chapter, three significant emerging concepts are presented to be used as a basis for final conclusions. This chapter, therefore, addresses the second (RQ-2) as well as implicates the third (RQ-3) research question.

9.1 The socio-institutional framework

As described, the socio-institutional framework applied in this chapter consists of two synthesised perspectives (see Chapter 4). The institutional perspective to provide the analytical lens to be able to (1) characterize and describe institutional pressures and barriers on a general level and (2) describe and assess their underlying institutional factors and predictive dimensions. This perspective also facilitates (3) the categorization and assessment of institutional pressures in terms of strategic responses and tactics launched to negotiate the outcome. Based on the previously described notion of perceiving barriers of an equal type as pressures, this perspective also facilitates institutional barriers to be addressed in a similar way. In contrast, the sociological perspective builds on the analytical findings and concepts from applying the described framework of ‘the sociology of translation’ (Callon, 1986), referred to as translation analysis (See Chapter 7 and 8). Thus, findings from each stage of the translation analysis such as identified problem areas bring the organizational and operational levels into this analysis. Hence, this analysis is performed with the aim of identifying central concepts to be further refined into conclusions in the final chapter. In line with the perspective and methodology applied in this work (see Chapter 2), emerging concepts presented throughout the analysis thereby represent abstractions of the interpreted empirical worlds. Further, aspects and details of institutional pressures and barriers are generated abstractions as based on my interpretations of the findings in the two cases. Hence, during this analysis, these abstractions will be further densified and conceptualized in order to facilitate an appropriate level of generalizability in upcoming conclusions (see Section 2.2.3). Since this framework comes with a certain level of complexity, for maintained transparency, I choose to structure this analysis in accordance with the identified stages of the previously described four-stage institutional model (see Section 4.4). In this outline (below),
each of the four stages are assigned with two sub-stages, each assigned with an important purpose and aim in this analytical process. Hence on a general level this process covers the exertion of institutional pressures to conform to the introduced eID programs, via the development and negotiation of barriers, to a potential institutionalization of barriers as well as a re-institutionalization of pressures. Each stage provides findings and insights along this path to facilitate the progression through this analysis to better understand the development of barriers as well as these barriers in turn influence pressures.

Throughout this analysis, theoretical concepts and proposals put forth in Chapter 3 and 4 will be used as a basis for discussions and reflections on emerging concepts in the light of extant theory and research in areas previously described as relevant. The application of the described socio-institutional framework results in the analytical model illustrated in Figure 32 (below) is also showing the relations to previous chapters as bringing important empirical and analytical inputs to this analysis.

**Stage 1: Pressure**
- Characterization of pressures
- Institutional factors and predictive dimensions

**Stage 2: Barrier**
- Characterization of barriers
- Institutional factors and predictive dimensions

**Stage 3: Negotiation**
- Pressures vs barriers
- Strategic responses and enrolment

**Stage 4: Institutionalization**
- Institutionalization of barriers
- Re-institutionalization of pressures

**Stage 1: Pressure** consists of sub-stages to characterize and describe institutional pressures on a general as well as on a detailed level assessing underlying institutional factors and predictive dimensions (Oliver, 1991). Thus, this first stage presents the needed overview of the pressures to be further analysed in later stages and is in turn based on empirical findings regarding basic constituents of pressures such as historical paths, official initiatives, government instructions and investigations as well as laws and directives (see Section 5.1 and 6.1).
Concluding analysis and discussion

Figure 32. Analytical model

**Stage 2: Barrier** is in line with the described suggestion of treating institutional barriers as equal institutional counterparts of pressures hence the same sub-stages are applied here. However, the empirical basis of this stage is the previous problematization (Callon, 1986) performed as the initial stage of translation analysis (see Section 7.1 and 8.1). This provides a problematized organizational view of pressures in order to introduce and characterize the barriers in turn based on actors’ problem areas and obstacles.

**Stage 3: Negotiation** provides a comparison of pressures and barriers as based on previous assessments of institutional factors and predictive dimensions. This also includes a discussion to bring a better understanding of similarities, differences and implications. Next, two illustrative examples of strategic responses and enrolment will be described and further discussed in the light of relevant theory. Hence, the typology of strategic responses (Oliver, 1991) will here be merged with results from interessement and enrolment (Callon, 1986) in translation analysis (see Section 7.4-7.5 and 8.4-8.5) to be able to analyse and discuss the negotiations enacted as well as the outcomes from an operational perspective.

**Stage 4: Institutionalization** is the final stage based on the concept of institutionalization as well as the results from mobilization and closure (Callon, 1986), implications of pressures and barriers are put forth. These implications are focused on the influence and further development of barriers (institutionalization of barriers) as well as on further influence on pressures (re-institutionalization of pressures). Two episodes, one from each case, will be used to illustrate and motivate the suggestions put forth.
9.2 Stage 1. Pressure

9.2.1 Characterization of pressures

This initial characterization of pressures focuses on the initial environmental pressures to introduce these eIDs put upon the main actors in the covered cases. Hence, these actors become catalysts or facilitators of the pressure being further exerted in their area of responsibility, i.e. the Board’s mandate to cover the entire public sector and Central IT’s responsibility of the health care organization. Hence, this characterization will facilitate an increased understanding of why the Board introduces the eGov eID and why Central IT is faced with the challenge of introducing the eHealth eID. The clear challenges these main actors face during the introduction will be further analysed and discussed in the later problematization of these pressures. Thus the external environmental pressures (DiMaggio & Powell, 1983) put upon these central coordinating actors in both cases are aimed at an increased conformity of eIDs in the public sector (Zucker, 1987). These are examples of introducing homogeneity or isomorphism (DiMaggio & Powell, 1983) into the area of eGovernment.

With on the one hand the eGov eID acting as a key for development of external digital services (Melin et al., 2013; Rössler, 2008; Seltsikas & O’Keefe, 2010) and on the other hand the eHealth eID facilitating internal secure authentication in order to safeguard patient confidentiality (e.g. Anderson, 2006; Hedström et al., 2016; Hedström et al., 2015). Accordingly, both pressures are examples of increasing needs of declaring users identity in a secure way in digital services (Corradini et al., 2006) for non-reputable service provision (Strauß, 2011). The pressures and barriers to negotiate in these cases are therefore some of the new challenges introduced when eIDs are getting increasingly important in organizations (e.g. Smith & McKeen, 2011). Due to the clear aim of eID conformity, from an ICT perspective, these efforts or pressures can also be seen as business and ICT alignment or IS strategic alignment (e.g. Preston & Karahanna, 2009) however focusing on this alignment of eID services from an inter-organizational perspective.

The pressure in the eGov case is motivated by a primary incentive of the eGov eID as an enabler of the needed increased development of public secure digital services towards citizens and businesses hence related to basic incentives of eGovernment efforts such as benefits, availability and participation (Axelsson et al., 2013; Grönlund, 2002). With this view, it can be seen as a front-office enabler of digital services as provided by authorities. However, in the eHealth case with the eID introduced for professional use to improve patient security in medical operations, the primary aim of the eID is related to basic civic rights such as privacy, integrity and the safeguarding of sensitive personal data. However, the eHealth eID also qualifies as being a back-office enabler with a focus on safeguarding of patient data in specific information systems contexts. In line with arguments put forth by Melin et al. (2016), and as shown in the both cases, I argue that
Concluding analysis and discussion

the eID in organizations today has reached a significant level of organizational integration, hence labelling it be related exclusively to a specific part (front- or back-office) of organizations can turn out to be problematic. Therefore, I argue that the institutional pressures of the eGov eID and eHealth eID are similar in the sense that the means of realizing these common infrastructures (Ke & Wei, 2004) of eID services by horizontal coordination of related services across the entire public sector covering front office services in the eGov case, as related to digital services for citizens, and back office services in the eHealth case, as related to internal information systems such as the EPR.

Thus, both introductions clearly relates to the move from former intra-organizational perspectives and focuses on efforts imposing inter-organizational coordination; a specific area in eGovernment described as one of the later stages of eGovernment (Layne & Lee, 2001) and in turn described as especially problematic (Kubicek & Hagen, 2000; Strejcek & Theil, 2002) since it in fact challenges historical paths as well as results in some radical changes for authorities (Hazlett & Hill, 2003). For example in the eGov case, authorities use of eID services in digital services will no longer be subject to independent decisions, but instead be regulated by a central eID program (c.f. Strejcek & Theil, 2002). Furthermore, I argue that it becomes important to acknowledge and understand how these institutional pressures arise since they are clearly bound to a historical context. Both introductions are clearly shaped by and are a result of former investigations, decisions and strategies in the public sector and health sector eID areas. I, therefore, argue that these introductions are clearly path dependent (David, 1985; Wilsford, 1994). The historical path can be seen as shaped in the form of an institution of more or less taken for granted norms and values (Zucker, 1977) that in turn influence and result in the proposed eID solutions introduced in the eGov and the eHealth cases.

Hence, this is also in line with prior research emphasizing the importance of acknowledging path dependency in relation to public sector eIDs (e.g. Kubicek & Noack, 2010a, 2010c; Melin et al., 2016). The proposed plan to realize the eGov eID is, in fact, the result of increasing returns and self-reinforcement (Page, 2006) being developed into an institution of a proposed path of a centrally coordinated eID regulation developing on institutional levels in government over a considerable time. Since this perspective is put forth in several following historical investigations of the public sector eID area, I argue that the described benefits and returns over time become assigned with increasing returns thus being reinforced as results (Page, 2006) of the institutionalized assumption of the benefits of regulation and coordination in a public eID context. The fact that this kind of efforts focusing on the coordination of technology and regulations of eIDs have not been introduced before in the public sector, in my opinion, strengthens this perspective. However, these are only the estimated benefits based on shared meanings and perceptions (Scott, 2014) of a suggested beneficial future path as formulated on the government level. Thus, I argue that prior to its introduction, it is clear that the eGov
Concluding analysis and discussion

eID ‘as an institution’ already exists on government levels as a result of repeated typifications and habitualizations (Berger & Luckmann, 1967) as reinforcing the benefits of this path. Further, the possibility of treating this artefact as an institution in itself is previously suggested (see Section 4.4.4) and also in line with the applied concept of generalized symmetry (Callon, 1986) of treating all actors participating in a network as equals. Thus, in a clear sociomaterial manner (Orlikowski, 2007; Orlikowski & Scott, 2008) this reduces any differences between the social and technical in the coming analysis. In addition, this institutionalized path of the eGov eID in fact clearly challenges the initial path of the eID to be used in the public sector as based on a market approach (Grönlund, 2010).

However, the development of the Market eID is, in fact, a direct result of officially assigned government mandates, investigations and guidelines from the beginning of the 2000s. Hence, this described weak eID governance (Söderström, 2012) with its lack of inter-governmental public and private sector coordination (Melin et al., 2013) is rather a result of deliberate decisions of the government from refraining from taking control of this area in the first place (see Chapter 5). Further, the historical path of the eHealth eID seems, from my point of view, less complex and more straightforward. Since the health care system is heavily regulated by several laws and regulations, the health care area has a long history of operating under extremely strict regulations. Thus, the eHealth eID is traced back to the Patient Data Act regarding aspects such as patient integrity, high quality and cost efficiency with respect to the patient’s integrity and restriction of unauthorized access to patient information.

There are also clear regulations regarding adherence to the law as well as what technical solution and infrastructure should be used (SITHS). Hence, this is a clear case of strong unproblematized coercive pressures (DiMaggio & Powell, 1983) put on organizations in the health care sector. It is also important to acknowledge that while the governing law is in place, the introduction of the eHealth eID in the covered case starts some four years later which indicates that any sanctions for not complying with this law are rather weak. In the eHealth case it is also clear that with regulations and technical infrastructure in place at an early stage several years prior to its application in the eHealth eID solution, this also shows a historical path that can be considered as technological lock-in (Arthur, 1989). There is also a clear dependency between paths of initial technical implementation of the framework and the introduction of the eHealth eID. Hence this suggests path interdependency since the organization then just awaits the introduction of systems, such as the EPR, that will make use of the eHealth eID (see Chapter 6). Further, if the previously concept of societal steering media (Myers & Young, 1997) is applied in these cases, I argue that there are several interesting differences emerging. Thus, the societal steering media in the eGov case resembles the described eGov eID as institution developing over time at the government level. The only steering mechanism (Myers & Young, 1997) applied prior to the Board becoming operative is the shared knowledge among
affected actors that the current procurement model will eventually expire and not be renewed. Hence, it is only during the introduction itself that the Board begins to formulate a range of steering mechanisms such as regulations and guidelines to try to affect or colonize the lifeworlds (Broadbent et al., 1991) of the affected societal systems, i.e. authorities as service providers, with the notion of the benefits and righteousness of the eGov eID. Thus, as previously indicated, the potential conformance to the eGov eID is depending on a positive institutionalization and transfer of clearly defined patterns of conduct (Berger & Luckmann, 1967) regarding how eID services is used in public digital services across an extremely broad and heterogeneous group of current and potential service providers as societal systems.

In the eHealth case, the societal steering media is much more distinct and regulative and steering mechanisms, for example in the form of the technical infrastructure to be used for the eHealth eID, is in place several years before the actual introduction of the eHealth eID begins. Hence, in this case, I argue that there is a far better chance of these mechanisms becoming part of the internal of the lifeworld (Myers & Young, 1997) since these are already in place in the organization albeit not in operational use. As suggested at an early stage in this dissertation, public sector eID introductions seem to apply a too narrow focus on technical and regulatory aspects. Hence, I argue that this proposition is well confirmed in the eGov as well as the eHealth case, from the main actors’ perspective as well as based on affected actors’ translations of the introductions. Hence, I argue this, in turn, are examples of an existing overconfidence in technology (Shalev et al., 2014) in the public sector regarding eIDs. These central pressures forcing acceptance and use of eIDs are in clear contrast to well-known research focusing on the role of ICT in an organizational context.

For example, the importance of fit between structure and context in an organizational setting is put forth in contingency theory (Drazin & Van de Ven, 1985) with structure here referring to the eID solution and the context of the organizational setting. Further, in ISR the importance of ICT and organizational convergence is put forth (Leifer, 1988) and organizational validity of ICT (Markus & Robey, 1983) puts the emphasis on the positive match between technology and organization. Hence, these aspects seem not to be accounted for especially in the eGov case since the prerequisites as well as the introduction bears clear signs of not being sufficiently grounded in eID practice among affected actors. Hence, this narrow perspective on the eID seems to show a significant neglect of the fact that technology and ICT are becoming increasingly integrated into modern organizations (Iivari, 1992). Thus, only focusing on regulatory and technical aspects can, in fact, result in more or less severe challenges as also shown in these cases. A general characterization, with central characteristics of these pressures is presented in Table 22.
Table 22. General characterization of pressures

<table>
<thead>
<tr>
<th></th>
<th>eGov</th>
<th>eHealth</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Type(s)</strong></td>
<td>Normative</td>
<td>Coercive/regulative</td>
</tr>
<tr>
<td><strong>Incentives</strong></td>
<td>Inter-organizational</td>
<td>Inter-organizational</td>
</tr>
<tr>
<td><strong>Ontology</strong></td>
<td>Substantialism</td>
<td>Substantialism</td>
</tr>
<tr>
<td><strong>Context</strong></td>
<td>Front-office</td>
<td>Back-office</td>
</tr>
<tr>
<td><strong>Path</strong></td>
<td>Institutional dependency</td>
<td>Operational dependency</td>
</tr>
</tbody>
</table>

Accordingly, by applying the different types of isomorphic pressures by DiMaggio and Powell (1983) and the three institutional pillars by (Scott, 2014), the institutional pressure in the eGov case is characterized as being of a normative type since there are no legal or regulative aspects associated. Hence, the Board anticipates institutionalization of norms values of values as assigned to the eGov eID, in turn clearly related to coordination and control for the greater good of the public sector. Further, these types of pressures are also related to the legitimacy gained by conformance thus the potential legitimacy later gained by the eGov eID becomes crucial. This type of pressure is also related to professionalism in a specific area, such as prescribed code of conduct or preferred practices. Hence this suggests a needed convergence between the incentives of the eGov eID and the translated incentives of eIDs in the public sector in among authorities as service providers.

This is contrasted by the eHealth eID that can be categorized as being a pressure of coercive/regulative type as exerted by government bodies these organizations are clearly dependent on, i.e. responsible ministry and authorities. Hence, the county council, in this case, must comply with current law and regulations in order to provide health care in the public sector. Thus, this pressure can also be described as regulative since there are legal sanctions and clear rules involved. Thus, both pressures are seen as clearly inter-organizational since they aim at introducing an increased conformity of eID services in the public sector. Also relevant is the ontology of the pressure as referring to how this institutional pressure itself perceives the area to be conformed. Thus, I describe both pressures as clearly substantialist (Cecez-Kecmanovic et al., 2014) since they perceive the eID being introduced as clearly separate from any social or organizational implications. Hence, the focus here is solely on providing the prerequisites in the form of technical infrastructures and regulations. As previously described, the officially stated central incentives of the eGov eID are clearly related to the eID in front-office use while
I interpret the eHealth eID as primarily facilitating the needed security levels in back-office information systems. Finally, the described path dependencies of these pressures are clearly different since the eGov eID follows a path of being conceived on an institutional level in government while the eHealth eID has clear operational characteristics due to early implementations of the needed infrastructure well before the actual eID introduction.

9.2.2 Institutional factors and predictive dimensions of pressures

In this section, the pressures are deconstructed into their inherent institutional factors with each factor linked to two dimensions each assessed with a predicted level of success. Hence, this is the suggested approach for predicting the outcome of pressures as related to their anticipated levels of resistance (Oliver, 1991). These factors and dimensions put the focus on the different inherent parts of pressures in order to develop a better understanding of these pressures as a whole and later to be compared to barriers in Stage 3.

eGov case

In relation to its cause, the eGov eID aims at increasing coordination, standardization and sustainability, as well as providing simplified access to eID services in order to increase development of public digital services. Hence, the aim is on the intra-organizational level of the public sector as a whole. However, the Board is well aware of the criticisms and questions raised right from the start hence the predicted legitimacy is considered to be on a moderate level. The gained efficiency of the solution is predicted as high since the governing report clearly states that the eGov eID by no means should negatively affect current eID solutions and transfer to the new solution will be facilitated. The constituents regarding multiplicity are regarded as low since this is a unitary eID solution as coordinated by a solely responsible authority thus in turn the dependence becomes high.

Consistency with regards to alignment with individual, organizational perspectives is seen as high since the eGov eID, in fact, will solve all the identified problems and shortcomings of the Market eID. Further, constraints are set at a moderate level since there are clear regulations and frameworks that must be adhered to. Regarding the factor of control, compliance is clearly at a low level of compliance with the eGov eID will not be enforced by any legislation. However, since the current procurement model will not be replaced I argue that this becomes a clear force for compliance. Hence enforcement is set at a moderate level. During the first years, the Board officially states that there will be no other option to gain access to eID services as a service provider in the public sector hence voluntariness becomes low. However, this is later changed by the Board into to an explicit volunteerism. In relation to the environmental context of the eGov eID, uncertainty is set to high since the existing procurement model is soon to be expired hence the need for a new procurement setup is urgent and as long as this is not solved the entire solution hangs in the balance. Further, interconnectedness of the context is assessed as
being high level since the Board is fully aware of existing relationships between SPs and IdPs (Table 23).

**Table 23. eGov case - factors, dimensions and predicted levels of pressures**

<table>
<thead>
<tr>
<th>Factor</th>
<th>Dimension</th>
<th>Level</th>
<th>Motivation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cause</td>
<td>Legitimacy</td>
<td>Moderate</td>
<td>Positive incentives for public sector as a whole</td>
</tr>
<tr>
<td>Efficiency</td>
<td>High</td>
<td></td>
<td>Market eID solutions not negatively affected</td>
</tr>
<tr>
<td>Constituents</td>
<td>Multiplicity</td>
<td>Low</td>
<td>A unitary eID solution</td>
</tr>
<tr>
<td></td>
<td>Dependence</td>
<td>High</td>
<td>The Board as the solely responsible authority</td>
</tr>
<tr>
<td>Content</td>
<td>Consistency</td>
<td>High</td>
<td>Solving problems in the eID area</td>
</tr>
<tr>
<td></td>
<td>Constraints</td>
<td>Moderate</td>
<td>Regulations and frameworks for quality of services</td>
</tr>
<tr>
<td>Control</td>
<td>Enforcement</td>
<td>Moderate</td>
<td>Compliance not enforced by law but forces used</td>
</tr>
<tr>
<td></td>
<td>Voluntariness</td>
<td>Low (High)</td>
<td>Initially mandatory to comply (later voluntary)</td>
</tr>
<tr>
<td>Context</td>
<td>Uncertainty</td>
<td>High</td>
<td>Expiring procurement model</td>
</tr>
<tr>
<td></td>
<td>Interconnectedness</td>
<td>High</td>
<td>Support by a major SPs and IdPs</td>
</tr>
</tbody>
</table>

**eHealth case**

The eHealth eID has a **legitimacy** set at a high level since the cause of this pressures seems very legitimate in ensuring patient security and integrity. The **efficiency** of this solution is also anticipated to be high with no significant negative effects on operations. The **multiplicity** of constituent demands is low since there is a sole focus on authentication and the **dependence** on institutional constituents is deemed to be high since this pressure is enforced by law and regulations as well as a prescribed technical infrastructure. The **consistency** of the content is high since in line with law and regulations, and **constraints** are set to a moderate level since there is a clearly prescribed use of the eHealth eID that users must adhere to. Control in the form of **enforcement** is rather high due to legislative origins which also results in low levels of **voluntariness**. The **uncertainty** of the external context is perceived as low since this organization must adhere to
the law and there is no another solution to be considered. Finally, the interconnectedness is assessed as being of a moderate level since there are clearly defined inter-organizational user groups such as the eHealth eID Management team (Table 24).

Table 24. eHealth case - factors, dimensions and predicted levels of pressures

<table>
<thead>
<tr>
<th>Factor</th>
<th>Dimension</th>
<th>Level</th>
<th>Motivation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cause</td>
<td>Legitimacy</td>
<td>High</td>
<td>Patient security and integrity</td>
</tr>
<tr>
<td></td>
<td>Efficiency</td>
<td>High</td>
<td>Should not affect efficiency</td>
</tr>
<tr>
<td>Constituents</td>
<td>Multiplicity</td>
<td>Low</td>
<td>Focused on authentication only</td>
</tr>
<tr>
<td></td>
<td>Dependence</td>
<td>High</td>
<td>Enforced by law, regulations and infras-</td>
</tr>
<tr>
<td></td>
<td>Consistency</td>
<td>High</td>
<td>In line with current law and regulations</td>
</tr>
<tr>
<td></td>
<td>Constraints</td>
<td>Moderate</td>
<td>Prescribed use of the eID</td>
</tr>
<tr>
<td>Control</td>
<td>Enforcement</td>
<td>High</td>
<td>Enforced by law and regulations</td>
</tr>
<tr>
<td></td>
<td>Voluntariness</td>
<td>Low</td>
<td>Mandatory to comply</td>
</tr>
<tr>
<td>Context</td>
<td>Uncertainty</td>
<td>Low</td>
<td>Organization must adhere to law</td>
</tr>
<tr>
<td></td>
<td>Interconnectedness</td>
<td>Moderate</td>
<td>Inter-organizational user groups</td>
</tr>
</tbody>
</table>

9.3 Stage 2: Barrier

9.3.1 Characterization of barriers

The stage of problematization (Callon, 1986) during translation analysis (see Chapter 7 and 8) provides a set of translated and validated problem areas relevant to the defined network as a whole as well as the individual problem areas of participating actors. The following characterization of barriers will be based on these problem areas to be able to further analyse and discuss them in the light of relevant theory. Thus, the aim is also to further develop these problem areas into the abstractions of institutional barriers later to be deconstructed into two factors and dimensions in the next step as well as compared
Concluding analysis and discussion

to pressures in Stage 3. For the first step in this characterization, I argue that these identified and validated problem areas can be seen as external influences that potentially facilitate the development of barriers. This is also in line with the stage of interessement (Callon, 1986) in translation analysis when these problem areas are regarded as external influences potentially affecting these actors’ participation in the network in a negative way (see Section 4.3.4).

Further, I argue that it is also possible to apply the typologies of institutional pillars (Scott, 2014) and isomorphic processes (DiMaggio & Powell, 1983) on these influences to provide a similar analysis as pressures facilitating a later comparison. Based on the performed problematizations (see Section 7.1 and 8.1), the eID introductions in both cases are facing some significant challenges. The eGov eID as an actor must deliver on security and trust hence meet existing normative systems (Scott, 2014) in specific fields of a professional code of conduct (DiMaggio & Powell, 1983) such as information security and trust frameworks. The main challenges of the eHealth eID as an actor are described as related to organizational, managerial and technological issues hence these are all examples of coping with challenges in a professional or normative sense.

The challenges of developing and presenting the new public procurement model and external directives (eIDAS) are potential regulative external influences on the eGov eID during its introduction. Turning to the service providers (SPs) and identity providers (IdPs) in the eGov case, these two actors share the same set of problem areas as related to their current eID practice, the eGov eID itself as well as cooperation and dialogue hence, these influences can be seen as normative as well as cultural-cognitive (Scott, 2014). Thus, the use of the Market eID in public sector digital services can be described as being a result of a strong path dependency (e.g. Wilsford, 1994; Zhu et al., 2006) showing several causes as prescribed by research such as increasing returns (increasing transaction volumes and decreasing costs), self-reinforcement (renewed procurement processes) and positive feedbacks (positive relations between SPs and IdPs) (Page, 2006).

Cooperation and dialogue in the eGov case are seen as a central means for affected actors to ensure the Board takes affected actors perspective into consideration during the introduction thus potentially facilitating a better organizational validity (Markus & Robey, 1983) or organizational fit (Leifer, 1988) of the eGov eID in affected organizations. Moreover, I argue that one of the reasons why different organizations have very strong arguments and comments on the eGov eID is a result of this artefact becoming increasingly important as well as increasingly integrated into modern organizations (c.f. Iivari, 1992). In the eHealth case, the users are assigned to the problem areas of current practice, knowledge and communication and the eHealth eID. Hence, their daily medical or administrative practice, as well as perceptions of how the eHealth eID should be integrated into their daily routines acts as a normative influence hence this is also an
example of an influence prescribing that the eID introduced, should positively converge with operations hence resulting in a positive fit (Robey, 1981). In addition, knowledge and communication as a cultural-cognitive influence also affect the users’ potential conformance to the introduction as shown in this case since I argue that these are key aspects for understanding the purpose of the eHealth eID as related to patient confidentiality.

This case indicates, there is a clear tendency of users acknowledging the purpose of the eHealth eID conforming to its prescribed use. Therefore, a lack of understanding and knowledge of the eID introduces a clear risk of users selecting non-use in this mandatory context of use (Marakas & Hornik, 1996) and I argue that this becomes particularly important in this case since findings show a clear path dependency (Page, 2006) of not considering patient security in the past. Hence, in the eHealth case, it is not only the eID being introduced but also the new concept of information security that needs to be institutionalized in actions and behaviours (Zucker, 1977). Hence this, in fact, becomes a significant challenge. Finally, the ITRs in the eHealth case depend on management to support the introduction as well as the eHealth eID to function properly. Hence these are to be considered as normative influences along with the current practice of these actors also affecting the conformance.

With these problem areas as potentially influencing these eID introductions, it is safe to say that the eGov, as well as the eHealth eID, will inevitably influence (Mason & Mitroff, 1973) the organizations introducing and conforming to these isomorphic pressures (DiMaggio & Powell, 1983). However, fully in line with research emphasizing the importance of considering the organizational perspective or context in relation to ICT (e.g. Ein-Dor & Segev, 1978; Leifer, 1988), this approach perceives the barrier as an equivalent to pressures hence I argue that organizational validity (Markus & Robey, 1983) of the eID becomes a key. Thus, I suggest that regarding eID introductions in the public sector, it may not be appropriate to perceive these as pressures of ‘organizational conformance’ (Scott, 2014) but rather ‘organizational equivalence’ between pressures and barriers as perceived from an internal view of affected organizations (e.g. Combs et al., 2009; Zucker, 1987). This is motivated by the fact that the eIDs being introduced in these cases are standardized solutions (Hong & Kim, 2002) for digital authentication. Hence, although these eIDs can be put in the hands of organizations and users rather quickly (Gremillion & Pyburn, 1983), empirical findings clearly point towards the eID as very dependent on actors’ translations of its validity and appropriateness (c.f. Markus & Robey, 1983) in its organizational and operational settings.

Therefore, I argue that this indicates that these barriers develop when there is a clear divergence between government assumptions and taken for granted aspects (Myers & Young, 1997) regarding these eID introductions such as the anticipated mimetic conformance (DiMaggio & Powell, 1983), to the eGov eID across authorities as service providers in the public sector and the users across the health care organization. Thus, it
Concluding analysis and discussion

should come as no surprise when for example the eHealth eID, as an example of societal steering media (Broadbent et al., 1991) with a clear lack of organizational validity, meets the societal systems (Myers & Young, 1997) of current practice in the health care organization (county council). Relating to the recurring problem area of current practice, with the eID in both cases as assigned with estimated benefits, this results in an ensemble view (Orlikowski & Iacono, 2001) of the eID that in essence is artificially constructed by the main actors.

Since benefits are estimated rather than established in practice, in my opinion, this results in a rather high risk of actors, as weighing costs against benefits (Keen, 1981; Markus, 1983), failing to acknowledge these benefits due to their lack of grounding in practice. In addition, these strategies of estimating benefits are clearly diverging from related research instead suggesting benefits should be perceived as positive by affected actors in order to facilitate conformance to use (Aubert & Hamel, 2001). Another emerging concept is that the eID in both cases becomes an institutional carrier (Jepperson, 1991; Scott, 2014), described as a carrier of institutionalized systems, activities and artefacts (Scott, 2014). Thus, the eID is assigned with specific meanings, norms and values and is used as a carrier for the transfer of the institution across an organizational context. However, when the introductions in the cases run into problems, I argue that it is a clear change in how these norms and values as assigned to the eID get translated by affected actors. For example, when the SP and IdP in the eGov network identify the security risks, this marks a significant change in translations and attitudes among these actors instead turn against the eGov eID as well as the introduction as a whole.

In the eHealth case, users that perceive the eHealth eID as negatively affecting their working situation similarly shifts to showing clear signs of negativity against it. These indications are also in agreement with Czarniawska and Joerges (1996) suggesting that such an institutional carrier can at any given time be assigned with a different translation or meaning. Thus, I argue that this interesting view of the eID are confirmed on several occasions in the cases with several described examples of the eGov eID and eHealth eID as ‘turning against themselves’ in times of challenges and difficulties during the introductions. Hence, this also confirms existing research suggesting resistance to ICT in general, the barrier in these cases, as often occurring in complex states (Hirschheim & Newman, 1988); a topic that will be further elaborated in the next stage of negotiation. Similar to pressures, this characterization is ended by a summary of barriers’ characteristics presented in Table 25.
Table 25. General characterization of barriers

<table>
<thead>
<tr>
<th>Type(s)</th>
<th>eGov</th>
<th>eHealth</th>
</tr>
</thead>
<tbody>
<tr>
<td>Incentives</td>
<td>Intra-organizational</td>
<td>Intra-organisational</td>
</tr>
<tr>
<td>Ontology</td>
<td>Relationism</td>
<td>Relationism</td>
</tr>
<tr>
<td>Context</td>
<td>All-office</td>
<td>Back-office</td>
</tr>
<tr>
<td>Path</td>
<td>eID practice (Market eID)</td>
<td>Non-eID use</td>
</tr>
</tbody>
</table>

The influence caused by barriers in the eGov case is seen as normative (professionalism regarding security and trust and of current practice), regulative (procurement and external directives) as well as cultural-cognitive (cooperation and dialogue). In the eHealth case, the regulatory aspects of the eHealth eID are left unproblematised hence barriers are seen as related to normative (organization, technology, management, current practice) and cultural-cognitive (knowledge and communication) challenges. The incentives or meaning of barriers is in the eGov case clearly related to intra-organizational perspectives of the current use of eID services in external digital services and in the eHealth case, barriers are based on a similar intra-organizational perspective but instead related to a previous non-use of the eID (lack of strong authentication) prior to its introduction.

Hence, barriers in both cases are clearly related to an ontology of relationism (Cecez-Kecmanovic et al., 2014) with the eID as taking part in a complex organizational and operational relationship. The context influenced by the barrier in the eGov case is exemplified by authorities describing it as an extremely important and integrated part of current business hence I choose to describe this as related to an all-office context to emphasise this strong need of eID services. However, in the eHealth case, the eHealth eID is still rather strictly related to back-office operations with the aim of providing health care to citizens. As described, the path leading up to the barrier in the eGov case is grounded in existing eID practice with the Market eID as currently integrated into digital services. This is contrasted by the eHealth case with a previous history of not using any eIDs for digital authentication.
9.3.2 Institutional factors and predictive dimensions of outcome

Similar to the previous analysis of pressures, this section assesses the institutional factors and predictive dimensions based on the actual outcome of pressures. Hence, the assigned levels are motivated by empirical findings in Chapter 5 and 6 as well as results from the translation analysis in Chapter 7 and 8. This structure will also facilitate a later comparison of pressures and barriers regarding these factors and dimensions.

eGov case

Based on the outcome of the pressure to conform to the introduction of the eGov eID, the legitimacy turns out to be very low as a result of several causes. Since there are strong criticisms to the eGov eID from the start, challenges of keeping an open dialogue and cooperation with affected actors do not have a significant effect on legitimacy in terms of conforming to the pressure. Later, the identification and acknowledgement of security risks result in a final drop in legitimacy. However, I argue that the single most important factor here is the Board as seeking legitimacy for a solution covering the public sector as a whole, while independent authorities are focused on providing the best possible service from their own perspectives. The efficiency as a result of accepting and joining the eGov eID is also seen as low since this will, in fact, result in a complex and resource intensive transition of services.

The multiplicity is also perceived as high since the eGov eID for several authorities as service providers proves to be incomparable with current efficient and cost effective eID practice such as higher costs and procurement constraints. Thus, I argue that this is clearly a contradictory demand to their government assignment of conducting their business in an effective manner. The history of highly independent authorities in Sweden also adds to this aspect since one of the main incentives of the eGov eID is conforming to a solution for the greater good of the entire public sector. With the Market eID fully functional and currently filling the needs of public sector SPs, the dependency of the institutional constituents of the pressure is described as very low. The threat of not being able to procure eID services outside of the eGov eID is also confirmed as untrue, hence bilateral agreements still being possible.

With the multiplicity of constituent demands also comes a low consistency with organizational demands of affected organizations, many of them just wanting to maintain their digital service businesses as usual. This level also being a result of the anticipated higher costs for SPs and lower levels of compensation for IdPs. The constraints are assessed of being at a high level since the eGov eID will require adherence to regulations as well as procurement procedure. The factor of control and enforcement is perceived as rather low since compliance and conformance with this pressure can not be forced. However, some authorities receive specific instructions from the government to investigate and prepare for conformance to the pressure which in turn indicates a significantly higher level of enforcement put on these actors. Accordingly, this also results in a high level of
Concluding analysis and discussion

**voluntariness.** Since the current procurement model soon expires, the continued procurement of eID services is one of the biggest concerns of SPs across the public sector. However, with identified possibilities of procurement workarounds, this **uncertainty** of the environmental context of the eGov eID becomes low. Finally, the **interconnectedness** in the surrounding context is set to high since there are several constellations or networks of actors in the eID area as a result of relations formed over time. The summary of the outcome of pressures in terms of dimensions and levels as influenced by developing barriers is presented in Table 26.

**Table 26. eGov case - factors, dimensions and outcome of pressures**

<table>
<thead>
<tr>
<th>Factor</th>
<th>Dimension</th>
<th>Level</th>
<th>Motivation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cause</td>
<td>Legitimacy</td>
<td>Low</td>
<td>Independent authorities, strong critique, acknowledged security risks</td>
</tr>
<tr>
<td></td>
<td>Efficiency</td>
<td>Low</td>
<td>Resource intensive transition, higher costs</td>
</tr>
<tr>
<td>Constituents</td>
<td>Multiplicity</td>
<td>High</td>
<td>Diverging from efficient and secure eID practice</td>
</tr>
<tr>
<td></td>
<td>Dependence</td>
<td>Low</td>
<td>Market eID as fully functional, procurement workarounds</td>
</tr>
<tr>
<td>Content</td>
<td>Consistency</td>
<td>Low</td>
<td>Inconsistency with organizational goals, higher costs, lower compensation</td>
</tr>
<tr>
<td></td>
<td>Constraints</td>
<td>High</td>
<td>Adherence to regulations and procurement procedures causing workarounds</td>
</tr>
<tr>
<td>Control</td>
<td>Enforcement</td>
<td>Low</td>
<td>Compliance can not be forced</td>
</tr>
<tr>
<td></td>
<td>Voluntariness</td>
<td>High</td>
<td>Voluntary to join</td>
</tr>
<tr>
<td>Context</td>
<td>Uncertainty</td>
<td>Low</td>
<td>Procurement workarounds</td>
</tr>
<tr>
<td></td>
<td>Interconnectedness</td>
<td>High</td>
<td>Connected SPs and IdPs</td>
</tr>
</tbody>
</table>

**eHealth case**

In the eHealth case, findings and analysis point towards the **legitimacy** of the cause of this pressure only perceived as moderate. Although conformity is clearly enforced by law and regulations, on the operative level there are several indications that the provision of health care is prioritized over conforming to the prescribed use of the eHealth eID. Further, **efficiency** is assessed as being of an equal moderate level since there are several
reports of the eID having a negative effect on working routines for example as a result of technical problems during the introduction such as significant reconnection times. Accordingly, due to the reported negative effects of the eHealth eID, the constituent of multiplicity is perceived as high since there is a clear divergence between the divergent demands of providing high quality medical care while conforming to the correct use of the eID.

Thus, the dependence of the eID introduced as a result of the pressure is seen as moderate since it marks a change from not being explicitly aware of security related issues in health care. Hence, institutionalized norms and behaviours are challenged, and in some cases, there is even a reported inconsistency of operational goals regarding healthcare, in turn, resulting in the consistency being perceived as rather low. Further, constraints are set to a high level since a majority of respondents report the process of adapting to the eHealth eID as cumbersome even the ones with good knowledge of its purpose as a security enhancing artefact. These constraints are clearly related to the prescribed use of the eID and recurring technical problems during the introduction. In terms of control, enforcement is interestingly enough low despite being a solution sanctioned by law. Hence neglecting to adhere to the correct use of the eHealth eID can be seen as a direct violation of the underlying regulations.

Although efforts to inform users across the organization, there is a reported lack of clear deterrents thus misuse of the eID leads to no significant sanctions. Although the voluntariness of this solution should be set at a minimum, I argue that the clear lack of control and enforcement nevertheless results in a moderate level of voluntary use. Findings also clearly indicate that adherence to the eHealth eID is clearly related to the level of knowledge of the aim and purpose of this solution. The uncertainty of the context is seen as being on a moderate level, since recurring technical problems during the introductions result in users being quite unsure how well the eID will work in the future. Finally, the interconnectedness in the context is seen as low since despite previous participation in user groups related to the eID, the organization still reports that being early adopters of the eHealth eID, inter-organizational communication and knowledge sharing regarding the eID are very limited (Table 27).

Table 27. eHealth case - factors, dimensions and outcome of pressures

<table>
<thead>
<tr>
<th>Factor</th>
<th>Dimension</th>
<th>Level</th>
<th>Motivation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cause</td>
<td>Legitimacy</td>
<td>Moderate</td>
<td>Priority put on providing health care</td>
</tr>
<tr>
<td></td>
<td>Efficiency</td>
<td>Moderate</td>
<td>Negative effects on working routines</td>
</tr>
</tbody>
</table>
Concluding analysis and discussion

<table>
<thead>
<tr>
<th>Factor</th>
<th>Dimension</th>
<th>Level</th>
<th>Motivation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Constituents</td>
<td>Multiplicity</td>
<td>High</td>
<td>Divergence between security and medical care</td>
</tr>
<tr>
<td></td>
<td>Dependence</td>
<td>Moderate</td>
<td>Security workarounds, patient security, has not been a priority in the past</td>
</tr>
<tr>
<td>Content</td>
<td>Consistency</td>
<td>Low</td>
<td>Conflicts between security and medical care</td>
</tr>
<tr>
<td></td>
<td>Constraints</td>
<td>High</td>
<td>Prescribed use of the eID and technical problems causing workarounds</td>
</tr>
<tr>
<td>Control</td>
<td>Enforcement</td>
<td>Low</td>
<td>No significant sanctions</td>
</tr>
<tr>
<td></td>
<td>Voluntariness</td>
<td>Moderate</td>
<td>Adherence as related to knowledge</td>
</tr>
<tr>
<td>Context</td>
<td>Uncertainty</td>
<td>Moderate</td>
<td>Technical problems during introduction</td>
</tr>
<tr>
<td></td>
<td>Interconnectedness</td>
<td>Low</td>
<td>Early adopters, very limited inter-organizational communication</td>
</tr>
</tbody>
</table>

9.4 Stage 3: Negotiation

9.4.1 Pressures vs barriers

To provide a better understanding on what grounds these barriers against the pressures to introduce the eIDs rest, the following section will cover all previously assessed factors, dimensions and levels of pressures and barriers. This will be done in the form of a comparison between the cases covering the dimensions of each institutional factor in order. This approach is chosen to be able to maintain transparency and clarity during this part of the analysis. Accordingly, by assessing each dimension for potential controversies provides an opportunity to develop a far better understanding of these barriers or resistance. Further, this is also in clear contrast to existing research on challenges related to ICT where resistance is often approached by instead focusing on how to potentially maximize user acceptance (Klaus & Blanton, 2010). However, in my opinion, instead of putting acceptance in the foreground poses a significant risk of avoiding to deal with resistance in a reflective manner hence, in turn, risking this resistance developing into powerful barriers over time, hence related to the concept of institutionalization of barriers described in Stage 4. In line with (Hirschheim & Newman, 1988) I argue that much can be learned from a more elaborate analysis of resistance to public sector eIDs. In addition, I argue that these two cases are examples of this predominant focus on acceptance while avoiding to further investigate resistance.
Legitimacy and efficiency

Legitimacy in the sense of desirable and appropriate actions according to a social system of norms and values (Suchman, 1995) is described as one of the central guiding incentives of organizations and therefore becomes essential for organizational survival (Dowling & Pfeffer, 1975). The perceived legitimacy of the eGov and eHealth eID becomes an important factor to facilitate conformity. However, the perceived legitimacy of affected actors in both cases turn out to be significantly lower than anticipated by main actors since there are clear divergences between the social system prescribing the legitimacy and the systems appraising it. Since the eGov eID, as well as the eHealth eID, are in need of active support, the authorities must actively join the eGov eID, and users must conform to be prescribed the use of the eHealth eID, hence in this context legitimacy is described as a means of gaining such support (Suchman, 1995). However, these aspects are not acknowledged in these cases since legitimacy turns out to be lower than expected hence a significant part of the independent authorities put the focus on their own business and legitimacy and healthcare staff prioritize the provision of health care. At the outset, none of the eID solutions is launched with incentives of reduced efficiency; hence current levels should be maintained as a minimum. However, the eGov eID, as well as the eHealth eID, fails to deliver regarding this aspect with examples such as the eGov eID resulting in significantly higher eID costs than the Market eID for authorities and technical problems of eHealth eID as having a negative impact working routines. Thus the view of these low levels of legitimacy and efficiency as facilitating barriers are also in line with research describing these as indicators of a potential resistance (Markus, 1983; Oliver, 1991). Research also describes that in some cases organizations can even conform to pressures gaining legitimacy at the cost of efficiency (Meyer & Rowan, 1977) however this does not apply in the eGov case where there seems to be no significant legitimacy to gain (Table 28).

Table 28. Legitimacy and efficiency

<table>
<thead>
<tr>
<th>Dimension (case)</th>
<th>Pressure (level)</th>
<th>Barrier (level)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Legitimacy (eGov)</td>
<td>Positive incentives for public sector as a whole</td>
<td>Independent authorities, strong critique, acknowledged security risks (low)</td>
</tr>
<tr>
<td></td>
<td>(moderate)</td>
<td></td>
</tr>
<tr>
<td>Legitimacy (eHealth)</td>
<td>Patient security and integrity (high)</td>
<td>Priority put on providing health care (moderate)</td>
</tr>
<tr>
<td>Efficiency (eGov)</td>
<td>Market eID solutions are not negatively affected (high)</td>
<td>Resource intensive transition, higher costs (low)</td>
</tr>
</tbody>
</table>


Concluding analysis and discussion

<table>
<thead>
<tr>
<th>Dimension (case)</th>
<th>Pressure (level)</th>
<th>Barrier (level)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Efficiency (eHealth)</td>
<td>Should not affect efficiency (high)</td>
<td>Negative effects on working routines (moderate)</td>
</tr>
</tbody>
</table>

**Multiplicity and dependency**

Since the coherence of pressures has a clear impact on potential conformance (Oliver, 1991) as described, the multiplicity of pressures become important. The eGov eID is presented with a rather low multiplicity as a unitary eID solution to cover the entire public sector. However, as it turns out, several authorities perceive this solution as creating a contradictory demand (Scott, 1987) since several consequences of the eGov eID clearly diverge from authorities’ missions including an efficient eID practice such as higher costs and the introduction of new security risks. Similarly, in the eHealth case, the pressure with the sole focus on security and digital authentication clearly fails to acknowledge the fact that the provision of medical care is the highest priority in this organization, hence this also creates a contradictory demand of different potentially conflicting expectations (Whetten, 1978) on users especially ones with a lack of knowledge about the purpose of the eHealth eID.

These perceived higher levels of multiplicity are clearly related to the divergence between the pressure and organizational perspectives in both cases poses significant risks of creating resistance as caused by the perceived organizational invalidity of pressures (Hirschheim & Newman, 1988). It is described that a high level of dependence on the actor exerting the pressure will facilitate conformance (DiMaggio & Powell, 1983) hence the Board as the only responsible authority for the eGov eID and eID services in the public sector and the eHealth eID as enforced by law and regulations should result in high levels of dependence as well as conformance. However, as it turns out, the dependence on the eGov eID and the Board is at a very low level since the Market eID solution is fully functional and procurement workarounds are identified. Further, in the eHealth case, there are reports of patient security not being a priority in the past which in turn might explain security workarounds such as leaving the eID in the card reader being a common behaviour. Thereby, none of these cases shows a dependency of resources (Pfeffer & Salancik, 2003) which in turn results in the dependency turning out lower than anticipated by pressures. Thus, higher levels of multiplicity and lower levels of dependency will work in favour of an increasing resistance (Oliver, 1991) (Table 29).
Table 29. Multiplicity and dependency

<table>
<thead>
<tr>
<th>Dimension (case)</th>
<th>Pressure (level)</th>
<th>Barrier (level)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Multiplicity (eGov)</td>
<td>An unitary eID solution (low)</td>
<td>Diverging from efficient and secure eID practice (high)</td>
</tr>
<tr>
<td>Multiplicity (eHealth)</td>
<td>Focused on authentication only (low)</td>
<td>Divergence between security and medical care (high)</td>
</tr>
<tr>
<td>Dependency (eGov)</td>
<td>The Board as the solely responsible authority (high)</td>
<td>Market eID as fully functional, procurement workarounds (low)</td>
</tr>
<tr>
<td>Dependency (eHealth)</td>
<td>Enforced by law, regulations and infrastructure (high)</td>
<td>Security workarounds, patient security, has not been a priority in the past (moderate)</td>
</tr>
</tbody>
</table>

**Consistency and constraints**

Theory prescribes a higher potential conformance with pressures that converge or are compatible with internal goals of organizations (Oliver, 1991). Thus, organizations are much more likely to reject inconsistent pressures (e.g. Covaleski & Dirsmith, 1988) in turn in line with organizational invalidity as a common cause of resistance (Hirschheim & Newman, 1988). The pressures in the eGov, as well as the eHealth case, are assessed as high since the eGov eID will, in fact, solve several outstanding issues and problems in the public sector eID area, and the eHealth eID is fully in line with current law and regulations. However, the outcome indicates significant lower levels as related to the eGov eID’s inconsistency or invalidity with organizational goals and the conflicts between security and medical care affecting the conformity to the eHealth eID. Further, pressures potentially constraining autonomy poses a higher risk of meeting resistance (Oliver, 1991; Pfeffer & Salancik, 2003). Although the levels of constraints introduced in both cases are assessed as being at a moderate level, the resistance and barriers show high levels resulting in active workarounds in both cases. This, in turn, indicates that costs for these regulated areas outweigh benefits (Hirschheim & Newman, 1988) but are at the same time also closely interrelated to other dimensions such as consistency, legitimacy and efficiency (Table 30).
Concluding analysis and discussion

Table 30. Consistency and constraints

<table>
<thead>
<tr>
<th>Dimension (case)</th>
<th>Pressure (level)</th>
<th>Barrier (level)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Consistency (eGov)</td>
<td>Solving problems in the eID area (high)</td>
<td>Inconsistency with org. goals, higher costs &amp; lower compensation (low)</td>
</tr>
<tr>
<td>Consistency (eHealth)</td>
<td>In line with current law and regulations (high)</td>
<td>Conflicts between security and medical care (low)</td>
</tr>
<tr>
<td>Constraints (eGov)</td>
<td>Regulations and frameworks for quality of services (moderate)</td>
<td>Adherence to regulations and procurement procedures causing workarounds (high)</td>
</tr>
<tr>
<td>Constraints (eHealth)</td>
<td>Prescribed use of the eID (moderate)</td>
<td>Prescribed use of the eID and technical problems causing workarounds (high)</td>
</tr>
</tbody>
</table>

**Enforcement and voluntariness**

Enforcement governs how pressures as imposed on organizations (Oliver, 1991) with law and regulations being some of the strongest types forcing compliance of organizations (DiMaggio & Powell, 1983). Thus in the eGov case, there are no regulations involved, but strong forces are used throughout the introduction process hence this level is assessed as being on a moderate level. Initially, the Board also states that it is mandatory to conform to this pressure, but this is later changed to voluntary. In addition, some authorities receive specific instructions to assess and prepare for conformance with the eGov eID which also can be seen as means of enforcing conformance. This is contrasted with the very strong enforcement in the eHealth case as related to law and regulations.

The outcome of the perceived level of enforcement in both cases clearly indicates being on significant lower levels since authorities in the eGov case avoid being influenced by the forces of conformity used by the Board. Similarly, in the eHealth case, with no significant sanctions issued to avoid misuse, non-compliance with the prescribed use of the eID hence violating the law and regulations, will, in fact, result in a minimum of negative consequences. However, still being rather notable since this means actors are restraining to comply with the imposition exerted by means of authority (Scott, 1987). Therefore, I argue that this outcome is clearly related to other perceived low levels of dimensions such as efficiency and consistency. In addition, it is also important to address the level of voluntariness since some pressures rely on a voluntary diffusion (Tolbert & Zucker, 1983) rather than regulatory enforcement. Thus, levels of voluntariness of pressures are assessed as initially low in the eGov case and equally low in the eHealth case. However, over time the Board changes this strategy and changes the eGov eID from being mandatory to voluntary to join. Hence, the outcome as the perceived voluntariness...
Concluding analysis and discussion

is low in the eGov case and moderate in the eHealth case. Therefore I argue that in the eGov case this poses a change in the underlying needed strategy in order to gain conformance since it changes from mandatory to voluntary hence becomes increasingly dependent on the voluntary diffusion and levels of institutionalization (Tolbert & Zucker, 1983) among authorities. As for the eHealth eID, findings indicate that the perceived level of voluntariness is closely related to knowledge of the purpose of the eHealth eID since more knowledgeable users show a significantly higher level of conformance (Table 31).

Table 31. Enforcement and voluntariness

<table>
<thead>
<tr>
<th>Dimension (case)</th>
<th>Pressure (level)</th>
<th>Barrier (level)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enforcement (eGov)</td>
<td>Compliance not enforced by law but forces used (moderate)</td>
<td>Compliance can not be forced (low)</td>
</tr>
<tr>
<td>Enforcement (eHealth)</td>
<td>Enforced by law and regulations (high)</td>
<td>No significant sanctions (low)</td>
</tr>
<tr>
<td>Voluntariness (eGov)</td>
<td>Initially mandatory to comply (later voluntary) (low, high)</td>
<td>Voluntary to join (high)</td>
</tr>
<tr>
<td>Voluntariness (eHealth)</td>
<td>Mandatory to comply (low)</td>
<td>Adherence as related to knowledge (moderate)</td>
</tr>
</tbody>
</table>

Uncertainty and interconnectedness

Since certainty as in the predictiveness of future states is a key factor driving organizations, a high level of uncertainty should, therefore, benefit conformance to pressures (Pfeffer & Salancik, 2003). In times of uncertainty, there are also higher levels of organizations imitating each other as means of hoping to cope with these uncertainties (DiMaggio & Powell, 1983). Hence, the level of uncertainty in the eGov case is initially assessed as high as the expiring procurement model is used as a main incentive of the solution. Thus initially the Board states that the only way authorities are going to get access to eID services is via the eGov eID. This results in very high levels of uncertainty in the public sector since major authorities are totally dependent on a working eID solution. This is contrasted by the eHealth case, where the uncertainty of the pressure is assessed as low since health care organizations have no other option that to adhere to the law and introduce the eHealth eID. However, as procurement workarounds are identified the uncertainty significantly drops in the eGov case hence actors are no longer
dependent the Board for continued access to eID services. In the eHealth case, uncer-
tainty increases to a moderate level due to repeated technical problems. Hence users
start to wonder about the future functionality and stability of the eHealth eID. Intercon-
ectedness or links and relationships that form between organizations tie these organi-
zations more closely to one another (DiMaggio & Powell, 1983). Thus this increased
connectedness and dependency will potentially work in favour of conformance to pres-
sures since it will, in turn, facilitate diffusion of institutional norms and values among
interconnected organizations (Oliver, 1991) and in turn also potentially facilitating con-
formance to pressures. The interconnectedness of the eGov eID pressure is assessed as
high since the support of major SPs, and current IdPs is described as crucial for this
introduction to succeed. However, as it turns out, the Board fails to interconnect these
actors with the majority of SPs and all current IdPs as clearly disconnected from the
solution. Thus, the connectedness between these actors seems to withstand the pressure
to conform and join the eGov eID. In my opinion, this outcome is clearly related to the
identification and later handling of the described security risks not working in favour of
the eGov eID as will be described in a later section. In the eHealth case, the pressure is
assessed as having a moderate level of interconnectedness since inter-organizational
user-groups are initially used to form links and relationships between health care organ-
izations introducing the eHealth eID. However, it later turns out that these forums are
not considered a success and as early adopters, the health care organization (county
council) in fact has very little contact with other organizations in the area (Table 32).

Table 32. Uncertainty and interconnectedness

<table>
<thead>
<tr>
<th>Dimension (case)</th>
<th>Pressure (level)</th>
<th>Barrier (level)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Uncertainty (eGov)</td>
<td>Expiring procurement model (high)</td>
<td>Procurement workarounds (low)</td>
</tr>
<tr>
<td>Uncertainty (eHealth)</td>
<td>Organization must adhere to law (low)</td>
<td>Technical problems during introduction (moderate)</td>
</tr>
<tr>
<td>Interconnectedness (eGov)</td>
<td>Support by a major SPs and IdPs (high)</td>
<td>Connected SPs and IdPs (low)</td>
</tr>
<tr>
<td>Interconnectedness (eHealth)</td>
<td>Inter-organizational user groups (moderate)</td>
<td>Early adopters, limited inter-organizational communication (low)</td>
</tr>
</tbody>
</table>
9.4.2 Strategic responses and enrolment

This section focuses on different types of strategic responses as enacted by main actors to try and negotiate emerging barriers in order to reach conformance to pressures. Unable to cover all enactments as featured in the cases in this analysis, this section will present a detailed analysis and discussion of two illustrative examples of acquiesce and escape (Oliver, 1991) one from each of the cases. Selection of these examples is based on the fact that in my opinion these are key events or aspects in these cases referring to how the identified security risks are handled in the eGov case and how the use of added benefits to the eID is used to prevent misuse in the eHealth case. Thus, presenting and analysing these two examples provide an overview and cover a certain range of different strategic responses at the same time trying to maintain a level of clarity and progression in this analysis. For analytical consistency, the next and final stage (Stage 4) will refer to the same two examples when discussing institutional implications of these examples. Moreover, this section provides yet another example of an applied typology as provided by Oliver (1991) covering strategic responses and tactics (see Section 4.2.3).

Acquiesce - compliance

The eGov case shows a clear example of acquiesce (agreeing) in the form of compliance when the Board finally acknowledges and conforms to the pressure put on the eGov eID introduction process to acknowledge and further analyse the identified security risks. However, this does not seem to be a result of negotiations and agreements with actors putting forth this need, but rather the result of resistance to the eGov eID being shared among authorities in the form of norms and values stating that the Board must deliver on security. Hence this is an example of normative external influences from actors’ professional fields such as information and cyber security putting strong demands on the eGov eID to deliver sufficient levels of security (c.f. interessement (Callon, 1986)). Moreover, the case shows that the Board first tries other strategies (dialogues, agreements, LoI), to try and potentially reduce or eliminate any negative consequences of the identified security risks.

These are examples of this actor initially trying to overcome resistance without acknowledging or addressing it (Hirschheim & Newman, 1991; Keen, 1981). Thus, when the barrier of security first starts to emerge as an institution among a constellation of SPs and IdPs, in my opinion, the Board applies rather traditionalist perspective perceiving the eGov eID as flawless, and any other opinions are only obstacles on the path of becoming fully operable (Hirschheim & Newman, 1988); this also resembling the myth of overt resistance to ICT introductions as inevitable and dysfunctional (Hirschheim & Newman, 1991). As will be described in the next section, this seemingly unwillingness to acknowledge these identified risks results in several SPs approaching another authority for an impartial security analysis and this, in turn, results in Government assigning the Board with the official task of leading this analysis. This final compliance of the requests of such an analysis is, in fact, the result of the barrier of security finally reaching
the top government level hence gets acknowledged in a government body that can exert pressure on the Board itself to conform to this barrier. This also becomes an example of organizations complying to external expectations in order to retain legitimacy and ability to perform activities (Meyer & Rowan, 1983). In terms of outcome and enrolment (Callon, 1986), the final acknowledgement and compliance to the barrier of security is on the whole perceived as positive by SPs and IdPs since this will finally result in a detailed security analysis of the eGov eID. However, since the road to this compliance shows the Board as initially dismissing and avoiding these issues, SPs and IdP as members of the different network or constellation based on very security aware participants, show clear concerns about how this analysis will turn out. Hence, the SP and IdP are still participating in the eGov eID network, but are extremely aware of how the Board will handle these issues onwards thus, in turn, doubting the competence of the Board to handle these issues.

Avoidance - concealment
In the eHealth case, there are clear indications of Central IT using the tactic of concealment as a means of disguising the underlying reason (Oliver, 1991) causing users not to conform to the prescribed use of the eHealth eID in order to maintain levels of security as delivered by the eID. Thus, I argue that this is an example of the main actors rather ceremonially adopting the myth (Meyer & Rowan, 1977) of making the eHealth eID card more valuable to users in order to enforce conformance to the prescribed handling of this card. Research suggests adoption and conformance to these types of smart card based solutions in health care are clearly dependent on perceived benefits (Aubert & Hamel, 2001) hence; this strategy seems relevant. However, the perceived benefits are, as described in this case, replaced with estimated ones, which turn out to be problematic.

Concealment can, therefore, be seen as a strategy of compliance (Oliver, 1991) however with a significant difference from compliance since conformity is only addressed on the surface. Hence, underlying controversies or covert behaviour as active resistance are not addressed (Marakas & Hornik, 1996). Further, to better understand why Central IT adopts this strategy it must be noted that it is applied in a strict reactive sense when problems of non-conformity and resistance to the eHealth eID emerge. Thus, prescribed proactive measures to address covert resistance (Markus, 2004) are not applied in this case since these problems and resistance emerges first after the eID is actually introduced in the user’s workplace. Thus, the applied strategy on concealment is used to enforce conformity on the surface by adding values and features to the eHealth eID card with estimated benefits and values to users.

The hope is thus put on these benefits acting as incentives to make the users perceive these cards as more valuable thus hopefully counteracting with the behaviour of leaving these cards unattended. Moreover, I argue that the organizational validity (Markus & Robey, 1983) of this strategy can clearly be contested since, as it turns out, the added
benefits are not perceived as valid by users. Instead of trying to address underlying factors such as the described relation between of knowledge and communication of the purposes of the eHealth eID as facilitating an increased institutionalization of its underlying purpose and incentives, I argue the estimated benefits as concealment in fact introduces a potential additional cause of resistance in the form of lack of felt need (Hirschheim & Newman, 1988). Since Central IT does not acknowledge the importance of a positive organizational fit as a key enabler (Robey, 1981) of the introduction as well as conformance to the eID, there is a clear tendency of trying to address symptoms of these underlying problems rather than the underlying constituent causes. Thus, I argue that this facilitates existing covert resistance to the eHealth eID to develop into a potential strong barrier for example as a barrier of flexibility based on high requirements of flexibility not med by the eHealth eID. This also indicated by the outcome of the negotiations enacted in relation to this estimated benefits strategy where users with specific requirements and demands as related to their medical working condition still perceive the eHealth eID as a clear negative influence on their work.

9.5 Stage 4: Institutionalization

9.5.1 Re-institutionalization of pressures

This final stage addresses the notion of pressures and barriers as institutions, being formed and reformed in a continuous reciprocal process as illustrated by the previously described four-stage institutional model (see Section 4.4.4). Hence this is motivated by institutions of normative, regulative or cultural-cognitive types being influenced as well as being influencers of actions and behaviours in turn also influencing other institutions. This also being in line with theories of institutional persistence (Zucker, 1977). Regarding how negotiations and outcome of the barrier of security affect the pressure of conformance to the eGov eID when the Government assigns the Board with the task of performing the detailed security analysis, the transmission (Zucker, 1977) of the pressure to conform and join the eGov eID continues. Hence, this is a clear indication of the Board trying to downplay any potential negative implications of these identified risks. This is exemplified by the Board continuing to transfer institutional norms and values among participant in the E-delegation (E-delegationen) by using the Letter of Intent (LoI) as an institutional carrier (Scott, 2014). Thus, during this time the institution of the eGov eID is maintained relative intact by the Board and not significantly affected by the barrier of security. However, with its government assignment, this actor can no longer maintain the institution as based on the notion that the eGov eID is not associated with any security flaws. Therefore, I argue that the resistance causes the institution of the eGov eID to be re-institutionalized with beliefs stating that there might be security risks in the solution but these will be handled accordingly. Therefore I also argue that this development of the Board being forced to re-institutionalize the norms and values assigned to the eGov eID marks a very important change in this process, however, as described, the institutional barrier of security will continue to exert significant pressures
on this process. In the eHealth case, I have found no similar clear change of resistance resulting in a re-institutionalization of pressures but still, maintenance of pressures as exerted by Central IT seem to change over time acknowledging the challenges of getting users to conform to pressures of how to handle and use eIDs. Thus, in a way the transmission of norms and values of the eHealth eID institution is over time adapted to the new estimated benefits added to the eID. However, in the latter case, the institution of the resistance, for example, the barrier of flexibility is not developed into the very strong force needed in order to make Central IT re-consider the estimated benefits strategy altogether.

With maintenance, this institution is contiguously adapted to the general strategy of trying to solve these problems of misuse. Another example is the ITR acting as an institutional agent on an operational level to try and enforce conformity to the pressure. However, over time there are examples of ITRs more or less resigning to the fact that users misuse their eIDs. The enforcement of pressure resigns to a silent acceptance of this type of misconduct with a clear lack of sanctions. Thus, this, in turn, allows this type of covert resistance to pass by without any significant resistance as a result of the ITR applying a strategy of avoidance. Therefore, I argue that this lack of re-institutionalization of pressures in the eHealth case is a result of Central IT not being subject to any pressure themselves in order to handle these issues, in turn, being a clear contrast to the eGov case where the Board is forced to acknowledge and accept the government task of leading the security analysis.

9.5.2 Institutionalization of barriers

In this final section of Stage 4, the two examples described above will be approached from a perspective focusing on the potential institutionalization of barriers thus referring to the transfer of inherent norms and values seen as real and taken for granted (Zucker, 1977) affecting actors as well as the organization (Berger & Luckmann, 1967). Thus, the restricting sense (Hughes, 1936) of the institutional perspective can in this context be translated as how the barrier restricts affected actors from conforming to the pressure of the eID being introduced. As previously described, the eID can in this work be seen as an institutional carrier (Jepperson, 1991; Scott, 2014) of norms and values, thus focusing on the institutionalization of this carrier as well as the related barrier, will provide new insights into the process of how translations of the eID actually affects this process. As indicated by the title of this dissertation, there is an emerging notion that these translations, in fact, are quite powerful and needs to be considered in order to better understand the process of institutionalization of barriers against eID introductions. The following two episodes as drawn from the cases will sum up the emerging insights and concepts described in the preceding three stages to provide insights into how and why these barriers, in fact, become institutionalized and reinforced during the introduction process. In addition, these episodes can also serve as examples of how the developing notion of the importance of translations as related to institutional barriers can be applied on actual episodes drawn from practice in the area of public sector eIDs. In detail, the
following illustrations and discussions will show how responses, as enacted by main actors in fact, strengthens the barrier instead of negotiating it. To provide transparency and a better understanding of the following illustrations, key events in each episode are numbered.

**Episode 1 – The security risks in the eGov case**

In the first episode illustrated in Figure 33, a major authority called Service provider #1 first puts forth the information of security risks in the eGov eID solution as identified by IdPs and this results in a mutual agreement with the Board to handle these issues as quickly as possible (1). Hence, if this swift handling of these risks turns out as anticipated these problems will be solved rather quickly. However, as it turns out, this is only the beginning of the following chain of interesting events especially from a process view on institutions (e.g. Barley & Tolbert, 1997). Time passes by and Service Provider #1, not being contacted by the Board, begins to wonder whatever happened to the agreement. Then, suddenly the Board distributes a Letter of Intent (LoI) to be signed by top management in selected authorities. Hence this will declare and confirm these authorities’ intent to join the solution (2).

Thus, Service Provider #1 reacts very strongly on this perceived clear act of avoidance by the Board and very actively re-negotiates the LoI to include phrasings such as the intent as conditional depending on the solving of outstanding issues prior to joining the eGov eID. In addition, this act also creates a clear mistrust in the Board on how the previous mutual agreement on the security as been handled (3). Hence, this lack of response from the Board causes a great deal of mistrust and concerns and eventually results in Service Provider #1 finally approaching the Swedish Civil Contingencies Agency (Myndigheten för samhällsskydd och beredskap, MSB) with a request for an external and impartial security analysis of the eGov eID (4). News about this request also spread among actors in the public sector and results in Service provider #2 and #3 submitting similar requests to this authority (5). As it turns out, MSB responds positively to these requests and reports that these should be taken very seriously (6). This outcome is in turn positively translated by the three service providers.

Finally, someone takes these concerns of the potential security risks in the eGov eID solution seriously. Later, these concerns reach the top government level results in the responsible ministry officially assigning a mission to perform a detailed security analysis of the eGov eID (7) and the mandate to lead this analysis is awarded to the Board accepting it (8). This results in a final official acknowledgement that the eGov eID might be related to security risks and hence is in need of a detailed analysis (Figure 33). So, at first glance, this seems like a very positive outcome. Although it started out a bit rough, the detailed security analysis of the eGov eID will be performed, and the outstanding issues hopefully addressed and solved. However, as described, the handling of these security risks are still one of the main reasons why Service Provider #1 finally later
chooses to opt-out of the eGov eID altogether. So what is exactly happening here – well I argue that this is a clear example of how the barrier of security manages to influence or not influence the introduction of the eGov eID.

Figure 33. Institutionalization of barrier - eGov case

Since security is one of the top priorities for Service Provider #1, representatives are profoundly dissatisfied with how these issues are handled by the Board after their initial agreement. Hence, the mistrust starts to grow which in turn also initiates the process of the development of the institutional barrier of security, in turn, putting pressure on the eGov eID solution in general and the Board in particular. This episode also shows that this particular authority is very dissatisfied with the dialogue or lack of dialogue with the Board during the path of the eGov eID introduction. In addition, an avoidance to act upon agreements is reported on repeated occasions. Based on the strong institutionalization of the institutional barrier of security, this authority translates almost all following actions and efforts related to the performed security analysis in a clearly negative way with every step and negative translation in turn further strengthening this barrier. Since the Board on repeated occasions try to push this authority into conformance and accept and join the solution, this authority continues to respond that it will not by any means sign until all security risks are solved and eliminated. Since negotiations fail to bridge this gap between the pressure, as exerted by the Board and the barrier, as exerted by this authority, this finally results in the authority officially stating its decision to opt-out of the eGov eID. Moreover, I argue that the lesson that can be learned from this episode is that institutional barriers over time can develop such strength that no means or measures
to handle or negotiate them seem to work. In this particular episode, I argue that this is a clear result of the actors, the Board and the authority, failing to establish an open dialogue to be able to better understand the constituents of pressures and barriers exerted.

Instead, with a lack of dialogue and communication, these two institutional ensembles continues to grow stronger in parallel with no chances of interrelation. In addition, this outcome may also indicate that the Board is simply overconfident in this particular authority eventually coming to senses and accepting the solution hence the importance and strength of this particular barrier is severely underestimated. As a result of the eGov eID introduction failing to take this particular aspect of eID practice into consideration, I argue that outcome nevertheless is far from surprising since identity providers also turn out to be very hesitant to sign with the Board and joint the eGov eID. Therefore, I argue that the lesson learned from this episode is that institutional barriers over time can develop such strength that no means or measures to handle or negotiate them seem to work.

**Episode 2 – Not removing the cards in the eHealth case**

To exemplify institutionalization in the eHealth case, the previously described efforts of Central IT to get users to conform to the prescribed use of the eHealth eID are used. Although, this episode is based on findings in the empirical world, for clear illustrative purposes I choose to formulate typical expressions based on my own interpretations of the main actors’ as well as affected actors’ views for pedagogical reasons (Figure 34). This episode starts with the main actor (Central IT) of the health care organization (county council) recognizing that the eHealth eID card is not handled according to instructions for example by users not removing the eHealth eID card from card readers when leaving the workstation (1). Thus, after further investigations, it comes to the Central IT’s attention that some users find the eID problematic and highly obstructing in their daily working routines.

![Figure 34. Institutionalization of barrier – eHealth case](image)

308
For example, the eID is perceived as rigid and related to significant latency during reconnection (2). These shortcomings are related to the prescribed use of the eID card. Thus, Central IT comes up with the idea of adding private benefits to the eID in an effort to increase its perceived value. As a result, users will hopefully to a greater extent treat it as a valuable document and in turn not leave it unattended (3). However, these private benefits such as being able to use the eHealth eID in public digital services are not perceived as anticipated by users. Instead, users respond that the eID is strictly associated with their professional role hence any added private benefits are perceived as irrelevant in a professional context (4). Central IT then moves one step further and tries to enforce users to conform to the prescribed use and remove the eID by adding door access as an added function to the card (5). However, as it turns out this only results in staff leaving doors open and emphasising that providing high quality has the highest priority (6).

This makes Central IT eventually being back to square one with users neither conforming to eID use nor responding as anticipated to added benefits and functions of the eID card (7). Further, I argue that one could clearly identify four different phases related to the barrier in the process shown in Figure 34. First, the enactment of the barrier when the users report that the eID actually obstructs their work hence the barrier puts pressure back on the introduction process. Second, the negotiation of the barrier when a central actor tries to negotiate this obstacle. Third, the enforcement of the barrier when users show that they still do not want to comply and finally forth, the institutionalization of the barrier when the collective behaviour of not conforming to the prescribed use is confirmed as shared meaning of social groups. Hence downplaying information security in favour of health care becomes the institutionalized reality in turn clearly related to existing institutions in health care. Not aware of neither the underlying gap between organization and technology nor the tendency of neglecting security in favour of the provision of medical care, the main actor is still left puzzled how this problem can be handled.

Thus, this episode clearly shows that Central IT chooses strategic responses that can be characterized as avoidance or escape by trying to change the behaviour of users with estimated benefits added to the eHealth eID cars without knowing exactly how these will affect operational practice or addressing the basic underlying controversies as a result of a poor organizational fit between the artefact (eID). Accordingly, this analysis shows that the eID’s sociomaterial context, such as the card reader, logon procedure, and information systems as well as users’ work contexts, intra- and inter-subjective translations, can become a significant barrier to being negotiated. Hence, I argue that these two cases together show potential re-institutionalization of pressures as well as institutionalization of barriers. The suggested relationship in this work is confirmed as well as the power to influence the introduction process as assigned to affected actors’ translations.
Concluding analysis and discussion

In summary, based on the analysis described above in the stage of institutionalization it should be quite clear that the affected actors to a significant extent acted as based on their own cognitive and cultural context as shaped by norms, values and beliefs (Barley & Tolbert, 1997). Thus the normative understandings of the institutional environment in the organization is important as put forth by Tolbert (1985), but I also stress that a significant emphasis needs to be put on cognitive understandings when trying to introduce IT artefacts depending on a complex interplay between social and material aspects; thus depending on the actor translating it in the same way as intended. Further, Scott (2014) even considers taking a step further and introduce a fourth pillar of ‘habitual dispositions’ to emphasize the force of habits as based on reasoning and conscious as well as unconscious choices. However, Scott also states that shared dispositions like habits instead can be seen as cultural-cognitive in essence but still acknowledging the importance of activities and routines as important carriers of institutional elements (Scott, 2014). This can also be seen as a positive indicator of the selected approach in this dissertation where I chose to arrange routines and habits alongside beliefs, norms and values while developing the concept of institutional barrier described above. In summary, these episodes provides the following insights:

The eHealth as well as the eGov case clearly show that by not acknowledging and addressing the root cause of the problem, the negative translations of the eID, there are clear risks that these translations turn into resistance that in turn can develop into a strong barrier against the eID introduction.

9.6 Three significant analytical concepts emerging

Based on the socio-institutional analytical approach applied in the analysis presented in this chapter, the process of densifying identified abstractions and conceptualizations results in the emergence of the following three significant concepts: (1) the barrier as related to pressures, (2) the artefact as an institution and (3) pillars, factors and dimensions. These concepts are in turn identified and motivated by showing a clear and potential level of generalizability in turn based on the interpretation of generalization as applied in this dissertation (i.e. as transferable knowledge, see Section 2.3.2). Hence, in preparation for upcoming conclusions, the following sections covers these concepts that will be further developed and presented in the form of more specific conclusions and propositions in the final chapter (Chapter 10).
9.6.1 The barriers as related to pressures

First, this analysis proves an important point; the ability and relevance to capture, characterize, assess and analyse institutional barriers in a structured and clear way in order to develop a better understanding of how and why they develop, their inherent factors and dimensions as well as their influence on the introduction process. I motivate this by the insights of responses and negotiations to barriers as enacted based merely on qualified guesses or estimations rather than any deeper understanding or reflections of the causes of these barriers. Thus, a lack of understanding of resistance and barriers in turn potentially results in responses and negotiations that are far from optimal since these are merely acting upon the symptoms of barriers rather than diagnosing any contradictions on deeper social and organizational levels. Second, this brings the question of how to approach the concept of institutional barriers, and here I argue that emerging concepts point toward the possibility of addressing these barriers in quite a similar analytic way as institutional pressures; a notion in turn further described in a later section. This indication, as motivated by new insights presented in this chapter, in turn, strengthens the developing notion of the institutional character of barriers as well as these barriers’ potential interrelatedness to the pressures they are actively opposing.

On a general level, this also indicates institutional barriers as, in my opinion, equally important to address, understand and handle as institutional pressures. Nevertheless, on several occasions in the presented cases, the pressures and barriers seem very far away from each other as for example in the case where the Board dismisses the security risks of the eGov eID while other actors claim these risks are extremely severe. Thus, as seemingly located on different polarities on a scale, I argue that this scale, in turn, is located in the very same institutional context as in this case regarding ‘norms and values of how security should be considered and handled by the eGov eID’. Hence, these opposing views might be considered as different translations reformed and reinforced as institutionalized norms and meanings in different organizational contexts. Hence, I argue that this, in turn, points towards insights where pressures and barriers can be perceived as ‘institutional siblings’ with assigned different translations rather than rivals measuring strengths and powers in different kinds of controversies and disputes.

9.6.2 The eID as a translated institution

In addition, with the application of established approaches regarding institutional pressures for conformity, the notion of the public eID as diverging from existing knowledge about the key forces behind these processes emerge. A recurring pattern in both cases is the apparent lack of emphasis on how the legitimacy of eID affects the introduction and conformance to the proposed eID programs. Hence, I argue that there are clear indications that main actors in these cases merely become institutional agents with the clear focus of further transferring the official and estimated incentives and benefits into different organizational contexts. Hence, this approach clearly diverges from existing the-
ory on the subject applying a rational focus on this process of conformance to institutional pressures with legitimacy as the preferable result. This is in clear contrast to the view presented in this chapter, with the emerging notion of perceiving the artefact being introduced (the eID) as an institutional carrier or even an institution in itself. Thus, this institution must be institutionalized in a positive way among affected actors in order to provide a successful introduction on social as well as organizational level.

This view being motivated by the eID as assigned with different meanings and translations over the course of the introduction. Hence, this perspective is clearly aligned with described current research emphasising the importance of addressing institutional aspects in order to better understand organizational behaviour and actions. However, still being in agreement with described views assigning an institutional character to agents as well as carriers and even technical artefacts, I argue that assigning this institutional character to these entities as carriers of institutional norms and values can also potentially result in introducing new levels of complexity into the research domain focusing on the relationships between the social and the technical (e.g. sociomateriality, see Section 3.3.2). Especially, since the analysis presented in this chapter also shows that different aspects of this institutional artefact, such as related to historical path dependence, also in turn can be seen as institutional, without this view applied in a rather well reflected and structured way I argue that there are clear indications that one could end up in a potential ‘institutional mess’.

In accord, to further investigate and explore the potential institutional character of artefacts in general and technical artefacts such as the eID in particular, I argue that the analysis performed in this dissertation suggests two important prerequisites for such approaches: (1) structured and clear approaches for analyses as well as (2) analytical approaches that facilitate the artefact to be addressed and analysed in the same way as other related actors. Hence, this is exemplified by the suggested approaches of focusing on pillars, factors and dimensions described in the next section as well as the underlying notions of agnosticism and generalized symmetry (Callon, 1986) as related to the applied translation analysis in turn related to Actor-Network Theory (ANT) (e.g. Latour, 1991; Law, 1999; Law & Callon, 1988).

9.6.3 Pillars, factors and dimensions

I argue that an important facilitator for the synthesis of the sociological and institutional perspective in the applied socio-institutional framework is the described underlying notion of institutional barriers as clearly related to institutional barriers. This view can potentially result in more integrative approaches in the future focusing on different translations of institutions. However, for this analysis, I choose to settle for a view where the pressure and barrier are treated as separate institutional entities or institutional forces but still, treating them as equals and clearly related offers the opportunity of applying a similar analytical approach to them. Further, as described in the early sections of this dissertation, a reflected strategy is to identify and potentially combine different existing
Concluding analysis and discussion

approaches for analysing institutional forces for conformity. The applied different existing typologies and concepts of institutional pressures potentially provides the needed structure and clarity as opposed to the rich descriptions provided by the sociological perspective. In my opinion, this analysis thus shows growing insights regarding the relevance, applicability as well as practical usefulness of the analytical concepts of institutional pillars (Scott, 2014) and institutional factors and dimensions (Oliver, 1991). Therefore, I argue that these typologies and classifications offer the significantly clear and hands-on approaches needed to avoid ending up with complex and/or diffuse meta-theoretical concepts and constructs that in turn result in propositions that are difficult to understand, evaluate and further develop; also referred to the potential risk of introducing an ‘institutional mess’. The application of ‘the pillars, factors and dimensions’ also allows for a quite powerful deconstruction of pressures into underlying aspects (factors) as well as potential outcome (dimensions). Converging with the hermeneutic stance applied in this work (i.e. to understand the whole by understanding the inherent parts and vice versa, see Section 2.2.2), these typologies are also indicated as being one of the key factors behind the synthesis of the institutional and sociological perspective in this framework.

This is motivated by the provided clear reference points to be matched and integrated with the different stages performed during translation analysis or ‘the sociology of translation’ (Callon, 1986). In addition, the underlying process perspective of the applied institutional as well as sociological perspective is identified as another important aspect facilitating this synthesis. Reflecting on the potential contributions of this approach, I argue that the presented level of detail and the fact that detailed aspects of institutional pressures and barriers get cross-referenced in turn results in a rather high level of complexity. Hence, as a result of this tentative stages of framework development, I argue that this implies a realistic emphasis on prescriptive knowledge rather than specific management measures. Nevertheless, I argue that this knowledge still can contribute to an increased understanding to be able to address these issues in a more informed way. In addition, this part of the analysis also put focus on important findings such as legitimacy not being significantly emphasised in efforts and enactments to negotiate pressures and barriers as related to the eID. Thus, in turn clearly challenging existing research describing legitimacy as a central driving force behind institutional pressures for organizational conformity.
10. Conclusions, implications and future research

This final chapter presents the conclusions, implications as well as suggestions for future work. The chapter starts with a summary of this work. This is followed by conclusions addressing research questions together with the knowledge contribution and central propositions. Next, to fulfil the described dual purpose of knowledge contribution, implications for research areas as well as for practice will be described. This is followed by a quality assessment including a follow-up of the applied framework by Klein and Myers and a discussion of limitations and potential criticisms of this study. The chapter is then concluded by areas and related questions for future research.

10.1 Introduction

10.1.1 A summary

One could say that classical phrases such as “Build it and they will come” and “Supply creates its own demand” as variations of Say’s Law on economics and how consumers of a particular service will automatically appear if provided by a supplier (e.g. Edmondson & Schluter, 1998) applies well in the eID cases presented in this dissertation. Since the incentives and benefits of these introductions are clear and positive from the main actor’s perspective, these actors anticipate a swift introduction and acceptance of the eIDs in these programs. The eGov eID will, by increased central governmental coordination and control, facilitate the development of eID enabled public digital services as well as simplify agreements between authorities as Service Providers (SPs) and Identity Providers (IdPs). In addition, it will facilitate new IdPs to more easily enter the market thus challenge the current oligopoly of commercial banks as the dominating IdPs. The eHealth eID, as regulated by law and national directives, will ensure patient security and integrity.

This increased level of information security in the public health safeguarding sensitive patient data is therefore seen as the unproblematic next step in the development of modern health care (eHealth). Moreover, I argue that the outset of these two eID introductions are very similar. With technological infrastructures and regulatory frameworks planned in detail (eGov eID) or already in place (eHealth eID), the supply of eID services created more or less by itself, and clear potential benefits for the public sector as a whole and the health sector respectively. Thus, both main actors anticipate that acceptance and use among affected actors will follow in a very unproblematic way. Therefore, I argue that both cases seem to apply described Say’s law in the public sector eID area – if the technical and regulatory foundation of eIDs are successfully implemented, an introduction resulting in acceptance and conformance will follow. However, as both
cases show, reality turns out to be somewhat more problematic since both eID introductions face significant obstacles and challenges. Accordingly, these challenges are focused in this dissertation with a special emphasis on the growing resistance to public sector eIDs among affected actors. In a similar way, both main actors face challenges in gaining the much needed broad acceptance of the eIDs. Needless to say, they really try to make an effort and handle the resistance predominantly by trying to address its negative consequences. As it turns out, these efforts are far from optimal. Hence, main actors are rather puzzled as to why a significant part of affected actors does not conform to the eIDs being introduced.

This resistance clearly influences the introductions in a negative way. In the eGov case, major authorities as SPs hesitate to join the eGov eID solution, and IdPs on the market are also very hesitant to accept the eGov eID as motivated by identified security risk in this solution. In the eHealth case, the main actor tries to handle the consequences of healthcare staff not accepting and using the eHealth eID according to instructions in turn seriously affecting the security level of confidential patient data. As a result of misuse by some users, the eHealth eID instead results in the introduction of new security risks instead of minimizing them. Therefore, I argue that both cases clearly illustrate the following paradox: The introduction of the public sector eID, with the aim of increasing security, results in decreasing security levels.

10.1.2 Insights related to research

There certainly is a considerable potential in introducing eIDs in the public sector as enablers of secure digital services internal as well as external to organizations (Melin et al., 2016) and the eID itself is becoming one of the basic pillars (EC, 2014a; Rössler, 2008) of eGovernment development on national as well as European levels (Grönlund & Horan, 2005; UN & ASPA, 2002). Put shortly, without the eID; individuals cannot be securely identified via digital channels (Corradini et al., 2006; Melin et al., 2013). Hence if this “small” and limited artefact for some reason fails to deliver, impact on society as a whole will be significant affecting external digital services to citizens, internal back office infrastructures as well as inter-organizational communications between authorities. Some officials even say, that due to current high levels of efficiency and digitization, without an eID they will have to go back and handle all issues on paper instead. Hence, in addition to the high dependency of public sector eIDs previously put forth, I argue that this also suggests a clear vulnerability. Therefore, I argue that this dependency is very important to keep in mind when trying to understand the role and concept of public sector eIDs since it not only enables digital authentication but also taps into and facilitates the current development of eGovernment (e.g. Chan & Pan, 2008) with aims such as efficiency of agencies and benefits for citizens (e.g. Axelsson et al., 2013).
In the light of challenges showed in the eGov and eHealth case, I argue that the eID, as a multi-level enabler, in fact rather drastically can turn into a powerful disabler of important societal functions, if the current supply of eID services to be used in the public sector is threatened. Thus, on a general level, this work shows that taking on and potentially challenging existing eID programs is a serious undertaking since the stakes are very high. Recently implemented EU regulations such as eIDAS (EU 910/2014), puts a renewed interest national eID solutions. Since being the object of interoperability in cross-border eID uses, the problematic character of national eID introductions, as confirmed by existing research (Kubicek & Noack, 2010c; Kubicek & Söderström, Submitted) as well as this dissertation, becomes a prerequisite to be able to understand the rather fragmented landscape of national eIDs across Europe. The international dependency prescribed to eIDs in such enforcing regulative efforts must, therefore, be weighed against the national dependency and historical path in the context of each country.

Challenges of introducing national eIDs are shared among several European countries such as Sweden (Grönlund, 2010; Söderström, 2012), Denmark (Hoff & Hoff, 2010), Finland (Rissanen, 2010), Estonia (Anthes, 2015; Martens, 2010), Germany (Noack & Kubicek, 2010) and United Kingdom (Beynon-Davies, 2011; Brostoff et al., 2013; Whitley, 2013). Hence, one important insight learned from these introductions is that unitary eID solutions as provided by the state are proven to be significantly less successful in terms of diffusion and use as compared to converging solutions between the public and private sectors. It, therefore, becomes important to acknowledge that as the dependency of eIDs in information society increases, this also creates an increased dependency on private sector actors in their role as leading identity providers; also touching upon the potential vulnerabilities of eIDs described above. Hence, as will be further described in implications below, any regulative efforts regarding national eIDs will have to take these important inter-dependencies into consideration.

As a sub area of research focusing on eGovernment challenges (e.g. Irani et al., 2007), this dissertation investigates current challenges related to public sector eIDs with a focus put on introductions of such eIDs. As described, this work suggests and contributes to a broader focus on public sector eIDs. Since I argue that previous research, as well as practice predominantly, apply a perspective of eIDs as artefacts or systems to be implemented in a technological and regulatory sense (e.g. Collings, 2008), such approaches tend to put other important perspectives such as social as well as organizational implications of the eID in the background. Hence I see a clear need of contesting and broadening such narrow perspectives of eIDs. This view is also strengthened by described current challenges in public sector eID efforts being, what I have interpreted, as clearly related to social and organizational implications of this artefact (see Section 1.1.3 and 1.1.4).
Therefore, this is in line with the suggested and confirmed unique character of the eID as a context-dependent artefact inherently bound to its social and organizational context. Hence, without a correctly issued certificate, in turn with a valid relation to a digital identity, and a service context for enrolment for a particular purpose (Beynon-Davies, 2006) the eID will not fulfil its aim of facilitating secure authentication. In this technical sense, I argue that the eID ‘becomes of the context’, a characteristic not shared by other more traditional ICT artefacts such as information systems, and this dissertation shows that this also applies in its organizational as well as the social setting. Therefore, a clear first conclusion of this work can be seen as the empirically confirmed view of the eID as a dependent and intertwined technical and social artefact (Orlikowski, 2007).

10.2 Conclusions and propositions

10.2.1 Addressing research questions

Presenting conclusions as related to described research questions (see Section 1.2) provides a clear and transparent way of ensuring the coherency of knowledge development. Hence this section covers the three research questions each presented with a related conclusion in turn followed by a motivation and discussion.

(RQ-1) What influence does the resistance among affected actors have on the introduction of public sector eIDs for use in external and internal digital services?

Conclusion: Resistance among affected actors as an important influence on the introduction of public sector eIDs is confirmed. Findings also provide important insights of social and organizational implications of such eID introductions.

The first research question (RQ-1) focuses on establishing the point of departure of this work with a confirmation of the existence of resistance among affected actors as well as its potential influence on the introduction process. Accordingly, the first step is to establish the existence of this phenomenon in the empirical world of authorities external use of the eID in public digital services (eGov eID) and eIDs for professional use in internal digital services in health care (eHealth eID). Addressing the first research question, provides the conclusion that the presented cases confirm affected actors as actively influencing the introductions based on their resistance to it and different types of influences on the introduction process are provided by both cases. However, despite resistance in these cases being handled as a problematic behaviour to be minimized or
Conclusions, implications and future research

reduced, I argue that these empirical findings also provide important insights of the social and organization implications of public sector eID introductions\textsuperscript{95}.

\begin{quote}
(RQ-2) How can this resistance be related to actors’ translations of the eID for further analysis, synthesis and insights?

Conclusion: By developing the socio-institutional framework integrating a sociological and institutional perspective, institutional barriers as opposing the institutional pressures of eID conformity are seen as institutions of shared norms and values as a result of actors’ translations. In addition, translation analysis also provides new insights on actors’ individual perspectives and relationships within the network.
\end{quote}

The second research question (RQ-2) puts the light on the suggested approach of relating the identified resistance with actors’ translation to facilitate further analysis, synthesis and insights. Addressing the second research question, the conclusion becomes the development and presentation of the tentative socio-institutional framework integrating the perspectives of sociology and institutionalism. The concept of actors’ translations is integrated into this framework by applying an actor- and network-focused approach which enables actors to be placed in a network facilitating analysis with a focus on individual perspectives as well as relationships between actors. This perspective treats all actors as equals. Hence human and non-human actors such as the eID, can be analysed in a similar way as affected human actors.

The concept of institutional barriers is also introduced as motivated by this resistance existing as shared meanings and behaviours among actors that I argue can be seen as socially constructed. The synthesis of these two perspectives results in the introduction of several existing theoretical concepts to facilitate further analysis. Since institutional barriers must be related to corresponding pressures, the concept of institutional pressures is used to categorize pressures to conform to eID introductions. This also results in the view of perceiving pressures as well as barriers as institutions of shared norms and values as developed from actors’ translations. This described mutuality of barriers and pressures also facilitates a clear level of comparison during analysis where the emphasis is put on the process of institutionalization.\textsuperscript{96}

\textsuperscript{96} This conclusion also relates to point no. 2 of the detailed aim and contributions of this work as described in Section 1.3.
The third question (RQ-3) focuses on how research and practice can potentially benefit from the insights and knowledge developed as a result of applying the socio-institutional framework. Special consideration also needs to be taken to how emerging insights and concepts are structured and conceptualized in order to facilitate this transfer of knowledge with the aim of facilitating research as well as practice. The aim here is to let the applied framework provide a structured and transparent analytic model to be able to present the logical reasoning behind the development of institutional barriers as related to actors’ translations later combined with emerging concepts to facilitate an improved understanding. Addressing the third research question results in the general conclusion that the socio-institutional framework provides the structure and concepts to be able to make this dual contribution.

To facilitate research for less problematic public sector eID introductions\(^7\), I argue that deeper insights into the underlying socio-institutional process are provided by presenting the synthesised framework. This, as an example of how institutions, in the form of barriers and pressures, can be linked to actors’ translations with a focus on resistance to public sector eIDs. Bringing these two levels together in the same framework will facilitate a better understanding of the root causes of barriers and pressures as related to actors’ translations. This also offers the opportunity of gaining a deeper understanding of how actors actually can influence and be influenced by these shared meanings, norms and values as assigned to institutions in turn transferred across organizational settings. In addition, by further developing and applying this framework, researchers will also be able to investigate and assess different parts of pressures for eID conformance as well as barriers opposing them. Since the actual outcome of negotiations of these pressures and barriers are integrated into this framework, this provides a rather straightforward way to assess these negotiations for a developed knowledge about causes of outcomes.

\(^7\) This conclusion also relates to point no. 3 of the detailed aim and contributions of this work as described in Section 1.3.
However, I argue that one of the main strengths of this approach that hopefully will facilitate research on public sector eIDs is the view of perceiving the eID introduction as a continuous institutional reciprocal process. Hence, only focusing on a particular part of this process, for example, pressures, will, in the end, turn out to be problematic. Regarding of how this approach will actually contribute practice with the aim of facilitating public sector eID introductions, I would say that it will probably be challenging to approach for practitioners in its current state. The framework is still in a very tentative state, rather complex and relational as well as full of abstract constructs and concepts are drawn from research. Hence, although having a potential validity, the applicability and usability of this framework in a practical organizational sense is far from optimal. However, me being an advocate of science outreach and different kinds of collaborative efforts, I still believe this framework can be used as a starting point for future collaborative efforts between academia and practice with the aim of discussing how these conclusions and results can potentially contribute to practice in the area of public sector eID introductions.

Since these kinds of inter- or intra-organizational introduction efforts are of a significant magnitude, they will inevitably affect a wide range of actors. Hence, I still argue that eID practice will benefit from an increased understanding of the central concepts presented in this work. By acknowledging the fact that actors’ translations, as well as institutional norms and values, will influence as well as be influenced by such efforts, the challenges we see today trying to negotiate the effects of institutional barriers can potentially be reduced. Operationalizing the concepts provided by this work will indeed be a challenge and in addition requires research methods of co-construction. However, I still believe such efforts and open dialogue between research and practice is a key. In addition, there are some rather clear typologies applied in the framework that can potentially be further developed and refined to potentially be used as a point of departure for this kind of collaborative efforts.

### 10.2.2 Knowledge contribution

In preparation for upcoming implications, it is relevant to discuss what type of knowledge being contributed by this dissertation. The contributed knowledge will be presented based on previously described knowledge types (Goldkuhl, 2011) covering conclusions as related to the research questions described above. The first conclusion clearly contributes with knowledge of a *categorical type* needed to be able to describe the basic notions and concepts of public sector eIDs as well as public sector introductions of eIDs (see Chapter 3). Further, the first conclusion also contributes knowledge of a *characterizing* type describing how resistance to public sector eID introductions influence this process and the implications of introductions on social and organizational

---

98 This conclusion also relates to point no. 4 of the detailed aim and contributions of this work as described in Section 1.3.
Conclusions, implications and future research

contexts. Hence, this knowledge contribution is based on the empirical evidence confirming this influence as well as its social and organizational implications (see Chapter 5 and 6). The second conclusion contributes with the socio-institutional framework hence presenting knowledge being of the three types of categorical, characterizing and explanatory. *Categorical* in the sense that basic concepts such as institutional pressures and institutional resistance need to be established (see Chapter 4). Actors’ translations play an important part in the synthesised framework hence this concept also needs to be established (see Chapter 4). The *characterizing* knowledge of the second contribution relates to translations of eIDs and related contexts as presented by translation analysis (see Chapter 7 and 8). In addition, the second conclusion contributes *explanatory* by developing and making transparent the process of synthesising the sociological and institutional perspective hence this covers the knowledge contribution of clearly relating institutional resistance to actors’ translations (see Chapter 4). The main explanatory contribution of this work is then related to applying the socio-institutional framework (see Chapter 9). Hence synthesising the proposed framework with translation analysis (see Chapter 7 and 8), with the proposed framework (see Chapter 4) as well as related theoretical and analytical perspectives (see Chapter 3 and 4). The type of *prescriptive* knowledge is contributed by the third and final conclusion in the delivery of the structures provided in the form of emerging concepts as a result of the applied socio-institutional framework. Hence, this facilitates prescriptive contribution in the form of conclusions as well as propositions. This concludes the knowledge contribution ending with insights to facilitate research as well as practice in the area of public sector eIDs (Chapter 10).

10.2.3 Three propositions

Next, emerging concepts presented in Chapter 9 will be further elaborated into the three propositions. This is motivated by the need of further refining these concepts into a more distinct form in order to act as a basis used to facilitate future research as well as practice. Hence, these propositions can be seen as the summarized and conceptualized knowledge contribution formulated on a general level aimed at the area of public sector eID introductions.

**P-1) The mutuality of pressures and barriers**

To facilitate future eID introductions, I argue that the concept of an existing relationship or mutuality between pressures and barriers (see Section 9.6.1) present opportunities for novel insights regarding challenges during public sector eID introductions. Hence, for an institutional force to be considered a pressure it should have some kind of opposition raised against it. Otherwise, in my opinion, it will just be an institution as assigned with norms and values just waiting to be institutionalized. The same applies to the institutional barrier, without an institutional pressure to resist, it will just be an institution as well. Hence, the proposition of ‘The mutuality of pressures and barriers’ emphasises the needed increased awareness and acknowledgement of the mutual existence and relationship between institutional pressure and barriers. Although I am fully aware that there is
a possibility of pressures being institutionalized without any significant covert or overt resistance. However, as related to the uniqueness of social and institutional contexts of organizations, I still argue that there will always be specific characteristics and requirements inherent to the organizational context that will challenge or influence the pressure seeking to be institutionalized.

(P-2) The translated institutions
The second proposition builds on the concept of perceiving the eID as a translated institution (see Section 9.6.2). Since this work shows that the eID, as well as institutional pressures and barriers, are all assigned with different meanings and values, these can be seen as institutions that get translated in different social and organizational contexts to be further transferred across organizational settings affecting actors as well as actions. The proposition of ‘The translated institutions’ put forth the need for an acknowledgement and increased understanding of these three institutions, as central to any public sector eID introduction, as constantly translated by affected actors during the introduction process. Hence as institutions, the pressure, the barrier as well as the eID, will change in meaning, norms and values as these are transferred across affected organizations and inevitably affect actors as well as actions. This also implies the above proposed mutuality be expanded to include the eID as illustrated in Figure 35. Thus, conformance regarding how these three central institutions are translated should be a matter of concern in any future public sector eID introduction.

![Figure 35. The translated institutions (inspired by Ogden & Richards, 1923, p. 11)](image)

(P-3) The importance of understanding and cooperation
The third and final proposition provides the initial suggestions on how to approach and apply the notions as prescribed by the previous two propositions (see Section 9.6.3). Hence, I argue that the suggested increase in levels of acknowledgement and awareness of this mutuality and translated institutions will only be facilitated if there is some guidance provided as to how these areas can potentially be approached. Hence this proposition of ‘The importance of cooperation and understanding’ is partly based on the described structured approaches and typologies applied in Chapter 9 that, when applied, will open up the previously black-boxed problematic aspects of pressures as well as
barriers. Hence, this will facilitate the revealing of different often conflicting views of pressures, barriers as well as eIDs. By addressing and analysing each of these institutions in a structured way, a new level of understanding of the constituent parts, the institutions as a whole as well the relations between them can emerge. This can therefore potentially facilitate a new era of cooperation in the area of public sector eIDs needed in order to be able to shape future eID developments. Cooperation based on knowledge and mutual understandings of different perspectives and translations rather than enforced pressures and opposing barriers.

10.3 Implications

10.3.1 For research

Discussing potential implications for research relates to how the described conclusions and contributions can bring new insights into related fields of research hence addresses the internal relevancy of this work (see Section 2.3.2). Based on my readings of literature, this dissertation, in fact, addresses several areas perceived as under researched or black-boxed and in need of further research. Regarding the research field of ISR, this work is a clear example of an multi- or transdisciplinary approach (e.g. Galliers, 2003a) addressing the historical lack of theorization of the ICT artefact (e.g. Orlikowski & Iacono, 2001) by providing a positive example of mid-range theory development (Grover & Lyytinen, 2015) based on qualitative interpretive case studies. This study will also bring positive insights to the research field of eGovernment since it, according to Heeks and Bailur (2007) qualifies as an example of good eGovernment research practice due to its multidisciplinary character, use of first hand empirical data and different perspectives of analysis.

Therefore, a central implication for research put forth in this work, with its process focus on the institutional contexts of public sector eID introductions, addresses two aspects described as being black-boxed in eGovernment research. (1) Underestimating complex institutional contexts in eGovernment development and (2) a lack of process oriented eGovernment studies (Yildiz, 2007). Due to this dissertations clear hermeneutic and interpretive character it also aims at providing a more holistic view of public sector eID introductions which in turn is a type of approach suggested to balance prior deterministic perspectives in eGovernment research (Lenk & Traunmüller, 1999; cited in Lenk & Traunmüller, 2002) as well as eID research (e.g. Collings, 2008). Further, with its rather solid grounding in existing theory, this work also addresses the reported lack of applied theory in this field (Heeks & Bailur, 2007). Hence, the described aim of further developing existing theory in the mid-range also addresses several calls for increased use of theory and theorization in eGovernment research (Bannister & Connolly, 2015; Grönlund, 2004; Heeks & Bailur, 2007). The perspectives putting forth the importance of organizational fit (e.g. Leifer, 1988) or organizational validity (e.g. Markus & Robey, 1983) are also expanded with the notion that organizational institutions also should be
Conclusions, implications and future research

considered in search of convergence between ICT and organizational context. Regarding resistance to ICT, with the applied focus of developing an increased understanding of resistance to public sector eID introductions, this work clearly challenges historical perspectives viewing resistance in this context as dysfunctional behaviours (Hirschheim & Newman, 1991) to be suppressed, ignored or eliminated (Hirschheim & Newman, 1991; Keen, 1981). Hence in line with Markus (1983) instead perceiving this resistance as a very important phenomenon to be used as a source for improvement. Since research tend to focus on different models and strategies for increased acceptance of ICT (Klaus & Blanton, 2010) this, in turn, results in a clear lack of how ICT artefacts are in fact related to organizational resistance (Marakas & Hornik, 1996; Markus, 2004).

In contrast and in line with Laumer and Eckhardt (2010) this dissertation does the opposite and focuses on the resistance thus in turn addresses this lack. In addition, this resistance with an institutional character by applying the concept of institutional barriers in line with Janssen et al. (2012). In relation to research in the area of path dependency, this dissertation clearly further explores the notion of institutions as having an important role when analysing the importance of historical decisions and actions (Page, 2006). In the context of eID research, the reported lack of research on what theories to consider to study eIDs when this phenomenon moves from being a new phenomenon approached from technical views (Halperin & Backhouse, 2008) to focuses on social and organizational implications. Further, this is also an attempt to describe an address implications of the reported high level of integration and dependence of eIDs in government (Melin et al., 2016). In addition, this dissertation also contributes to eID research field by addressing the historical lack of qualitative, empirical and transdisciplinary approaches (Halperin & Backhouse, 2008).

In the area of research focusing on national eIDs, this study also positions the eGov case in an international setting when identifying similarities and differences to other national eID introduction processes. Hence, I argue that it, therefore, contributes to the body of knowledge needed in order to further investigate and analyse the implications or ongoing European eID efforts such as cross-border eID use (the eIDAS regulation). Since these efforts have also been prescribed with a clear potential resistance (e.g. van Oranje-Nassau et al., 2009), I argue that this study is clearly in line with much needed efforts of investigating the prerequisites and potential challenges for cross-border eID interoperability on the European level. Interestingly enough, in my opinion, these EU initiatives can also be seen as institutional pressures of eID conformity on an international level – a potential perspective for the future research described in a later section. Regarding the applied sociological perspective as related to Actor-Network Theory (e.g. Latour, 1991; Law, 1999; Law & Callon, 1988), this perspective is applied in line with suggestions of ANT as suitable for research applying a sociomaterial perspective (Orlikowski & Scott, 2008) as well as an approach to address the important relationship between the artefact and technology in practice (Hanseth et al., 2004). In addition, by the applied perspective
of forming a relationship between actors’ translations and institutional resistance, this
dissertation also becomes an example of how ANT can potentially be integrated or syn-
thesised with other perspectives influenced by sociology such as institutionalism as an
example of mid-range theorization. Turning to the applied institutional perspective, this
dissertation clearly addresses the reported need of paying more attention to processes of
institutionalization (e.g. Barley & Tolbert, 1997; Tolbert & Zucker, 1996) thus in addi-
tion also unpacking the reported black-boxing of institutions (Zucker, 1977).

Since research has already acknowledged that resistance can be seen as an institutional
factor, but this resistance is often studied from an alignment perspective in order to fa-
cilitate ICT success (Sharma & Yetton, 2003). Hence, I argue that this is contrasted with
the approach in this work instead of focusing on the constituents and origins of this
resistance. In addition, described propositions clearly imply a potential convergence be-
tween institutional pressures and resistance to such pressures. I argue that these are only
different instantiations of similar institutional forces as related to clearly diverging trans-
lations. As exemplified in previous analyses, there can be clear potential synergies in
research if these two areas of pressures and resistance, previously perceived as distinctly
different, converge. The described implications of this work for research as based on the
reported lacks described above is summarized in Table 33.

Table 33. Implications for research

<table>
<thead>
<tr>
<th>Implication</th>
<th>For research areas</th>
</tr>
</thead>
<tbody>
<tr>
<td>Holistic view of eID introductions</td>
<td>eGovernment, eID</td>
</tr>
<tr>
<td>Complex institutional contexts</td>
<td>ISR, eGovernment, eID, ANT</td>
</tr>
<tr>
<td>Process orientation (creation, alteration and reproduction)</td>
<td>eGovernment, institutional</td>
</tr>
<tr>
<td>Organizational validity</td>
<td>Institutional</td>
</tr>
<tr>
<td>Organizational resistance</td>
<td>ISR, institutional</td>
</tr>
<tr>
<td>Path dependency</td>
<td>Institutional</td>
</tr>
<tr>
<td>Institutional barriers</td>
<td>ISR, institutional</td>
</tr>
<tr>
<td>Convergence of pressures and resistance</td>
<td>Institutional</td>
</tr>
</tbody>
</table>
10.3.2 For practice

The implications for practice described below are aimed at public sector actors as related to or affected by eID introductions on inter- as well as intra-organizational levels. Hence, the external relevancy of this work (see Section 2.3.2) is presented in the form of seven main implications for practice as the result of my efforts of trying to transfer and translate the described conclusions and contributions into a public sector eID practice context. The first implication for the practice is that any significant changes to a current operational eID solution will have consequences hence these consequences have to be acknowledged and handled accordingly. The most significant example of this is the Board’s efforts to gain acceptance for the eGov eID, without having any clear positive incentives or legitimacy, while there is a fully working eID solution in place (the Market eID). Major authorities are already having eID enabled digital services to expect or even demand business as usual while the eGov eID will inevitably result in significant consequences. The second implication is formulated as a need of acknowledging actors and eID contexts in affected organizations. Hence, for an eID to be accepted and used by actors in an inter- or intra-organizational context, implications and consequences of the eID to be introduced must be investigated a priori to be able to address any potential challenges in a proactive way, and this is best done in close collaboration with affected actors.

The third implication states the importance of gaining legitimacy for the eID to be introduced by presenting perceived and established benefits to affected actors. This is suggested since the cases in this dissertation clearly shows that benefits of the eID as based on mere estimations will not work in practice. Implication number four puts forward the importance of establishing the eID in practice by cooperative efforts and an open dialogue with affected actors. I strongly suggest that this should be a proactive effort since empirical findings clearly indicate that trying to establish an eID among affected actors during its introduction has proved to be very cumbersome and far from optimal. Implication number five suggests that if barriers or resistance to the eID being introduced develops, trying to identify underlying causes and negotiating them in an understanding and balanced way will most likely result in a decreasing resistance. The eGov, as well as the eHealth case in this dissertation, clearly show that ignoring or avoiding to address developing resistance will result in the development of strong barriers against the eID introduction that in turn can have severely negative consequences on the introduction process. The sixth implication for practice tries to introduce the importance of acknowledging and understanding actors’ translations in a practice context. Although being formulated in a research context, I argue that the importance of allowing and acknowledging different perspectives of the eID during the introduction process. Hence, this work clearly shows that the eID is an artefact that shows a significant variance in how it is perceived by different actors in different contexts. Even though it will be practically impossible to survey all different perspectives, proactive collaborative, communicative
Conclusions, implications and future research

and educational efforts will most likely work in favour of establishing a common definition among affected actors prior to the introduction.

![Diagram of triangle with eID, Enrolment, and Service]

Figure 36. The triangle of potential eID success (inspired by Ogden & Richards, 1923, p. 11)

In the final implication for practice, I put forth the importance of understanding and acknowledging the important relationship behind eID introductions in the public sector. As previously indicated, there seems to be a clear relationship between the eID, its service context as well as its diffusion and use (see Section 3.4.5). Hence, research shows that the eID is totally dependent on its context, for example, the digital service to which it contributes with secure authentication. Hence, without any digital services to use it in the eID will be useless. Further, for an eID introduction to become successful, the practice also shows that eID certificates must already be diffused and used to a significant extent for an eID introduction to become successful. For example, National eID solutions as managed solely by the state are the clearest examples. Nearly all cases in Europe show that without any convergence with IdPs already existing on the market the eID solution will inevitably fail due to low levels of diffusion and use. This clearly indicates that users still perceive the use of eID in private digital services as a very strong incentive for getting an eID. These three aspects make up this important relationship as illustrated by the triangle inspired by Ogden in Figure 36. However, in this triangle, I am refraining from using the word diffusion and instead use enrolment as inspired by Beynon-Davies (2006). Hence, to borrow this term from ANT seems very appropriate in this context since the term enrolment as related to eIDs implies diffusion among users as well as use. Although, these implications are primarily formulated for practice, they may still be relevant for research (Table 34).
Table 34. Implications for practice

<table>
<thead>
<tr>
<th>Implication</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Current eID solutions</td>
<td>Current eID solutions must be acknowledged and handled accordingly</td>
</tr>
<tr>
<td>Actors and eID contexts</td>
<td>Acknowledge actors and eID contexts in affected organizations</td>
</tr>
<tr>
<td>Legitimacy and perceived benefits</td>
<td>Work actively to gain legitimacy based on perceived benefits</td>
</tr>
<tr>
<td>Cooperation and dialogue</td>
<td>Use cooperative efforts and dialogue to establish the eID in practice</td>
</tr>
<tr>
<td>Understanding barriers</td>
<td>If barriers develop – identify underlying causes and negotiate in an understand-ing and balanced way</td>
</tr>
<tr>
<td>Understanding translations</td>
<td>Acknowledge and understand translations – they are powerful</td>
</tr>
<tr>
<td>The relationship</td>
<td>Acknowledge the critical relation between the eID, the service context and eID enrolment</td>
</tr>
</tbody>
</table>

10.4 Quality assessment

10.4.1 Klein & Myers’ seven principles

Since Klein and Myers (1999)’s seven principles of “Conducting and evaluating interpretive field studies in Information Systems” is presented in Chapter 2 as the selected approach to assessing the quality of this dissertation, a reassessment of these principles in the light of the concluded work is appropriate. As seen in Table 35 below, all principles have been accounted for and fulfilled different extents, and a more detailed assessment will follow. Previously described in Chapter 2 (see Section 2.7.2), these principles are adapted and guide this work throughout its process as a means of ensuring quality and validating the applied research methodology.

Table 35. Addressing principles by Klein & Myers' (1999)

<table>
<thead>
<tr>
<th>Principle</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. The Fundamental Principle of the Hermeneutic Circle</td>
<td>-An underlying hermeneutic perspective</td>
</tr>
<tr>
<td></td>
<td>-Analytical strategy (Multi-Grounded Theory, MGT)</td>
</tr>
<tr>
<td></td>
<td>-Development of the different chapters of the dissertation</td>
</tr>
<tr>
<td></td>
<td>-An underlying assumption applied throughout the entire dissertation process.</td>
</tr>
<tr>
<td>Principle</td>
<td>Example</td>
</tr>
<tr>
<td>-----------------------------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| 2. The Principle of Contextualization         | - Context awareness  
- Clear research focuses on explanation and findings in social and organizational contexts  
- Analytical perspectives grounded in sociology and institutionalism |
| 3. The Principle of Interaction Between Researchers and the Subjects | - The researcher and respondent as active interpreters  
- Interpretive interviews as social construction  
- Knowledge as co-constructed  
- High level of integration in applied research methodology |
| 4. The Principle of Abstraction and Generalization | - Analytical strategy (MGT)  
- Clear relation between concepts, abstractions and empirical context  
- Validity to the empirical context  
- Structure, transparency and clarity during sociological and institutional analysis  
- Analytical generalizability as transfer of knowledge  
- Applicability of theoretical and analytical perspectives  
- Dual contribution to research and practice |
| 5. The Principle of Dialogical Reasoning      | - Repeated cycles of revision  
- Iterative qualitative analysis  
- Empirical and theoretical grounding (MGT)  
- Constant comparisons between extant literature and emerging concepts during theory development  
- Presenting underlying assumptions and personal perspectives |
| 6. The Principle of Multiple Interpretations  | - Applied concept of double hermeneutics  
- Awareness of multiple interpretations among respondents/within empirical data  
- Different translations as a central focus  
- Agnosticism & general symmetry (ANT)  
- Data triangulation  
- Cross-checking with key informants |
Conclusions, implications and future research

<table>
<thead>
<tr>
<th>Principle</th>
<th>Example</th>
</tr>
</thead>
</table>
| 7. The Principle of Suspicion | - An applied general critical perspective  
- Identifying hidden agendas & inherent biases  
- Triangulation of subjects  
- Tracing historical events and decisions  
- Agnosticism & general symmetry (ANT) for undistorted views |

1. The fundamental principle of the hermeneutic circle
This dissertation, as being of an interpretive character, also applies the underlying perspective of hermeneutics (Butler, 1998). Thus constant focus shifts between the inherent parts and the whole become, as described throughout this work. Clear examples are the applied strategy of qualitative analysis as inspired by Multi-Grounded Theory (MGT) (Goldkuhl & Cronholm, 2010) (see Section 2.6.1). Further, the separate parts of this dissertation such as problem area addressed, research questions, theoretical and analytical perspectives, different levels of analysis as well as discussions and contributions also emerge in a close interplay and the work as a whole (c.f. Boell & Cecez-Kecmanovic, 2010).

2. The principle of contextualization
Since this dissertation focuses on social and organizational implications and challenges regarding public sector eIDs, the importance of contexts and contextualization becomes essential to this work on several levels. This principle is operationalized throughout this work in the form of me as a researcher being very context aware in each stage of this process. This is also the result of the fact that the aim of this work prescribes findings in social and organizational contexts as essential. Hence, with an analytical perspective as grounded in sociology and institutionalism, I argue that this also becomes an assurance of staying true to this principle since both of these theoretical views are highly context dependent.

3. The principle of interaction between researchers and the subjects
Since empirical data is mainly collected via interpretive interviews, this principle also becomes a very important aspect in order to fulfil the aim and purpose of this dissertation. Since this work, as described, applies a perspective on interpretive interviews as a social construction of data (c.f. Berger & Luckmann, 1967) and knowledge as co-constructed and facilitated by this interaction (Kvale & Brinkmann, 2009), principle number three in fact becomes fully integrated into the applied research methodology which I argue ensures a very high level of compliance.
4. The principle of abstraction and generalization
As described, the applied analytical strategy as influenced by MGT is well in line with the hermeneutic circle. MGT also facilitates the needed careful and reflective relation between concepts and abstractions to the empirical context (Klein & Myers, 1999). Further, this principle is also applied during later stages of analysis and discussions such as translation analysis (Chapter 7 and 8) as well as the applying the socio-institutional framework in Chapter 9. The potential generalizability of this work is described as resting rather on an interpretive interpretation of this concept focusing on a positive transfer of knowledge between organizational contexts (Walsham, 1995b). Hence, the focus is put on the logical reasoning behind results and conclusions (Walsham, 1993) and understandings of the deeper structures on the studied phenomenon as informed to other settings (Orlikowski & Baroudi, 1991).

The described conclusions and propositions will hopefully inform research as well as practice. An emphasis is put on the importance of focusing on the relationship between institutional pressures and resistance as in turn closely related to actors’ translations in a public sector eID context. Thus, the dissertation as a whole will also be an important contribution in order to support the reasoning as well as describe the analytical path arriving at these results. The generalizability of this work can also be related to the selected and applied theory in this work as a means of developing the knowledge hence the applicability of theoretical and analytical perspectives become an important contribution (Myers, 2009). Further, since generalizability also is related to the broader relevance of research (Lee & Baskerville, 2003), the intended dual contribution to research (internal relevancy) and practice (external relevancy) is explicated by the third research question (RQ-3) and handled accordingly (see Section 2.3.2).

5. The principle of dialogical reasoning
Since this principle, it is mainly adapted throughout the stages of analysis. Hence, these prescribed subsequence cycles of revision (Klein & Myers, 1999) converge with the performed iterative qualitative analysis as inspired by MGT. Further, regarding later stages of analysis such as translation analysis and developing the conceptual socio-institutional framework, this work is also done with constant comparisons between extant literature and emerging concepts as suggested by Eisenhardt (1989). In addition, since this principle addresses preconceptions, I also argue the importance of presenting underlying philosophical assumptions and research perspectives (Myers & Avison, 2002; Myers, 1997) in a clear transparent way as well as any personal preconceptions. Therefore, throughout this work I have tried to be as clear as possible regarding how these aspects potentially influence the work being performed.

6. The principle of multiple interpretations
This principle relates to respondents and researchers as active interpreters and the concept of double hermeneutics (Giddens, 1984). Being aware of multiple interpretations
become important if contradicting interpretations emerge (Klein & Myers, 1999). However, since one of the main focuses of this dissertation is actors’ translations in relation to the eID, multiple interpretations as translations become an essential part of the study. The multiple existing interpretations among respondents have been handled in an appropriate way by the methodology prescribed by the translation analysis. Especially the concepts of agnosticism and generalized symmetry (Callon, 1986) as means of providing impartiality towards the actors and using the same neutral vocabulary have been very helpful throughout this process. During this analysis, this impartiality is important for example as related to the use of assigned spokespersons (see Section 4.3.4). However, there are also situations when the existence of multiple interpretations results in a revision of my own preconceptions (Klein & Myers, 1999) as particularly related to the study of official documents to develop knowledge about the government context of the two cases. Thus, whenever possible, data triangulation (Janesick, 1994) is used to minimize any misinterpretations as well as cross-checking with individuals with expert knowledge in the field of study (key informants, see Section 2.4.1).

7. The principle of suspicion
This principle has been easily adapted throughout the entire process of this dissertation hence the search for possible biases or hidden agendas preferably regarding the eGov eID has been an ongoing process. I constantly try to find the plausible reasons why different actions or non-actions took place as well as repeatedly asking respondents to further elaborate on their arguments. Hence, any assumptions are based on several respondents putting forth similar perspectives of any given aspect of the eIDs – positive as well as negative. The level of suspicion is also manifested in the form of trying to identify any hidden agendas or covert measures by tracing government decisions back in history via official documents and respondents’ recollections of relevant historical events. In addition, during translation analysis, the concepts of agnosticism and generalized symmetry (Callon, 1986) turned out to be very helpful to be able to present empirical evidence in an undistorted way.

10.4.2 Limitations and potential criticisms
In this section, I will put forward two identified potential criticisms of this work. First, as described, I am fully aware that the applied perspective of Actor-Network Theory (ANT) (e.g. Latour, 1991; Law, 1999; Law & Callon, 1988) has been contested in several ways (see Section 4.3.3). Shortcomings described are for example the neglect of social structures (Harbers, 1995), being amoral (Star, 1991), treating humans and non-humans equally (Pels, 1995) and paying too much attention to details (Walsham, 1997). Nevertheless, I am fully confident that several of these potential criticisms are handled positively in this work neither clouding the objects of study nor negatively affecting results and conclusions. By applying a sociological as well as an institutional perspective, much attention is in fact paid on social structures (c.f. Harbers, 1995) since the concept of institutions becomes one of the central areas of focus. The sociology of translation (Callon, 1986) as applied during translation analysis also turns out to be very
helpful in identifying any influencing social relations and structures among actors. Not diving into the vast domain of ethics, I have still not been able to identify any moral or political bias influencing the study in a negative way; instead any potential revealing of covert political or government agendas is one of the main focuses of the eGov case to be able to understand the emergence and current challenges of the eGov eID. Further, not facing any problems with treating humans and nonhumans as equals during translation analysis and later stages of analysis and discussions. Thus, non-human actors are instead assigned with clearly defined spokespersons as prescribed by Callon (1986). During early stages of analysis, I am overwhelmed by the vast amount of empirical data and quite convinced I will end up with descriptions being too rich in details. However, through constant iterations and revision, I am confident about arriving at a suitable level of detail in these parts of the dissertation (Chapter 7 and 8) that hopefully will interest the reader but still maintaining the level of detail needed in order to synthesise these views with the institutional perspective. Second, I am aware that bringing together two significantly different cases as the eGov and eHealth case is an aspect of this work that will be challenged.

In relation to institutional analysis this challenge described as the ability to link different levels of analysis is also acknowledged (Schneiberg & Clemens, 2006). However, as I see it, the benefits of this approach clearly outweighs any costs since this also brings the opportunity of investigating and identifying recurring patterns across organizational levels which I argue further strengthens the concepts and propositions put forth as a result of this work. Hence, the selected strategy of using the eGov case being situated on a national level and the eHealth case covering organizational aspects in fact results in the identification of several important similarities between these cases for example how translations of the eIDs very actively facilitated the development of resistance to it, in turn, developed into the central concept of institutional barriers. Moreover, since translation analysis is performed in both cases, within the context of this dissertation, the differences regarding on which organizational levels empirical data is collected are effectively minimized. Hence, both cases are assigned with a level of analysis in close proximity of empirical data later to be synthesised with the institutional perspective which in turn addresses the challenge of linking together the level of explanatory factors and the institutional level of analysis (Schneiberg & Clemens, 2006). However, a key aspect that has to be solved in order for the socio-institutional framework to be applied is identifying during which stages of the institutional analysis to bring in the sociological level of empirical findings. However, after extensive work on the framework, I arrived at a suitable model with the framework being divided into separate, distinct stages which in turn are assigned with the output of different stages of translation analysis. I am fully aware of potential critique doubting the need for another conceptual model in ISR. However, in this work, I do perceive the framework as a ‘product of research’ but rather a means of developing knowledge in a structured and clear way. Having reflected on this seemingly positive fit between these two analytical strategies, I assume that they, in
Conclusions, implications and future research

essence, share several similarities such as clearly influenced by sociology, process driven, assigned with a clear goal as well as focused on actors, relationships and negotiations. However, it should also be noted that the identified four stages of the socio-institutional framework are based on my own interpretation and further development of an existing conceptual framework as presented by Mignerat and Rivard (2009). Moreover, in addition to these two potential criticisms, I am also very aware of the presented socio-institutional framework as potentially receiving critique due to its highly tentative status and primary focus on academia. However, the aim of this dissertation is not to develop and present any complete conceptual framework as a product with a potential transfer between organizational settings. Instead, this framework is rather the result of me addressing the third research question (RQ-3) and finding this tentative framework as providing a clear and structured path for the final analysis as well as presenting itself with a clear potential for future development and refinement.

10.5 Questions for future research

This section will cover some of my ideas and thoughts on how to further develop some of the concepts presented in this dissertation or to use the developed knowledge to pursue new research in other related directions.

10.5.1 The socio-institutional perspective

Since I argue that the applied socio-institutional perspective, as exemplified by the presented framework, provides a positive structure and synthesises the sociological and institutional perspective in a rather clear way to bring new insights, further development of this approach seems very relevant. At present, although I worked really hard to try and simplify this approach, I clearly agree that this perspective and framework covers stages that are too complex and/or too abstract to be considered outside academia. However, I argue that merging the sociological and institutional perspectives provides the identification of relationships that facilitate new insights that I have not come across during my readings of relevant literature. Hence, I argue that the explanatory power (Schneiberg & Clemens, 2006) of ‘the sociology on translation’ (Callon, 1986) applied in translation analysis in combination with different perspectives in institutionalism (e.g. DiMaggio & Powell, 1983; Oliver, 1991; Scott, 2014) has proved to be significant. This approach also confirms the possibility of interlinking case studies performed on different organizational levels hence in addressing one of the main concerns when seeking explanatory factors on other organizational levels (Schneiberg & Clemens, 2006). Thus I argue that this is facilitated by using translation analysis as a stage of pre-analysis with a result of reaching similar levels of abstractions and conceptualizations. However, as I see it one clear prerequisite being these case studies being performed with a similar focus as exemplified by the focus on investigating resistance to public sector eID introductions. This also suggests a future focus where the ties to the context of public sector

99 Yet again with a clear reference to the title of this dissertation.
eID introductions as loosened, hence perceiving the socio-institutional perspective as a general conceptual approach to investigate and understand different organizational settings and contexts where institutional pressures meet resistance in the form of institutional barriers. Thus my suggestion for future research in this area would be to seek the answer to how this perspective and framework can potentially bring further contributions to research as well as practice as guided by the following questions:

- How can the socio-institutional perspective be further developed in order to reduce its complexity and improve its usefulness and explanatory power?
- Can this perspective and framework be used as a basis for formulating clear and useful guidelines for practice and if so, how?
- What is the level of generalizability of this approach and how can it be improved?

### 10.5.2 New perspectives on digital identities and eIDs

Another very interesting area to further investigate is the potential of new emerging perspectives on digital identities and eIDs. This is motivated by my belief that we are still only in the early stages of digitization across society where prefixes such as e, smart or digital are still added to traditional concepts and constructs. Hence I argue that more integrated instantiations of these entities will follow as results of later stages, development and integration. Since the eGov case as well as the eHealth case clearly shows that the eID is still perceived as a separate digital entity with a particular use in a specific service context I argue that this in turn clearly indicates a rather weak connection between the eID and our digital identity. Hence with the current pace of technological development in mind, it might be fully possible that our identity will be predominantly digital based on the majority of services delivered via different digital channels. Thus, further pursuing these ideas and concepts would definitely be interesting but these are also my thoughts about the development in these areas in a longer perspective. Hence, related to the development in the near future it becomes clear that the eIDs of today will soon be outdated since these are based on quite old general concepts. Hence, in my opinion, this motivates investigating near future developments and uses of eIDs as related to the shown challenges of government to increase the level of coordination and control of eIDs while still keeping affected actors enrolled in the network hence this would suggest the development of some kind of hybrid eID model where the public and
private sector become equal players with clear mutual incentives and benefits. Thus, this area of research can be guided by questions such as:

-How can a new eID model be designed that facilitates increased governmental coordination and control while maintaining the legitimacy, trust, diffusion and use among public and private sector actors as well as users?

-Can such a coordinated market based hybrid eID model be facilitated by new forms of collaboration between the public and the private sector and if so – how can this processes be designed?

10.5.3 Translating institutions in other public sector areas

The final area of suggested future research relates to the positive incentives of the described emerging concept and proposition perceiving the institutional pressure, the barrier and the eID as being institutions that are constantly translated in a different way when transferred across organizational settings during the process of institutionalization. With this view, I also see a clear positive potential in applying this perspective in other ICT related areas depending on an institutional conformance in order to be successful. What comes to my mind here is the very relevant area of information security in the public sector. In 2015 information security in the public sector receives significant attention resulting in several investigations (SOU 2015:23; SOU 2015:25) and it is described that this area will need an increased focus and extensive efforts in the near future. This also becomes very interesting since a national eID solution, such as the eGov eID, would require authorities to classify their information from a security perspective, hence a nationally coordinated eID could very well become an active lever for this increased focus. Hence, questions to initially guide this area of research are formulated as:

-How can the perspective and concept of translating institutions be further developed and applied in the area of public sector information security efforts to facilitate a positive contribution?

-What are the relations between the information security and eID area and is there a potential of converging efforts with mutual benefits?
References

Literature


References


Denzin, N. K., & Lincoln, Y. S. (1994b). Introduction: Entering the field of qualitative research *Handbook of qualitative research* (pp. 1-17): SAGE.


Flick, U. (2004). Triangulation in qualitative research *A companion to qualitative research* (pp. 178-183): SAGE.


References


References


Lyytinen, K., & Klein, H. K. (1985). The critical theory of Jurgen Habermas as a basis for a theory of information systems *Research methods in information systems* (pp. 219-236).


References


Massacci, F., & Gadyatskaya, O. (2013). How to get better EID and Trust Services by leveraging eIDAS legislation on EU funded research results. *white paper.*


References


References

References


References


355
References


Webster, J., & Watson, R. T. (2002). Analyzing the past to prepare for the future: Writing a literature review. *Mis Quarterly, 26*(2), XIII-XXIII.


**Public Documents**


References


358
References


References


Lag om offentlig upphandling, Finansdepartementet, Svensk författningssamling, Stockholm.


Förordning med instruktion för E-hälsomyndigheten, Socialdepartementet, Svensk författningssamling, Stockholm.


References


References


Laws and regulations


Lag om valfrihetssystem i fråga om tjänster för elektronisk identifiering, Näringsdepartementet, Svensk författningssamling, Stockholm.

Reports

363


OECD. (2012). Rebuilding the scallop fishery in St. Brieuc Bay, France. OECD - Rebuilding fisheries,


LSE Media Policy Project Blog


Web and media


364
References


SKV. (2015a). Folkbokföringen igår och idag. Retrieved from https://www.skatteverket.se/privat/folkbokforing/omfolkbokforing/folkbokforingigari_dag.4.76a43be412206334b89800023140.html
upphandling/upphandlingar/forstudier/forstudie-informationsforsorjning-infratjanst-och-shs/default.htm

Interviews

Area Manager Agency#1 03/03/2014. (2014, 2014-03-03) Interview.
Assistant nurse Health Centre#1 17/12/2012. (2012) Interview.
Assistant nurse Health Centre#2 05/06/2013. (2013) Interview.
CIO Agency#1 15/10/2013. (2013) Interview.
Head of Digital Channels Agency#1 05/06/2014. (2014) Interview.
ITR Health Centre#1 13/03/2013. (2013) Interview.
ITR Health Centre#2 14/02/2013. (2013) Interview.
ITR Hospital Clinic 07/05/2013. (2013) Interview.
Manager Health Centre#1 05/12/2012. (2012) Interview.
Manager Hospital Clinic 07/05/2013. (2013) Interview.
Medical secretary Health Centre#1 17/12/2012. (2012) Interview.
Medical secretary Health Centre#2 14/02/2013. (2013) Interview.
Medical secretary Hospital Clinic 07/05/2013. (2013) Interview.
Registered nurse Health Centre#2 07/06/2013. (2013) Interview.
Registered nurse Hospital Clinic 07/05/2013. (2013) Interview.

Communication

Head of Secretariat 26/06/2015 (2015). [Conversation - Email].
Head of Secretariat January 30 2014 (2014). [Conversation].
References

Head of Section April 20 2015 (2015). [Conversation - Email].
Infrastructure Manager Agency#1 October 14 2013 (2013). [Conversation - Email].
Product Manager Agency#1 June 9 2015 (2015). [Conversation - Email].
Product Manager Agency#1 May 4 2015 (2015). [Conversation - Email].
Product Manager Bank#1 April 29 2015 (2015). [Conversation - Email].
Product Manager Bank#1 June 16 2015 (2015). [Conversation - Email].
Product Manager Bank#1 May 21 2015 (2015). [Conversation - Email].
Security Specialist Agency#1 December 2 2014 (2014). [Conversation - Email].
Security Specialist Agency#1 December 13 2013 (2013). [Conversation - Email].
Security Specialist Agency#1 December 18 2014 (2014). [Conversation - Email].
Security Specialist Agency#1 February 17 2014 (2014). [Conversation - Email].
Security Specialist Agency#1 January 14 2014 (2014). [Conversation - Email].
Security Specialist Agency#1 January 15 2014 (2014). [Conversation - Email].
Security Specialist Agency#1 January 16 2014 (2014). [Conversation - Email].
Security Specialist Agency#1 May 9 2014 (2014). [Conversation - Email].
Security Specialist Agency#1 November 3 2014 (2014). [Conversation - Email].
Security Specialist Agency#1 November 26 2014 (2014). [Conversation - Email].
Security Specialist Agency#1 September 5 2014 (2014). [Conversation - Email].
Appendix 1 – Interview guides

This appendix describes the two interview guides in the form of guiding questions used during semi-structured interview in each case study. Presented in Swedish with English translations in italics.

eGov case

1. Hur är er syn på Svensk e-legitimation, hur skulle ni förklara vad det är?
   *Your view of the eGov eID, how would you explain it?*

2. Fördelarna med en central koordinering och en sammanhållen infrastruktur?
   *The positive incentives of a central and coordinated eID infrastructure?*

3. Samverkan och er roll i införandet från utredningen och framåt nämnden – hur ser ni på den?
   *The cooperation and your part in the introduction from the investigation and onwards?*

4. Konsekvenser för er org. och hur det påverkar ert beslut att ansluta? Hantering av hinder ur ert perspektiv?
   *Consequences for your organization and how your decision to join is affected? The handling of challenges from your perspective?*

5. Orsaken till att utfärdare och myndigheter dröjer med att ansluta? Hade det kunnat hanteras på annat sätt?
   *The reason why providers hesitate to join? Could this have been handled in other ways?*

6. En hållbar lösning ur ett koordinerande perspektiv men hur ser ni på Svensk e-legitimation ur ert verksamhetsperspektiv?
   *A sustainable solution from a coordinating perspective but what is your view of the eGov eID from your business perspective?*

7. Hur har problem och brister i infrastrukturen hanterats? Hur har detta påverkat acceptans och tillit?
   *The handling of problems and shortcomings of the infrastructure? How has this affected acceptance and trust?*

8. Det arbete som kvarstår för att kunna gå i mål, hinner man eller kan det bli aktuellt med alternativa typer av lösningar t ex avtalsmässiga?

---

100 Courtesy phrases, presentation of the study, the issue of consent for audio recording as well as questions of organizational role and duties have been removed from these guides.
Appendix 1 – Interview guides

The work that remains to be done, will the Board make it on time or will there be a need for alternative solutions?

8. Slutligen, den största nyttan med Svensk e-legitimation t.ex för myndigheter, banker, medborgare etc?

Finally, what is the greatest benefit of the eGov eID, for authorities, banks and citizens et cetera?

**eHealth case**

1. Vad är er syn på e-tjänstekortet? Hur skulle ni förklara vad det är?

Your view of the eHealth eID? How would you explain it?

3. Hur har ni tidigare arbetat med e-tjänstekortet och hur ser ert pågående arbete ut?

How have you worked with eIDs in the past? What are your experiences of the introduction of the eHealth eID, positive as well as negative?

4. Vilka aktörer har deltagit i denna process och hur är er relation till dessa? Har resultatet av deltagandet motsvarat era förväntningar och intentioner?

Actors participating during this process and your relationship to them? Have the expectations and intentions been met?

5. Hur har kommunikation, förståelse och samverkan mellan olika parter fungerat under arbetets gång– positiva/negativa aspekter?

Cooperation, understanding and collaboration between different actors – positive as well as negative aspects?

6. Vilka planer och strategier ser ni som betydelsefulla för införande av e-tjänstekort och vilka möjligheter/utmaningar finns med dessa?

What plans and strategies are important to the introduction of the eID – what are the opportunities and challenges?

7. Vilka förväntningar och intentioner har ni haft på e-tjänstekortet och i vilken mån har dessa infriats? Finns det aspekter som inte identifierats/realiserats och i så fall ser ni någon förklaring till varför?

Your expectations and intentions of the eHealth eID – have these been met? Are there outstanding issues and if so – why?

8. Hur ser er fortsatta utveckling kring e-tjänstekortet ut? Vilka möjligheter respektive utmaningar ser ni?

The continued development of the eHealth eID – opportunities as well as challenges?
9. Hur har spridningen och användningen av e-tjänstekortet sett ut och hur ser ni på nuläge och framtid kring dessa aspekter?
*The diffusion and use of the eHealth eID – current state and future prospects?*

10. Vilka skillnader i behov och användning av e-tjänstekortet finns i er organisation och hur hanterar ni dessa?
*Are there any differences regarding the needs and use of the eHealth eID in your organization – how are these handled?*

11. Finns det andra nyckelaspekter som möjliggör respektive hinder spridningen och användningen av e-tjänstekortet?
*Are there any key factors facilitating or obstructing diffusion and use?*

12. Hur ser arbetet kring e-tjänstekort ut på regional och nationell nivå? Finns det sammanhang ni ingår i och vilka aktörer har ni i så fall kontakt med?
*Cooperation regarding the eHealth eID on regional and national level? What are the context and your role?*
Appendix 2 – Qualitative data analysis

To further clarify this process, the selected stages of Multi-Grounded Theory (MGT) are described in detail each with a selected exemplification from the dissertation.

Inductive coding

Inductive coding, the equivalent of open coding (Corbin & Strauss, 2008), is a process where the researcher, free of preconceptions, analyses the empirical data in a pure inductive manner. This is described as the proper approach to be able to be open minded and open for discoveries hidden within the data (Goldkuhl & Cronholm, 2010). This process is related to the strategy of approaching data from the ground up rather than relying on any theoretical propositions (Yin, 2014). Hence, the aim is to discover concepts from collected data for further development of concepts and categories. Thus, the developing concepts are representing the ideas found in data as interpreted during analysis (Corbin & Strauss, 2008).

Exemplification

Even though first stages of analysis are performed using Swedish language transcriptions, to be able to illustrate this process, a section of empirical data is translated and used as the basis of the exemplifications below. Hence, the original translated quote below describes an example of negative reactions of the eID as described during an interview by a Business specialist involved in the eID introduction at the central IT department (Central IT) in the eHealth case:

> Then there are others that think this [the eID] is very cumbersome and stupid. Why do we have to do this? They think that we [Central IT] have made this up just to make things harder for them. I think this is a quite common view. (Business specialist Central IT 08/10/2012)

This statement describes an example of the lack of acceptance among affected actors as reported to the respondent at Central IT. During inductive coding this piece of data is interpreted and analysed for further identification of concepts and interesting sections.
of data are highlighted and labels or codes formulated in my own words, i.e. interpretations, are assigned describing emerging ideas and thoughts during this process as illustrated in Table 36 below.

Figure 37. Example – First round of inductive coding

This first round of coding results in the identification of the concepts, properties and dimensions illustrated in Figure 37 and summarized in Table 36 below. Hence, the concept of the eID is assigned with the properties of reported resistance and Central IT to clarify that this is an example of resistance to the eID introduction as governed by Central IT. Further, the concept of causes of resistance is also developed with the properties of lack of understanding, lack of knowledge and negative view of Central IT to illustrate that there is clearly a lack of understanding and knowledge about the eID as well as a negative attitude towards Central IT in general that can potentially be related to this resistance. In addition, both these concepts are assigned with the dimension of assumed being common views of the eID in this organization. In addition, there is a clear level of uncertainty shown when the respondent only estimates that this resistance is a common view, hence the dimension of uncertainty is added to both concepts.

Table 36. Result from inductive coding

<table>
<thead>
<tr>
<th>Concept</th>
<th>Properties</th>
<th>Dimensions</th>
</tr>
</thead>
<tbody>
<tr>
<td>eID</td>
<td>Reported resistance, Central IT</td>
<td>Common view, Uncertainty</td>
</tr>
<tr>
<td>Causes of resistance</td>
<td>Lack of understanding, Lack of knowledge, Negative view of Central IT</td>
<td>Common view, Uncertainty</td>
</tr>
</tbody>
</table>
Appendix 2 – Qualitative data analysis

Conceptual refinement

Conceptual refinement means to be critical and constructive when working with the developing categories and this also includes a critical attitude towards the empirical statements to try to challenge and look beyond the data. This is motivated by empirical statements in turn are the products of the respondents own interpretations. Thus, a critical perspective is necessary to avoid being misled (Goldkuhl & Cronholm, 2010). Conceptual refinement refers to the process of clarifying the concepts developed during inductive coding or the other stages of the analysis. It should be performed in iteration with the other stages of theory generation to be able to refine and assess the developed concepts in order to define the categories. Hence, Goldkuhl and Cronholm (2010) suggest the use of the following six types of questions to guide this refinement:

| Q1. What is it? |
| Q2. Where does it exist? |
| Q3. What is the context of it? |
| Q4. What is the function of if? |
| Q5. What is the origin of it? |
| Q6. How do we speak about it? |

This use of questioning is also in line with Corbin and Strauss (2008) describing these questions as sensitizing, theoretical, and practical as well as guiding. In line with the critical stance in this stage, to be able to avoid any ambiguities and uncertainties, it is very important that emerging concepts and categories are further validated against empirical data. This being one of the strengths of this approach where further empirical grounding can include such validation for example by the use of previously described triangulation techniques.

Exemplification

During this process the guiding questions above are used to further refine the identified concepts above into categories and the result of this process is described in Table 37 below. The second identified concept from inductive coding (Causes of resistance) is addressed with the guiding questions with developing categories as a result. Hence, this could be an example of challenges or obstacles at operational level in this organization to be managed in order to successfully introduce and gain acceptance of the eID. The central categories of eID and resistance are assigned together with the developed categories of knowledge and norms and values. This is motivated by the described lack of knowledge about the eID and the seemingly oversimplified negative attitude towards it.
In turn this is interpreted as possibly related to an inherent negativity against the eID as potentially based on existing norms and values or the persons’ inner world, i.e. the knowledge of the self and external world (Goldkuhl, 2002).

### Table 37. Result from conceptual refinement

<table>
<thead>
<tr>
<th>Concept: Causes of resistance</th>
<th>Properties: Lack of understanding, Lack of knowledge, Negative view of Central IT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dimension: Common view, uncertainty</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Guiding questions</th>
<th>Answer</th>
</tr>
</thead>
<tbody>
<tr>
<td>Q1. What is it?</td>
<td>A potential obstacle regarding successful introduction and acceptance of the eID.</td>
</tr>
<tr>
<td>Q2. Where does it exist?</td>
<td>Central IT’s view of affected actors’ resistance to the eID.</td>
</tr>
<tr>
<td>Q3. What is the context of it?</td>
<td>The eID as perceived by affected actors.</td>
</tr>
<tr>
<td>Q4. What is the function of it?</td>
<td>Describes lack of acceptance and knowledge about the eID.</td>
</tr>
<tr>
<td>Q5. What is the origin of it?</td>
<td>Existing lack of trust in Central IT and perhaps a general resistance to ICT.</td>
</tr>
<tr>
<td>Q6. How do we speak about it?</td>
<td>Related to how the users’ perceive the eID and how it fits the users’ work context.</td>
</tr>
</tbody>
</table>

Developing categories: eID, resistance, knowledge, norms and values, work context

Further, related to the way the eID is spoken of by these users, as an obstacle in their daily work context, the category of **work context** is also added. However, the uncertainty still being a dimension regarding this being a common view or not among eID users has to be addressed and minimized. The concept as well as its properties shown in
Table 37 are validated among respondents working in operative roles in the following data collection process thus identified concept, properties and dimension are further empirically grounded.

**Theoretical matching**

As previously described, the stage of theoretical matching balances perceived insufficiency of pure empirical grounding in the evolving theory. Hence, in this process the researcher confronts the developing theory with other existing theories which in turn correlates or relates to the phenomena in focus. Then it is up to the researcher to identify these external theories to match the emergent one and this also involves matching of theories at different levels of abstraction. This theoretical matching can result in the need of revisions of the emerging theory and external categories can replace the formulated ones. This stage of the analysis is of great importance for the process as a whole and serves several purposes; the most obvious one being to minimize the risk of reinventing the wheel as a researcher and be able to develop knowledge based upon existing knowledge (Goldkuhl & Cronholm, 2010). Moreover, theoretical matching should not be confused with the concept of theoretical sampling where concepts derived from data influence coming rounds of data collection (Corbin & Strauss, 2008). Hence, theory here referring to the emerging one and not to already existing theory. The analytical stages of coding, conceptual refinement and theoretical matching forms an iterative circular process similar to the previously described hermeneutic principle where identified ideas in empirical data (the parts) are coded, conceptually refined and categorized and used as a basis for further matching of relevant existing theory that in turn informs the continued analysis (the whole). In this theoretically informed analysis as illustrated in Figure 38, I consider the stage of coding as being of an abductive character.

![Figure 38. Theoretically informed analysis](image-url)
Although the first stage of coding is inductive and not theoretically informed, the theoretical matching and conceptual refinement influences the further coding process with new concepts to look for and/or re-formulation of existing codes, concepts and categories. Hence this process of coding can be seen as being inductive during the first rounds of coding, as well as deductive when applying concepts from existing theory; a combination often described as abductive (Alvesson & Sköldberg, 2008).

**Exemplification**

As described above, my initial approach is to let the data speak for itself or get to grips with data as my supervisor so aptly put it. This is performed in an inductive manner during the inductive coding having as few preconceptions as possible regarding existing potential theoretical approaches and perspectives. However, not in any way being a pure inductive approach since the data collection is focused on some identified central concepts and themes previously described in the introduction such as the introduction of the eID, actors’ translations of the eID as well as a potential resistance to the eID. Hence, theoretical matching proved to be a very useful approach in letting developing concepts and categories act as keywords in online database searches. As an example, the category of resistance started to develop from data and is established and strengthened during the analysis together with the concepts of norms and values and work context as described above. Literature focusing on such contextual and social aspects in an organizational setting is identified resulting in the identification of the institutional perspective where the organizational and social context becomes an influence on actions and decisions within an organization (e.g. Berger & Luckmann, 1967; DiMaggio & Powell, 1983).

There are also examples of theoretical matching influencing conceptualization and categorization where for instance institutional pressures (e.g. Oliver, 1991) seems to be the accepted term for the forces exerting pressures upon organizations with the aim of increased homogenization in a specific field such as the eID. Hence the introductions of eIDs in both cases can be seen as examples of isomorphism (e.g. DiMaggio & Powell, 1983). Further, the clearly different interpretations or translations of the eID among affected actors in turn strengthens the selection of Actor-Network Theory (ANT) (e.g. Callon, 1986; Law & Callon, 1988) as a suitable analytical perspective to further investigate these variations in actors’ translations. The analysis proceeds with constant iterations between coding, categorization, theoretical matching as well as repeated reflections and revisions. Hence, the process of theoretical matching also assisted in establishing concepts and categories based on the accepted existing terminology that in turn facilitated further identification of existing literature as well as a using well established terms during analysis.
Appendix 3 – Assessment of SOU 2010:104

This appendix contains a detailed description of the Report (SOU 2010:104) governing the coming eGov eID as well as the mandate of the Board. To enable further elaboration while keeping transparency, important and critical parts of this report have been coded as numbered key action items in the following sections. This appendix is concluded by an assessment of the potential challenges of the eGov eID as presented in the Report.

The Board and the eGov eID

Background

The investigation, as prescribed by (Dir. 2010:69), is given the name “The investigation on the formation of an eID board” \(^{101}\) (Fi 2010:05) and started its work in the middle of the summer of 2010. Several interim reports are published in the fall of the same year, and the investigations’ final report “The eID Board and the Swedish eID” \(^{102}\) (SOU 2010:104) is presented in December of 2010. In this final report, henceforth referred to as the Report, the current Market eID system is described as relatively well functioning but with several inherent problematic aspects. Regarding these shortcomings, the report focused especially on the lack of a common public sector eID infrastructure (Key Action 1). The potential benefits of such an infrastructure are described as to facilitate and simplify the increased development of public sectors e-services (Key Action 2). The Report also described that the current model negatively affected new actors’ ability to enter the eID market (Key Action 3), i.e. the introduction of new identity providers. A federated eID solution is suggested (Key Action 4) (see The infrastructure below), which should provide a more coordinated and simplified eID infrastructure for the entire public sector (Key Action 5). In addition, it is also described that this type of solution would facilitate a continued positive eID development in the public sector (Key Action 6). In this infrastructure, citizens and employees should be able to use all eIDs, meeting the requirements of this infrastructure, for access to all current and future public sector e-services. Further, the report explicitly stated that the infrastructure should not prevent any existing solutions but rather create opportunities for the use in existing as well as future eID solutions (Key Action 7). The report also put forth that the current eID model is based on a framework agreement model that is soon to expire (Key Action 8) without any option of renewal. Hence, the conditions for public sector procurement had changed over time making it impossible to reuse the current framework agreement model, i.e. to sign multiple parallel contracts with several identity providers, and this is described as an important incentive for implementing the new eID solution.

---

\(^{101}\) Sv. Utredningen om bildande av en e-legitimationsnämnd

\(^{102}\) Sv. E-legitimationsnämnden och Svensk e-legitimation
Thus, this report described how the Swedish Government’s aims and goals concerning the public sector eID should be realized and in turn how the eID Board, as regulated by law (SFS 2010:1497)\(^{103}\), should accomplish it. In addition, it also described in detail how the federated eID infrastructure for the public sector should be designed and implemented (SOU 2010:104). Judging by the name (The investigation on the formation of an eID board), it is quite surprising to find out that the Report (SOU 2010:104) also contained a highly detailed technical description of the new eID solution (Key Action 9). However, the high level of detail in several of the aspects described in the report is motivated by the investigator with the aim to start an active dialogue about the outstanding issues of the solution (Key Action 10) and the Board would be able to make necessary amendments and modifications to the proposed plan. The investigation is described as conducted with different levels of cooperation with actors such as SKL, the agencies represented in the E-Delegationen, Datainspektionen, PTS and Domstolsverket. Several consultation meetings are also held with current providers within the eID 2008 and Infra framework agreements. In addition, the investigation is supported by a law firm and a technical consultant with several subcontractors. In addition, a person with competence of federated eID solutions in the academic world also acted as support to the group of consultants (SOU 2010:104).

**The Board**

The aim of the Board is described as to coordinate the public sector’s development and use of services for eIDs and eSigning and to ensure the availability of associated services and functions. This aim is in turn based on previous suggestions regarding how this area should be coordinated put forth by former actors such as Verva (Verva 2008:12) and E-Delegationen (SOU 2009:86). The Board is also described as an important prerequisite for the creation of a well-functioning eID as well as the creation of a strong trust in this authority on a national and international level. The proposed business model relied on actors working together, i.e. the Board, the service providers, the identity providers as well as citizens and employees. With this model, the service providers would gain a simplified access to eID services through the Board which in turn also would facilitate integration and e-service management. Further, the Board should also facilitate the creation of a corresponding eID infrastructure for the private sector in turn simplifying the use of the eID in public as well as private e-services. (SOU 2010:104). Although not described in the same detailed way as the public eID infrastructure an equivalent solution for the private sector would have a significant and rather unknown impact on the private market of eID solutions. However, this private market diffusion is described as very crucial for gaining profitability and the future success of the entire eGov eID model (SOU 2010:104) The five clear incentives of creating the Board have been summarized along with simplifying comments in Table 38.

\(^{103}\) Regulation with instructions for the eID Board;
Table 38. Main incentives for the eGov eID (SOU 2010:104, p. 14)

<table>
<thead>
<tr>
<th>Incentive</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>“[A] commercial and pricing model is created that is simple, transparent and long-term. It will lead to more predictable and possible lower cost than current framework agreement model”</td>
<td>A simple, sustainable and transparent business and pricing model</td>
</tr>
<tr>
<td>“[I]t should be easy for state agency, county or Municipality of access to services for electronic identification and signing. A state agency, county or municipality shall by a party - eID Board - get access to all services covered by the model”</td>
<td>A simplified access to eID and eSigning services for public sector actors</td>
</tr>
<tr>
<td>“[A] state agency, county or municipality in so small extent possible, should have to have the skills and functions to use services for electronic identification and signature of the business”</td>
<td>A minimum of competence and functionality needed for implementing public sector eID and eSigning services</td>
</tr>
<tr>
<td>“[T]he model should be, if, having regard to the other conditions possible, support technology neutrality and build on solutions developed by the market. Existing eIDs should, possibly with some adjustment to cope with the selected confidence level, function in the new model”</td>
<td>Support technology neutrality and be based on solutions developed by the market and existing eIDs should with adjustments work in this new model</td>
</tr>
<tr>
<td>“[A]ll actors on the market that meets the applicable requirements must be to become suppliers in the new model”</td>
<td>All actors that meet the relevant requirements should be able to become providers in the new model</td>
</tr>
</tbody>
</table>

Thus, it becomes clear that the incentives guiding the eGov eID solution is the need of a simple, sustainable and transparent business and pricing model (Key Action 11), a simplified access to eID and eSigning services (Key Action 12), a reduced dependence on specific skills among public sector actors (Key Action 13), ensuring technological
neutrality and the prevention of technological lock-in (Key Action 14) and to support existing as well as new identity providers (Key Action 15). On a more detailed level, the report described that the Board should manage, develop and be responsible for the infrastructure which would include the formulation of the required regulations, business and framework agreements. In addition the Board should develop guidelines for the Swedish eID and document the technical requirements i.e. the specification of trust levels (Levels of Assurance, LoA) and related technical solutions. The Board should also procure technical services for operation and maintenance of registers of eID and service providers, i.e. metadata registers and establish a system of choice for the Swedish eID.

However, these registers should not contain any personal data, i.e. only contain data on identity, attribute and service providers. Collaborative activities and activities to establish the new model in current eID practice are described as very important (Key Action 16) parts of the Board’s coming work. These should include actors such as public and private service providers as well as identity providers and other important related actors to optimize the potential of the new eID model (SOU 2010:104). Accordingly, the Board should establish and manage several different forums for cooperation with the most important affected actors of the eGov eID solution (Key Action 17). This would ensure the development of the best possible solution and introduction of the eID. The cooperative activities should also concretize important stages of the transitional process (Key Action 18). These cooperative efforts will also ensure that important aspects of the model will be analysed from several different perspectives and ensure participation and minimizing the negative aspects for actors (Key Action 19), i.e. users, service providers, identity providers and other relevant actors.

These cooperative efforts should be initialized on an early stage and include existing as well as future potential relevant actors (Key Action 20). A special need of cooperation with SKL is also described to ensure a successful transfer to the new eID model. The aim of these forums would be to discuss common questions, the further development of the model, problems and outstanding issues (Key Action 21). Thus the general aim would be to make available for the current actors in the market to create a dialogue and address important questions and issues. In addition the Board is instructed to host an annual event, the annual eID day (Key Action 22), as a way of communicating with the actors affected by or involved in the process (SOU 2010:104). On the practical level, the Board should be organized as a board and located physically at Skatteverket’s Headquarters in Stockholm. Thus this agency should provide facilities as well as administrative resources and the employees should also be employed by Skatteverket. The number of employees is estimated to 4 AWUs (Annual Work Units) hence during the development and introduction of the solution the Board would be dependent on external resources. Regarding the financing of the Board, it is described that its operations would need to be funded by annual grants during the period of 2011 to 2013. Since, the model
is planned to be fully operational from mid-2012, the additional operational costs introduced by the Board could then potentially be covered by the membership fees paid by the members of the infrastructure (see below). It is estimated that from 2014, the Board’s costs would be fully covered by the membership fees but this would in turn mean that the total fees paid by the service providers would need to be significantly increased (Key Action 23) (SOU 2010:104). Further, one could argue that this model could be perceived as quite risky since it would in fact mean that the costs of eID services would increase for the service providers and also it would also require the total acceptance and joining of all current service providers. Symptomatically, if the joining of the service providers instead would progress in a more gradual manner, the Board would need additional grants to finance its operations and the introduction of the eID2.0 would take longer time.

**The infrastructure**

In the report, the eGov eID regulative model is described as a rather complex infrastructure consisting of: (a) the accepted eIDs (Svensk e-legitimation), (b) a standardized infrastructure for electronic identification i.e. the identity federation (Infrastrukturen för identifiering), (c) a service for eSigning (Signaturtjänsten) and (d) a framework of regulations for the infrastructure. Hence on a functional level the services that needed to be provided within this infrastructure is (i) the issuing, use, verification and validation of the eIDs, i.e. eID-services, (ii) the infrastructure where the service providers would be able to obtain identity and attribute certificates\(^\text{104}\) to be able to check the validity of identity, legal authority or other attributes, (iii) a central register of actors’ services and functionality, i.e. the meta-register, for trust and secure exchange of needed information, (iv) a redirection service where the user is able to select the preferred identity provider and the identification process in turn takes place between the users and the selected provider and finally (v) a central service for eSigning. Thus, a result of this model is described as the service providers would no longer need to implement functionality to validate the identification and signing and be forced to negotiate and sign multiple agreements with identity providers (Key Action 24). Hence, the validation of the identification and signing will no longer be a part of the service provided by the service provider. This information will instead be established via identity and attribute certificates (SOU 2010:104). The infrastructure contained several interacting regulating frameworks established by legislation or civil contracts for procurement and the eID itself should be able to be issued to citizens (private eIDs) as well as to employees (business or professional eIDs) and the report described that specific technical solutions regarding the operation and management of this solution would have to be procured on the existing market. In addition, for this federated eID solution to work, the identity providers would also have to be able to supply standardized identity certificates to the public sector service providers (Key Action 25) (SOU 2010:104) which in turn would result in a supply

---

\(^{104}\) A digital certificate, i.e. document, containing attributes associated to the holder by the issuer e.g. legal or professional authority, employment or other attributes of importance to an individual.
of an additional service, i.e. identity certificates, if compared to the current eID1.0 model solely focused on authentication and validation of the eID, i.e. PKI and validation control. This specification together with the other identified actors of the eGov eID is illustrated in Figure 39.

![Figure 39. eGov eID actors (adapted from SOU 2010:104)](image)

It is also described that the transition to the new eGov eID model would require additional adjustments to existing e-services (Key Action 26) thus it would also be up to the service providers to assess the risks in preparations to the transfer to the eGov eID model (Key Action 27). This would in turn require competence and resources on the service provider’s side during the transitional phase (Key Action 28). The identity providers would have to adjust their businesses to the regulations in order to be able to get accepted as members of the eID infrastructure (Key Action 29) and the Report also described the potential need of having the two eID systems running in parallel during this transitional stage which in turn would be associated of additional costs and risks (Key Action 30) by the affected actors (SOU 2010:104). In addition the report described that the Board also should promote the creation of a parallel eID infrastructure for the private market (Key Action 31) in accordance with the objective of using the national eID in the private market as well (Key Action 32). Thus, eIDs accepted within the infrastructure should be able to be used in the public as well as e-services provided in the private market. A corresponding infrastructure for the private sector is described as central and essential for the eGov eID model to bear its financial costs (Key Action 33). The aim would be to establish two cooperating infrastructures of identification – one for the public sector and one for the private market that in essence make use of the same common regulations. The regulatory framework is designed to work in the public as well as private sector and support the coordination between these infrastructures. The same applied for the technical specifications (SAML 2.0\textsuperscript{105}) as well as the trust framework. However, still being in the early stages of development the details of the regulations of such coordination between a public and private eID infrastructure would need to be specified further (Key

\textsuperscript{105} A technical architecture used mainly for propagating identity certificates and attribute certificates among several trusted web domains, i.e. to provide Single-Sign On to multiple web sites.

384
Action 34) (SOU 2010:104). The central service for eSigning should be able to support security solutions of a higher level that supported by the current eID (Key Action 35) since it would not be able to provide an advanced electronic signature in accordance to the Act on Qualified Electronic Signatures (SFS 2000:832). This type of signature service will hence become independent of the design of the users specific eID solution. However, to ensure the security level, the user would have to identify oneself with the eID each time the signature service will be used (Key Action 36). In addition, to be able to present the text to be signed to the user the central signing service must have access to the text to be signed (Key Action 37) (SOU 2010:104) which in turn can be a potential security risk with the potential problematic aspects of centralizing a eSigning service as well as communicating sensitive information, i.e. the signed documents, between the service provider and the central eSigning service.

The Report also described specific details on how to handle eID solutions for professional use already existing in public sector organizations such as the SITHS eID solution used in the health care sector. To integrate such existing eID solutions into the eGov eID, the Report described the need of public authorities such as county councils becoming identity providers (Key Action 38) or Certificate Authorities (CAs) and this is motivated by the fact that they are the ones issuing the SITHS eIDs and hence is seen as the identity provider from the employee’s perspective. The solution proposed by the report for these kinds of solutions is quite interesting since the SITHS solution in fact is based on a private certificate issued by a third party (Telia) (Key Action 39) (SOU 2010:104). In summary, the infrastructure is aimed at establishing functions for eIDs, eSigning, identity certificates and attribute certificates in a model that is described as easy to understand and use for eID users and service providers and at the same time the infrastructure should provide legal and information security and personal integrity (SOU 2010:104). Thus, the infrastructure is described from a coordinating legal and business based perspective (Key Action 40) and in addition the technical specifications describe the model as based on the SAML v2.0 architecture (Key Action 41).

The regulations and trust framework

The regulations will establish the infrastructure in the public sector and coordinate and facilitate the use of eID and eSigning for service providers. Further, the infrastructure should be based on a trust framework in turn based on international standards that will provide the flexibility on a national and international level (SOU 2010:104). The trust in electronic identities in a federated identity context is most commonly referred to as identity assurance, i.e. that the identity can be assured or trusted to actually belong to the correct (human or technical) entity. Important actors on the work on standardization of identity assurance have been the National Institute of Standards and Technology’s Electronic Authentication Guideline (NIST, 2006), the Kantara Identity Assurance Framework (Kantara IAF, 2009) and the International Organization for Standardization

---

106 Sv. Säker IT för Hälso- och Sjukvården (Secure IT for Health Care)
and the International Electrotechnical Commission (ISO/IEC 29115, 2013). Commonly, the different levels of identity assurance are categorized into assurance levels and referred to as LoA (Level of Assurance) and the four levels of Kantara IAF is described in Table 39:

Table 39. The four assurance levels (Kantara IAF, 2009, p. 6)

<table>
<thead>
<tr>
<th>Level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Little or no confidence in the asserted identity’s validity</td>
</tr>
<tr>
<td>2</td>
<td>Some confidence in the asserted identity’s validity</td>
</tr>
<tr>
<td>3</td>
<td>High confidence in the asserted identity’s validity</td>
</tr>
<tr>
<td>4</td>
<td>Very high confidence in the asserted identity’s validity</td>
</tr>
</tbody>
</table>

These LoAs correspond to the provider’s different levels of technical and operational security and the different levels of validation of an individuals’ eID. Thus they could also be seen as an indication of the level of usability and issuing, i.e. the lower levels are more easy to use and eIDs are more easily issued although with a lower level of security. Higher levels include higher costs for issuing as well as usage and results in a higher level of trust associated with the identification. The report suggested that the Swedish eID should require LoA 3 or higher (Key Action 42) which in turn is described to correspond to the assurance level of current eIDs (SOU 2010:104). Hence, the aim of the trust framework is to provide a sustainable and technology neutral solution where the providers will free to develop and design the services as long as they live up to the requirements in the trust framework. Complex technical and administrative issues should not be regulated by law to facilitate the future development of the area. The civil regulations that will be required will be integrated into the agreements signed by the actors joining the infrastructure, i.e. the service providers and the identity providers. However, since the report is focused on constructing the new eID model, further development of these regulations will be needed. There is described that there are no existing regulations or agreements to refer to when constructing the eID model thus there would be a need of establishing a hierarchy of regulations and collaborative rules in law, regulations and government regulations that are clear and accessible (Key Action 43) (SOU 2010:104). Regarding information security and personal integrity, these are described
as very important aspects of the infrastructure (Key Action 44) and the regulations regarding these aspects are based on guidelines presented by MSB. In addition, a detailed analysis of information security aspects are described as necessary and prioritized and this should be done in close cooperation with relevant and affected actors (Key Action 45). To ensure personal security and integrity it is described that no personal data should be kept in the registers kept of identity providers and service providers (Key Action 46). These registers should not contain any information of the communication between the user and the service provider. Hence, by keeping this kind of data from the registered hosted by the Board would keep these registers from falling under the Personal Data Act (Personuppgiftslag, PUL) (SFS 1998:204) Any personal data needed, the service provider should communicate with the appropriate provider of this data e.g. related to roles and attributes and this handling will then regulated by the PUL.

Amendment to law - The System of Choice

In an interim report presented by the investigation (Fi 2010:05) it is concluded that the objectives with the eGov eID model could not be reached within the limits of the Public Procurement Act (Key Action 47) (SFS 2007:1091) since it required one winner to be awarded the contract. As a result, only users with eIDs issued by that particular provider would be able to access public sector e-services. In addition, the report described that there is a clear need of diversity within the eID area where the user should be able to select the most appropriate identity provider based on requirements like trust, service, functionality and quality. Accordingly, the report suggested an amendment to the law enabling a different procurement setup i.e. the creation of a System of Choice for the eID (Key Action 48). Since the eGov eID solution opens up for new identity providers the report suggested the introduction of a System of Choice based on existing law (SFS 2008:962) which prescribed that all providers, meeting the requirements, are accepted and entitled to sign agreements with the Board. This would in turn make it possible for the eID users to choose their preferred provider of the eID since all contracted IDPs would become available to all SPs assigned to the eGov eID solution. The System of Choice is also assessed to be a type of service concession, i.e. a service agreement which means that the compensation for services completely or partly consists of the right to use the service (SFS 2007:1091). This is also motivated by the proposition on the Law on Systems of Choice (Prop. 2008/09:29) which prescribed that service concessions where to be considered when the provider bears the financial risk of the service agreement (SOU 2010:104). Since the identity provider bears the economic risk of the agreements made with the Board, a System of Choice could be considered to be service concession (Key Action 49) (Prop. 2008/09:29) enabling the System of Choice to be designed without considering specific laws and directives such as the Public Procurement Act (SFS 2007:1091). Further, the existing system of choice that the report referred based the eGov eID model on had been previously implemented in health and social care (SFS 2008:962). Thus, establishing a System of Choice for the agreements with the providers of eID services would require an amendment to existing law (Key Action 50) and is considered a very important and basic prerequisite for the proposed eID model.
However, existing regulations prohibit municipalities and county councils to entrust an external part to decide which supplier should be awarded a contract (Key Action 51) i.e. a coordinated procurement process. In such a process the decision to award the contract must be made by each municipality and county council. Thus, the possibility for municipalities and county councils to delegate the awarding of the contract within the System of Choice is described as to be further investigated (Key Action 52) (SOU 2010:104).

**The business and pricing model**

The report described that the business model should work effectively with clear benefits for the affected actors and the costs for the service providers should be predictable and transparent and easy to budget (Key Action 53). The costs of the Board should initially be financed through fixed annual fees paid to the Board by the service providers (Key Action 54) and the main part of these fees should thereafter be paid to the identity providers based on their market share of the eID model (Key Action 55). The identity providers should also pay annual fees to the Board to become members and cover its supervision and administrative costs (Key Action 56). The rate of the fees paid by the service providers on municipality and county council level should be based on the number of potential users (Key Action 57) and the fees for service providers on agency level should be based on the number of employees (Key Action 58). Initially, the total compensation to the identity providers should correspond to the current market size hence the growth should be provided by an increasing number of public sectors actors joining the solution. The model prescribed that the use of services for eIDs and eSigning should be financed by the service providers (Key Action 59) i.e. the same layout as in the Market eID model and the identity providers should also establish the terms and conditions for issuing of eIDs (Key Action 60) which in turn may include additional costs for the users. This business and pricing model, although described quite briefly in the report, is described as simple, transparent and sustainable and result in foreseeable and possibly lower costs for the public sector than the current framework agreement model (Key Action 61). Further, the revenues from annual fees should as far as possible be used to cover the additional costs of the Board for coordinating the area (SOU 2010:104).

**Identified risks and obstacles**

The following aspects of the eID model is considered as critical for its success: the current identity providers choose not to participate in the model (Key Action 62), the service providers choose to use the current framework agreements instead of transferring to the new model (Key Action 63), the grants to the Board are decommissioned or drastically decreased after the first three years (Key Action 64) and the profitability should not be reached if the private sector is not included in the model, i.e. the parallel eID infrastructure for the private sector (Key Action 65). Accordingly, the countermeasures to handle and possibly minimize these identified risks are the following. It should be considered crucial to create the incentives needed in order for the identity providers to join the solution (Key Action 66). If the service providers choose to use the current
framework agreements as long as possible, this will also slow down the process of the public sector actors joining the model and in turn prevent the new solution from reaching its full potential. Hence the report suggested that the fees should be kept at an appropriate level to create incentives for service providers joining the solution (Key Action 67). Since it would only be possible to finance the eGov eID model’s operative costs if 100% of the current service providers joined the solution, the effects of the additional fees had to be limited. Although the focus in financial terms should be on securing the compensation to the identity providers it should also be considered to minimize the additional financial costs of the service providers instead of ensuring cost recovery for the Board by full market coverage from the beginning (Key Action 68). Since the new model would not be profitable without including the private sector, the market related to the public sector’s use of eIDs would be relatively limited (Key Action 69). It is described that there are several international examples showing that it would not be clear to reach profitability when establishing a national eID model and experiences showed that it is the private market that is the key to a future profitability of the eID model (Key Action 70). Therefore a proposal should be developed where a part of the private markets’ share of the eID use would be provided to the Board (Key Action 71) (SOU 2010:104).

An assessment of potential challenges

Assessment of probability and impact

Going through the Report (SOU 2010:104), I sensed that this plan, for several reasons, needed to be analysed and assessed further. Although the aim of this report is to describe the tasks of the Board and the coordinated eGov eID model that would simplify and facilitate the use of eIDs and eSigning services in the public sector, I argue that the report itself turned out to be equally complex and challenging to interpret and understand. The eGov eID solution is described in a relatively clear way from a coordinating perspective. However, from a perspective focusing the potential business consequences, i.e. an affected actor’s view, the descriptions are fragmented, sometimes unclear and sometimes quite drastic if compared to the current Market eID. Further, the Report itself described that the eGov eID solution needed to be further discussed and grounded in practice and I started to sense there would be a need to further analyse and assess it from a potential affected actor’s perspective, i.e. a practice view. This approach would in turn possibly provide important insights and serve as an interesting point of departure when describing the eGov eID efforts and the actual outcome of this project in the next chapter. Further, based on the identified challenges as derived from the Report (SOU 2010:104) and presented in Key Actions 62-69 (above); I argue that the preparatory work to provide the much needed trust and acceptance in the eGov eID solution might even have been underestimated. Although I fully agree with the identified risks and challenges presented in the Report, I argue that these challenges and potential obstacles related to the eGov eID model should instead have been based on the benefits and consequences of the Re-
port in its entirety rather than derived from a limited number of key aspects. Accordingly, this described lack of grounding in practice resulted in an analysis and assessment of the proposed model’s potential challenges and consequences in practice. In addition, this approach is chosen based on my view of the investigation (Fi 2010:05) as performed with a slightly naive perspective of how the entire public sector eID area could be coordinated as described in the Report (SOU 2010:104). The assessment process is performed by categorizing the set of identified key action points described above and further translating them into potential challenges with a related estimate of probability and impact on the entire eGov eID program. These challenges are then ranked based on their combined level of probability and impact, i.e. a challenge with very high probability and very high impact is considered as the most critical one to handle. This could be seen as the result of a qualitative probability assessment (e.g. Farahmand et al., 2005) and the result of this process is presented in Table 40. The motive of this assessment is to identify the main challenges of the eGov eID and rank them based on an estimated probability and impact to enable a later evaluation in the light of the actual outcome of the eGov eID introduction process. For intact traceability in relation to the Report (SOU 2010:104), the related key action points are also shown for each challenge.

Table 40. Assessment of identified challenges in (SOU 2010:104)

<table>
<thead>
<tr>
<th>Rank</th>
<th>Challenge</th>
<th>Probability</th>
<th>Impact</th>
<th>Related Key Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>The eGov eID fails to deliver a sufficient level of information security, assurance levels and personal integrity</td>
<td>Very high</td>
<td>Very high</td>
<td>35, 36, 37, 42, 44, 45, 46</td>
</tr>
<tr>
<td>2</td>
<td>The eGov eID model is not sufficiently established in public sector eID practice</td>
<td>Very high</td>
<td>Very high</td>
<td>16</td>
</tr>
<tr>
<td>3</td>
<td>Failing to cooperate and keep an active dialogue with actors affected by eGov eID model</td>
<td>High</td>
<td>Very high</td>
<td>10, 16, 17, 18, 19, 20, 21, 45</td>
</tr>
<tr>
<td>4</td>
<td>Consequences of the eGov eID will prevent current identity providers from joining</td>
<td>High</td>
<td>Very high</td>
<td>25, 29, 55, 56, 60, 62, 66</td>
</tr>
</tbody>
</table>
The next step is to translate the challenges into requirements of the eGov eID and a
detailed description and motivation of each of these will follow in the next sections.
Hence, the general progression of this process is to (1) categorize the key action points
in order to (2) identify and assess the challenges which in turn (3) are translated into
eight important requirements that need to be managed in a successful way by the forth-
coming Board.

**#1 - The need of an appropriate level of information security and personal integrity**

Information security and integrity described as important aspects in the Report but a
need of a more detailed information security analysis is also described that in turn could
be translated as a potential insufficient grounding in information security for the eGov
eID solution. This need also includes aspects like the central eSigning service that in
turn will need access to text to be signed and hence could be challenged from an infor-
mation security perspective saying that this in turn could be a clear risk of introducing a
centralized eSigning service that in the worst case scenario could be the single point of failure. Further, this also implies that public authorities such as county councils need to become identity providers in the eGov eID solution and the Report actually describes an example that involves an active and deliberate switch of certificate ownership that could

<table>
<thead>
<tr>
<th>Rank</th>
<th>Challenge</th>
<th>Probability</th>
<th>Impact</th>
<th>Related Key Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>Consequences of the eGov eID will prevent service providers from joining</td>
<td>High</td>
<td>Very high</td>
<td>2, 5, 23, 24, 26, 27, 28, 30, 38, 39, 53, 54, 57, 58, 59, 61, 63, 67, 68,</td>
</tr>
<tr>
<td>6</td>
<td>The incentives of eGov eID model are not accepted by affected actors, i.e. service providers and identity providers.</td>
<td>High</td>
<td>High</td>
<td>1, 2, 3, 4, 5, 6, 7, 9, 11, 12, 13, 14, 15, 22, 40, 41, 43, 64</td>
</tr>
<tr>
<td>7</td>
<td>Current law of public procurement will prohibit the new procurement model of the eGov eID</td>
<td>Low</td>
<td>Very high</td>
<td>8, 47, 48, 49, 50, 51, 52</td>
</tr>
<tr>
<td>8</td>
<td>The key private market will not be realized and the eGov eID model will be limited to the public sector and not reach profitability</td>
<td>High</td>
<td>Low</td>
<td>31, 32, 33, 34, 65, 69, 70, 71</td>
</tr>
</tbody>
</table>
be questioned or even deemed incorrect. The Report also described that no personal data should kept in registers but this is motivated not from a personal integrity perspective but rather from a legal one since it is described as a means of actively avoiding the PUL from being applied on the eGov eID model. Therefore, since I argue that the eGov eID model in itself is a clear case of a national security model for eIDs hence: The aspects of information security and personal integrity should be of critical importance. With its inherent lack of an in depth information security analysis, the proposition of a central eSigning function that could be highly vulnerable and its exemplification of a potential unauthorized switch of certificates, thus the related challenge of failing to meet this requirement has been assessed as being associated with: a very high probability and an equal very high impact.

#2 - The need of establishing the eID model in current practice

The Report very briefly touched upon the need of the Board establishing the eGov eID in practice and described this as very important. Thus, this should be accomplished by collaborative as well as specifically focused activities that should include public and private service providers, identity providers and other important related actors and the main aim of these activities is described as an optimization of the potential of the eGov eID. Although, I argue that it is noteworthy that this objective only is described very briefly, it can also be seen as closely related and a potential result of the objectives of getting the affected actors to accept the incentives of the solution and ensuring cooperation and keeping an open dialogue. Nevertheless, I argue that the view of establishing the eGov eID in practice as described in the Report is quite alarming and carries clear traces of an unproblematised management perspective of this process. A successful establishment in fact means that any problems encountered during the introduction is successfully solved and especially that all affected actors in the public sector, e.g. current and future service providers, perceive clear benefits and advantages of the eGov eID. Hence based on the fact that this is a very heterogeneous group of actors and that this establishment in a way is the key to a general acceptance of the eGov eID, I have chosen to rank this challenge as the second highest one with: a very high probability with an equal very high impact.

#3 - The importance of cooperation and dialogue with affected actors

The Report clearly described the need of an active dialogue regarding inherent problems of the eGov eID solution and outstanding issues. It is suggested that several different forums for cooperation should be created and involve important and affected actors. This approach would in turn facilitate an analysis being based on several different perspectives and ensure participation as well as having the potential of minimizing any negative effects. These cooperative efforts should be launched on an early stage of the eGov eID process to be initiated by the Board and also include a cooperative detailed information security analysis. I fully agree with this approach, where emphasis is put on the important aspects of cooperation but I also argue that seeking ex-post acceptance can prove to be highly problematic: Without developing the model in close cooperation

392
Appendix 3 – Assessment of SOU 2010:104

with the affected actors it will never be fully accepted in the public sector. Further, establishing an active dialogue between the Board and the affected actors in the public as well as the private sector and arrange these different kinds of forums will most likely take considerable time since this process also includes several related tasks such as identifying the suitable competence to be represented in each of these forums. In addition, and this part could be seen as the most crucial, the Board must create a sufficient level of legitimacy and trust in itself and regarding its mission to be able to get the affected actors interested in taking part in these cooperative processes.

Hence, I argue that the Report did severely underestimate the need of preparatory actions in order for these cooperative actions and forums to work. I argue that this is crucial since the public sector authorities in Sweden have a strong history of acting autonomously. Hence, without a mandatory law stating that authorities have no other choice than to accept and implement the eGov eID solution, the potential participation in these suggested cooperative efforts will most likely be based on each authority’s individual assessment of the benefits as well as costs of participating in these forums. An assessment in turn highly influenced by the authority’s trust in the Board and perceived legitimacy and acceptance of the eGov eID especially since the authorities have managed their own introductions and use of eID service for a considerable time. Hence I argue that the perspective on cooperation described by the Report is clearly un-problematised since a potential positive outcome of such efforts is based on careful preparatory work and also based on the fact that the Report described the time schedule of the eGov eID introduction as extremely forced on time, i.e. fully operational by mid-2012. Cooperation is extremely important especially for this kind of effort than spans the entire public sector that in turn is a clear starting point for a completely new public sector eID approach. However, as important this aspect is it cannot be enforced upon the affected actors but rather reside on acceptance, trust, legitimacy and volunteerism. Thus, this challenge is assessed with: a high probability and a very high impact.

#4 - The identity providers will need to accept and join

Although the Report clearly described the risk of identity providers not joining the eID solution and the importance of creating the incentives to get them to accept and join, I have found several contradictions regarding this important aspect. First, in the eGov eID model the identity providers are supposed to provide a new type of service i.e. the identity certificates to be used within the proposed federated eID solution. This would in fact be an addition to the eID services provided in the current Market eID solution which focuses solely on authentication and signing hence this functionality will have to be financed by the identity providers themselves. This also is an example of other anticipated adjustments to their businesses that the current providers will have to do in order to comply with the regulations and be accepted as providers within the eGov eID. The current providers will also be exposed to new competition since the eGov eID will open up the market for any identity provider that meets the requirements of the eGov eID. Although, one could argue that there are in fact no other providers existing within the
eID market with the same high level of diffusion and use, this could be seen as an approach that would possibly risk the positive relations between the banks and authorities that have developed since the Market eID is launched in 2003. Further, existing identity providers would also have to depend on the Board’s ability to assess and accept any new providers but there would still be a risk of the banks as providers existing in the same eID solution as less serious actors.

Thus it could be difficult to motivate why the banks would expose themselves to this risk since they are extremely dependent on the security level of the eID model as well as their high level of legitimacy and trust of their own e-banking customers. In addition, in the eGov eID model the providers should be compensated based on their actual market share which in turn is a clear departure from the previous Market eID transaction based pricing and compensation model. The providers will also have to pay annual fees to the Board to cover additional costs of the model. Even though the providers will be able to establish the terms and conditions towards their customers it is quite hard to see actors providing their eID services free of charge today moving to a non-free of charge model. To the current, the banks as identity providers have provided the public sector with eID services without any significant financial benefit. Hence the success of the Market eID has rather been built on a historical decision of providing the eIDs to the public sector as a service for business and citizen benefit. With the eGov eID, this setup can in fact be risked since the new model fails to deliver any clear positive benefits for current identity providers but instead is almost in its entirety focused on adding additional adjustments and costs. Accordingly, the risk of current identity providers choosing not to join the eGov eID has been assessed as: A high probability and an equal very high impact. As stated by the Report, the current identity providers are crucial for the eGov eID model but one have a hard time finding the incentives that should acknowledge this fact. Especially when very important aspects such as information security is to large extent left unaccounted for by the Report as described above. Hence, it could be questioned if the Report really aims at just supporting the current providers or to support and keep them, since they are clearly described as crucial for the eGov eID model to succeed. This is motivated by my standpoint that if the eGov eID is relying on the identity providers to accept and join, they might have been presented with a stronger business case and less additional costs. This challenge is assessed with: a high probability and a very high impact.

#5 - The service providers will need to accept and join

In addition to the identity providers joining, the acceptance and participation of the current service providers are also crucial for the success of the eGov eID model. Without the public sector service providers joining the eGov eID its main mission to provide a common eID infrastructure for the entire public sectors would completely fail. Accordingly, getting existing as well as future service providers to accept and participate should be considered as one of the highest priorities by the Board. However, it is assessed that the joining of the identity providers are considered as a higher priority (#3) than the
joining of the service providers (#4) since I argue that a scenario with no existing identity providers in the eID would definitely affect the service providers’ willingness to join, i.e. why join an eID model that lacks identity providers? Regarding the incentives for service providers such as agencies, municipalities and county councils to join, they are described as they will no longer have to sign multiple contracts with identity providers, their costs for the eGov eID services will be lower than in the current eID model, in some cases they will have an option to become identity providers (CAs) and will be transparent, predictable and easy to budget. Thus, they will benefit from the simplified eID infrastructure in order to simplify and facilitate their secure e-service development utilizing the eGov eID authentication and signing services. However, the Report also puts forth several effects of the eGov eID that one would doubt will serve as incentives for service providers to join but will rather serve as incentives not to join. Although the aim is described as lowering the costs this is clearly contradicted by the fact that the Report described that the total fees to be paid by the service providers needed to be increased. Further, in their role as the main financial contributors to the eGov eID solution, i.e. to finance the Board and its related services, there would also be limited chances of negotiating the levels of these charges. The temporary solution described for lowering the costs is in fact depending on the Governments increased funding of the Board. Further, the fees to be paid by the service providers would be paid based on their estimated number of users (citizens or employees) which in turn is a clear departure from the working transaction based pricing model in Market eID that in turn could be argued to be a more relevant pricing model for these kinds of services i.e. where agencies with high transaction e-service volumes pay a high cost than the smaller municipalities with lower volumes. Further, in this type of model the provider actually pays based on the usage of the service rather than an estimated of potential users or employees. In addition the transfer to eGov eID will result in the service providers needing to assess the risks of the transfer itself and account for the resources needed for adjustments of e-services. Hence there will be a need of competence and resources during this phase that in contrast to the aim of minimizing the need of competence on the service provider level. The providers will also have to account for need of running two parallel eID systems during the transition which in turn would be associated with both significant costs and risks. The Report also described that the legal aspects of the System of Choice needs to be further investigated on local government level which in turn also adds a significant uncertainty to the eGov eID model. In combination with the fact that providers in fact could continue with business as usual until further directives to join are issued, for example via legal pressures on agency level, I argue that this should be seen as a very likely scenario mainly due to the lack of clear positive benefits for service providers to join. The main question here being; will the identity providers join eGov eID purely based on loyalty towards the Board and trust in the eGov eID even if it results in significant costs and efforts? Thus the possibility of the providers not joining the eGov eID is assessed with: *a high probability and a very high impact.*
#6 - The incentives of the eGov eID model needs to be accepted

The process of accepting the basic incentives of the eGov eID model should be one of the important cornerstones of the process of developing and implementing it. On a general level, the investigation made use of the eID requirements put forth by actors like Verva, E-delegationen and Riksrevisionen and also included the aspects deemed as required from business, legal and technical perspectives. However, the investigation is clearly focused on progression on time and although it is described as a result of an active dialogue between affected actors, it also clearly acknowledged further development and grounding in practice. One could therefore assume that the grounding and acceptance in practice for obvious reasons is put in the background in favour of finalizing the details of this complex plan that in turn is produced on a tight schedule itself. Accordingly, the basic tenet that needs to be accepted by the affected actor in the public sector is first of all the need of a common eID infrastructure. This argument is in turn motivated with several positive benefits such as facilitate and simplify increased public sectors e-service development and that new actors must be able to enter the eID market. Further, this coordinated and simplified eID infrastructure should facilitate the use of existing and future eID solutions by offering a simplified access to eID and eSigning services and a reduced dependence of specific skills among public sector actors. However, it is a fact that public secure e-services have been developed at a successful rate during the 2000s but symptomatically some of the largest public agencies have taken the lead. The investigation, in line with previous reports, described the problem of the slow local government development of e-services. However, I argue that this aspect might not be seen as a problem at all but rather is the result of a much slower maturing process regarding the identification and realization of positive digitization effects. As described above, the initial driving force behind the agencies secure e-service development is firstly the identified internal efficiency and secondly the benefits of external e-services towards citizens. Thus, the identified lack of e-services on local government level described could in turn be a result of a lack of clear incentives and benefits for e-service development rather than the local government actors lacking the required skills and competence for implementing eID and eSigning services. A top down strategy based on political e-government strategies and incentives could prove much harder to accept and implement especially since local government has a history of strong autonomy. In addition, one could also have a hard time in agreeing with the argument that a simplified eID model is the key to local government e-service success since several intermediaries already have offered packaged eID solution to the public sector under several years. To ensure technological neutrality and the prevention of technological lock-in should also most likely been seen as mainly a problem on political level since the current market driven Market eID model is a result of the public and private sector coming together for mutual causes whereas the eGov eID model could be perceived as built upon mainly political incentives.
Further, the aim of ensuring the supply of eID and eSigning services for the entire public sector and describing a solution covering a wide range of related aspects resulted in the Report being a very complex hierarchy of directives and regulations i.e. the regulations framework. Thus, I argue that the argument of the aim of producing legal and business regulations and law in a clear accessible way in itself is a contradiction especially when the aim is to cover the entire public sector as well as participating actors on the private market. Further, the need of a simple, sustainable and transparent business and pricing model resulted in a pricing model based on potential users rather than transaction volumes which in turn are a clear departure from the fully working and rather successful transaction based business model of Market eID. The aim of opening up the eID market for new providers seems like a positive benefit but the outspoken support of existing providers probably gets dented based additional investments for adjustments and an inferior business model. In summary I argue that the basic incentives of the eGov eID clearly reflect the inherent political agenda and strategy which resulted in clear contradictions in the incentives and consequences to join for the service providers as well as the identity providers as described above. Since, the acceptance of the model should be a basic prerequisite therefore the challenge of these affected actors failing to accept the model is assessed with: a high probability and an equal high impact.

#7 – The need of legal amendments to support the eGov eID procurement model

As described, the need for an updated procurement model regarding eID services used in the public sector is one of the main incentives put forth in the Report. This is motivated by the current model being based on a soon to be expired agreement model that in turn had been confirmed by a special investigation of the prerequisites of a continuance of the procurement of eID services within the current procurement act. In addition the need of diversity in the field of identity providers as well as freedom of choice is put forth as incentives of the suggested System of Choice for eID services that in turn would require significant amendments to law, i.e. the introduction of a new law dedicated to this new way of procuring eID services within the public sector where contracts with IDPs are signed on a central level with an awarded power of attorney from the SPs hence making all IDPs eID services available to all SPs and in turn all end users of online services. However, I argue that there are several concerns regarding this new procurement setup. First, as acknowledged by the Report there is the question of how this model will work in conjunction with the Local Government Act (Kommunallag) (1991:900) regarding awarding the Board to sign with IDPs under a power of attorney for public sector actors. Second, even though this proposed model is based on existing law this is a system of choice regarding health care services i.e. in a completely different context. Third, this model would result in the creation of a new law regarding the procurement of a specific technical service hence I argue that the appropriateness of this approach can be questioned and forth, this amendment to law will most likely take a considerable time to finalize and thus require full attention from the Board with the potential of affecting the overall introduction of the eGov eID negatively. But nevertheless, since the
proposed new procurement model is a result of extensive legal preparatory work, failing to realizing its potential is assessed with: a low probability but with a very high impact.

#8 - The eID model must be realized within the private market

The aim of the importance of spreading the use of the eGov eID to the private market is clear; without the use in the public as well as the private market the eGov eID will not reach its anticipated profitability and the Report even put further emphasis on this aspect stating that it is central and essential for the model’s success and for it to able to cover its financial costs. Although it sounds somewhat strange that a public sector infrastructure should have profitability with the aid of the private sector as an aim, it could also be seen as a paradox that an eID model that aims to minimize the banking sector eID proprietary monopoly results in a new model where the private market holds the key to its profitability and success. Hence, it is described that the Board should promote the parallel private market eID infrastructure but regulations and coordination between infrastructures needed to be specified further. Since the aspects of the private infrastructure is described very briefly in the investigation it stands quite clear that this aspect of the eGov eID might have been added to show that the solution really could be a better financial success than just limited to the public sector. However, it is also a fact that there probably is not much of a business case regarding eID and eSigning services since the tendencies for e.g. the banking sector is that the transaction volumes increase while the price per authentication or signing decreases. This service has no significant value in itself, it is in a given context that requires authentication and signing that gives it a meaning. Hence I tend to argue that the aim of a profitable private eID infrastructure would most likely be extremely hard or even impossible to reach. However, if there would be a strong demand on consumer level and the private sector actors should perceive that the eGov eID is related to a very high level of trust and legitimacy the outlook should definitely be more positive. However, this is just mere assumptions but the fact is that the Report clearly described the need for legitimacy and trust in the eGov eID but left out a description of the process to create it. Legitimacy and trust are developed between parties during a significant amount of time hence it would be very hard to understand why and how the eGov eID solution should have these important aspects automatically accounted for from the start. I argue that the basic incentives for the private market eID infrastructure is rather unclear and have a hard time seeing it should have a great impact on the eGov eID solution as in general, the challenge of this aspect failing is assessed with: a high probability and low impact.
Appendix 4 – Authorities

This appendix provides a translated summary of the Swedish authorities referred to in the referral process (see Section 5.2.5)

Swedish Internet Infrastructure Foundation (.SE)
National Employment Office (Arbetsförmedlingen)
Swedish Companies Registration Office (Bolagsverket)
Swedish Student Aid (Centrala studiestödsnämnden, CSN)
Commercial banks (Handelsbanken, Swedbank)
Swedish Data Protection Authority (Datainspektionen)
Swedish Courts (Domstolsverket)
Swedish Defence Materiel Administration (Försvarsmaterielverket, FMV)
Agency for Disability Policy Coordination (Myndigheten för handikappolitisk samordning, Handisam)
Board of Agriculture (Jordbruksverket)
County Council of Jämtland (Jämtlands läns landsting)
Administrative Services Agency (Kammarkollegiet)
Competition Authority (Konkurrensverket)
Swedish Mapping, Cadastral and Land Registration Authority (Lantmäteriet)
County Administrative Board of Västra Götaland (Länsstyrelsen i Västra Götalands län)
County Administrative Board of Örebro (Länsstyrelsen i Örebro län)
Migration Agency (Migrationsverket)
Municipality of Norrköping (Norrköpings kommun)
Municipality of Nacka (Nacka kommun)
Swedish Civil Contingencies Agency (Myndigheten för samhällsskydd och beredskap)
Swedish Pensions Agency (Pensionsmyndigheten)
Swedish Post and Telecom Authority (Post- och Telestyrelsen)
National Archives of Sweden (Riksarkivet)
National Police Board (Rikspolisstyrelsen)
Municipality of Sandviken (Sandvikens kommun)
Swedish Tax Agency (Skatteverket, SKV)
Swedish Agency for Economic and Regional Growth (Tillväxtverket)
Swedish Transportation Board (Transportstyrelsen)
Swedish Customs Office (Tullverket)
Swedish Bankers’ Association (Svenska Bankföreningen)
Swedish Association of Local Authorities and Regions (Sveriges Kommuner och Landsting, SKL)

107 Later The Internet Foundation In Sweden (Internetstiftelsen i Sverige, IIS)
108 Later the Swedish Agency for Participation (Myndigheten för delaktighet)