MANAGING THE DEVELOPMENT OF SECURE IDENTIFICATION – INVESTIGATING A NATIONAL E-ID INITIATIVE WITHIN A PUBLIC E-SERVICE CONTEXT

Melin, Ulf, Linköping University, Department of Management and Engineering, Information Systems, SE-581 83 Linköping, Sweden, ulf.melin@liu.se

Axelsson, Karin, Linköping University, Department of Management and Engineering, Information Systems, SE-581 83 Linköping, Sweden, karin.axelsson@liu.se

Söderström, Fredrik, Linköping University, Department of Management and Engineering, Information Systems, SE-581 83 Linköping, Sweden, fredrik.soderstrom@liu.se

Paper accepted to the 21st European Conference on Information Systems, June 5-8, 2013, Utrecht, The Netherlands. To be included in conference proceedings available at: http://aisel.aisnet.org/ecis2013/

Abstract

This paper investigates the management of developing electronic identification (e-ID) within a public e-service context. e-ID is an important key enabler for secure identification, authentication and digital signing via the Internet and a part of e-service design. As users, and citizens, we become reliant on electronic solutions that give us a certain level of utility and trust, and use e-ID solutions to interact with local and central government in an e-service context. The management of e-ID development in a national context is the case in focus for investigation. Such development initiatives, and especially inter-organizational projects, face a number of challenges. Therefore it is a need for a more thorough understanding of e-ID development within a public e-service context. The purpose is to analyse the contemporary management of e-ID development in Sweden from: a) an e-government systems development life-cycle perspective and b) a project challenge and critical success factor perspective. This study concludes that there are significant challenges involved in managing integrated e-ID development. Challenges involve the organization and management of the program and can be traced back to e-government and general project management literature, but based on this study one can question, e.g. governance models, centralization, and a narrow focus on a technical artefact. Important implications from this paper are a call for further contextual studies of e-ID development, putting the user and organizational setting, path dependency, and governance models in focus.

Keywords: e-ID, electronic identification, public e-services, government, e-government, project management.

1 Introduction

Electronic identification (e-ID) is an important prerequisite and key enabler for the secure identification, authentication and digital signing via the Internet and as a part of all aspects of secure e-service design (European Commission, 2010; Halperin and Backhouse, 2008; Price, 2008; Rössler, 2008). As users, and digitized citizens, we become reliant on electronic solutions that give us a certain level of utility and trust, and use e-ID solutions to interact with local and central government (Collings, 2008) in an e-service context. In digitizing Europe for example, e-ID is regarded as an important back-office enabler for launching e-services and transforming government (European Commission, 2010). Launching e-IDs for citizens and businesses is therefore very important for the governments in order to realize e-government policies and to provide better services to citizens, in an efficient, secure and trusted way. Developing and implementing e-services and e-IDs continues to receive much attention in practice. In Europe, for example, individual EU states had issued e-ID solutions to more than 22.5 million citizens already in 2008 (Collings, 2008) and there is more to come in the area of development and distribution of e-IDs (Halperin and Backhouse, 2008). Significant investments are needed in development of e-government in general (Irani et al., 2005; 2007), trying to create new opportunities in the public sector's delivery of e-services which in turn requires identified citizens. Accordingly, the e-ID is of paramount importance for almost all e-government service applications (Rössler, 2008).

Developing, implementing and managing public e-services and secure e-ID solutions are challenging and require coordination and management. The European Commission recognises that common standards in issuing procedures are highly desirable in the field (Collings, 2008). Such procedures include people, processes and technology (ibid.), which stresses the complexities and interwoven character of the e-ID as an artefact in an e-service and in an institutional (or governmental) arrangement. Managing e-ID development can on a general level be governed by an active role of the government, and/or managed by market driven solutions (cf. Grönlund, 2010; Kubicek, 2010).The reported fact that several e-government initiatives face a number of challenges of complexity and risk is another factor that calls for further studies (Irani et al., 2007; Gil-García and Pardo, 2005; Rosacker and Olson, 2008), using e-ID as a contemporary example. The embedded complexity and risk in projects can be considered as one explanation to why reports on project failures are common. An important issue for information systems (IS) project management and e-government, in practice and research, is to understand how we organize initiatives like this and why some initiatives progress to success while others end in failure (e.g. Heeks and Stanforth, 2007; Melin and Axelsson, 2009).

Scholars have started to investigate e-ID, but often from a technical oriented perspective focusing the artefact as such as a part of e.g. an e-government initiative. However, this perspective represents much more than an information technology program; "[…] the technology is only the customer facing front-end of a complex set of organizational structures, policies, and processes that are designed to provide particular services." (Grant and Rose, 2010, p. 29). Therefore, there is a need for more contextual studies focusing on implementation, processes and organizational settings and in accord we suggest a program level analysis of the e-ID development.

In this paper the management of e-ID development in Sweden is studied as an example of a national e-ID program initiative. Learning from the past and from the experiences of different development initiatives is essential for the development of public e-service (Irani et al., 2007). There is also a call for empirical e-ID studies moving away from the technical artefact (Halperin and Backhouse, 2008). The challenges in developing e-government, with e-ID as one part, can be related to factors covering: information and data, organizational and managerial issues, legal and regulatory preconditions, and overall institutional and environmental aspects (Gil-García and Pardo, 2005). One critical barrier that needs to be overcome is the delaying factor of the lack of organizational cooperation (Kubicek and Hagen, 2000) in inter-organizational projects or programs. In general, agencies tend to act too independently – the initiatives tend to be poorly coordinated (Irani et al., 2007). The actions within the initiatives studied in this paper are a response to what is perceived by the Swedish Government as poor coordination of e-ID solutions. The poor coordination in this case have later been acknowledged by the Government forming of the e-identification (e-ID) Board that focuses solely on coordination and sustainable development of the e-ID solution. The main objective in this paper is to contribute to a better understanding of the progress and the success vs. failure in public e-service and e-government development in general, focusing the management of e-ID development in Sweden in particular.

Based on the reported fact (above) that e-government development initiatives, and especially inter-organizational projects, face a number of challenges, this paper argue for a more thorough understanding of e-ID development within a public e-service context. The purpose of this paper is to analyse the contemporary management of e-ID development in Sweden from: a) an e-government systems development life-cycle perspective (Heeks, 2006) and b) a project challenge and critical success factor (CSF) perspective (Gil-García and Pardo, 2005). The e-ID development is regarded as a special case of an IS development (ISD) initiative; performed under a certain set of laws and regulations, and therefore interesting to learn from. The research questions are: 1) What challenges and success factors are represented in a national e-ID development initiative?, 2) How can we judge the success/failure of an e-ID initiative using a life-cycle framework?, and 3) What can we learn from the management of development of e-ID in a public e-service context on a program level?

One way of structuring e-ID development is to investigate the development process in different phases; like any ISD project with generic phases like analysis, design, construction, and implementation (e.g. Avison and Fitzgerald, 2003; Melin and Axelsson, 2009; Heeks, 2006). According to Tsai et al. (2009) government agencies often use traditional ISD life cycles with generic phases. In the analysis below, inspired by Melin and Axelsson (2009), five generic stages are used to structure, assess and analyse the degree of success/failure in the e-ID development case.

After this introduction, the paper is organized in the following way: in Section Two related research and theories on managing e-government and e-ID development are addressed; this section is followed by the research design and case study introduction in Section Three. The paper continues with analysis and findings from a life-cycle perspective together with challenge and CSF's in Section Four; and finally, the paper is concluded in Section Five, also with suggestions for further research.

2 Related Research

Within this section identity and identification are briefly defined and an outlook of previous e-ID studies is made, followed by the management of e-ID from a program and a life-cycle perspective.

2.1 e-ID in a Public e-Service Context

e-ID builds on *identity* as a central element. On a general level identity can be viewed as a "[…] dynamic collection of all attributes related to a specific entity, normally a citizen but the concept can be extended to include an enterprise, or object. […] an identity is what allows entities to be distinguishable." (Collings, 2008, p. 62). This makes identity a critical component in several transactions (social, economic and administrative). *Identification* can be defined as "the process of using claimed or observed attributes of an entity to deduce who the entity is." (Kubicek, 2010, p. 10). The field of identification and identity contains technical as well as social aspects of organizational and personal identity (Lyon, 2009; Söderström and Melin, 2012). There are studies focusing on identification (Seltsikas and O'Keefe, 2010; Whitley and Hosein, 2008), and on organizational and personal identity (e.g. Kotlarsky and Oshri, 2005). Studies of identity in the IS field focus e.g. on identity management (Barnard-Wills and Ashenden, 2010; Kubicek, 2010; Kubicek and Noack, 2010b) and policy engagement processes (Whitley and Hosein, 2007). Some studies have focused on the concept of national e-IDs and identity cards. In Denmark for example, the development of the Danish e-ID has been studied by Hoff and Hoff (2010). They describe an, in many ways, troublesome way of developing a national e-ID, despite a political attention and a high degree of e-readiness. The case of the Danish e-ID is described as a paradox, and the main problems of implementation are related to privacy concerns, a lack of inter-governmental coordination, and a lack of private-public sector cooperation (ibid.). Another Scandinavian e-ID initiative (Rissanen, 2010), focuses on the introduction and diffusion of the Finnish Electronic Identity (FINE-ID) card. Grönlund (2010) focuses on the Swedish e-ID, where the market approach is further investigated. Grönlund describes the Swedish e-ID, before the development focused in this paper (e.g. the creation of the e-ID board and a more centralized approach), as a fairly complex solution based on a market approach with no central governance, but with a good service supply and use (ibid.). Given the focus of these studies of national e-IDs, we identify a need to investigate the Swedish e-ID further.

Kubicek and Noack (2010a, p. 237) describe the timeline and the rollout phases of e-ID projects (Figure 1) and reflect upon the choices of different solutions for e-IDs and digital signatures. A high degree of path dependency is identified e.g. in Denmark and Sweden (ibid., p. 240) based on the fact that these countries are not following the European standards of hardware-based solutions for IDs and digital signatures. This is one aspect that describes the challenges related to the management of national e-ID development and the need to have a contextual perspective when investigating e-ID.

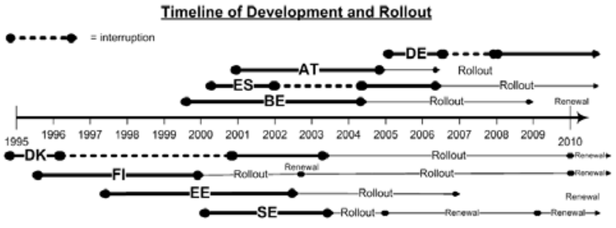

Fig. 1 Timeline of development and rollout of eIDs in eight countries

Figure 1 Timeline of development and rollouts of e-IDs (Kubicek and Noack, 2010a, p. 237)

2.2 Managing e-ID Development

Rose and Grant (2010) report that the implications of e-government growth and evolution are not obvious. There are several unintended consequences and unfulfilled expectations. This calls for further studies of the management of such initiatives. The sections below describe theoretical points of departure for the management of e-ID development.

2.2.1 Managing e-ID Development – A Life-cycle Perspective

Viewing development of e-government in different life-cycle phases is common. Heeks (2006) describes that an e-government development project typically consists of five stages; (1) project assessment, (2) analysis of current reality, (3) design of the new system, (4) system construction, and (5) implementation and beyond. The development model for e-government suggested by Heeks (2006), and applied by e.g. Melin and Axelsson (2009), has several similarities with traditional systems development life cycles or so called waterfall models (e.g. Avison and Fitzgerald, 2003; Tsai et al., 2009). The development of public e-services, including e-IDs, takes place in a certain context, but the tasks performed in each stage seem to be more or less the same. As mentioned above these phases will be used to structure the analysis (Section 4.1) in this paper. Project assessment (1) in the development model, described by Heeks (2006), is the identification of possible e-government projects. In this phase, the outline of basic project parameters is completed, together with the assessment of whether or not to proceed with the project. E-government projects are typically oriented towards pragmatic problem solving or opportunity seeking (Heeks, 2006, p. 162). An opportunity can arise from different sources (internal or external). Analysis of current reality (2) includes the creation of descriptions of information, technology, processes, objectives and values, staffing and skills, management systems and structures, and other resources such as money and time. This stage consists of a mixture of hard and soft techniques such as an IS audit, an IS analysis, a problem analysis, a context analysis, etc., in order to build an overall map. A SWOT analysis can be completed at this stage (ibid.). The design stage (3) consists of setting objectives related to dimensions (objectives) of the new system (including hardware and software). Organizational processes are also necessary to take into account from a design perspective. System construction (4) consists of the process and activities in acquiring new IT, undertaking detailed design of the new e-government system, building it, testing it, and documenting it (ibid.). The last stage, implementation and beyond, (5) is represented by the planning of implementation processes (training users, data conversion, systems maintenance activities, introducing the new system, monitoring and evaluating performance and context) (ibid.). In accord, diffusion and use of the system is not a part of the scope of this paper.

2.2.2 Managing e-ID Development – A Challenge and CSF Perspective

There are several reported challenges when managing e-government initiatives. Reasons for failure are multifaceted (Sarantis et al., 2011), but some common reasons are: lack of internal ownership, a weak strategy and/or vision, poor project management (including management of technology), unsuitable technological infrastructure, and challenges related to data interchange. Interestingly, over-reliance on IT as a main driver for e-government development and inadequate administrative reform/process change are patterns also mentioned (ibid.). Kubicek and Hagen (2000) present six key areas of barriers to be overcome for fewer delays, failures and obstacles in e-government development. The first key area is the lack of organizational cooperation, the second key area is the deficiency of legal regulations, and the third key area is the necessary area of pre-conditions in regard to technology and, fourth, in regard to human factors. The last barriers are the lack of appropriate funding and political support. Signs of project failure in general are reported by e.g. Reel (1999). Those signs can be linked to the e-government patterns above. Examples are: project managers do not understand users’ needs, the project scope is ill-defined, project changes are managed poorly, the chosen IT changes, business needs change, deadlines are unrealistic, users are resistant, sponsorship is lost, the project lacks people with suitable skills, and managers ignore best practice and previous lessons learned (ibid.).

Going back to e-government in particular, Gil-García and Pardo (2005) propose five categories of *challenges* for e-government initiatives. These categories cover the CSF above well and will be used to structure the analysis in Section 4.2. The categories are: (1) information and data, (2) IT, (3) organizational and managerial, (4) legal and regulatory, and (5) institutional and environmental. Adapted from Gil-García and Pardo (2005, p. 191-192), using Melin and Axelsson (2009) as a point of departure, and including a source covering software development risks to project effectiveness (Jiang and Klein, 2000), the categories can be summarized as follows: Information and data (1) covers the capture, management, use, dissemination, and sharing of information (ibid.). There are also aspects of data quality and data accuracy in this category, important in e-government initiatives. In the IT category (2) usability and security issues, technological incompatibility, technological complexity, technical skills and experience, and technological innovation are present. Organizational and managerial challenges (3) are considered to be the main challenges to ISD initiatives. The size (scope) of project, strategic alignment (IT and organization) and the diversity of users and organizations involved are important factors in this category. Dawes and Pardo (2002) also address the existence of multiple, partially conflicting goals in the public sector, which is critical for e-government initiatives. Legal and regulatory changes (4) represent the formal rules that government organizations operate upon. Restrictive laws and regulations must be taken into account when developing e-government in general and e-ID in particular. The institutional and environmental challenges (5) are the institutional framework in which governments operate (ibid.) and include the policy environment. Norms and actions are also examples of the policy environment which is important for the success or failure of e-government development initiatives (Gil-García and Pardo, 2005). Success in e-government is not only a question of choosing the appropriate technology; it includes managing capabilities in organizations, and regulatory and environmental conditions (ibid.). Looking at the other side of the coin, the literature in the area of e-government and ISD projects reports on several sets of *success* *factors*. Gil-García and Pardo (2005) and Ho and Pardo (2004), have carried out literature reviews of key success e-government strategies. Examples of CSF's are top management commitment, project linkage to business, technical alignment, knowledgeable personnel, and user involvement.

Challenges and success in managing e-ID development can also be linked to how we frame the development initiatives. Rose and Grant (2010) propose a conceptual framework supporting the management (planning and implementation) of *e-government programs* (a collection of projects/initiatives). The framework, built around traditional marketing mix components, takes a point of departure in customer (citizen) focus and a relationship management perspective. Aspects like price, product, place, and promotion (4Ps) are addressed within a CRM approach (e.g. Schierholz et al., 2007). Each of the aspects in the conceptual framework includes critical issues derived from a literature review in the field of planning and implementation of e-government initiatives (ibid.). Rose and Grant (2010) emphasize that program management significantly can contribute to an overall success of a program. They list critical program management issues and relate them to e-government. A strong and active leadership is at the top of the list followed by several aspects linked to the broad spectrum of e-government programs being far more than technology implementation programs. Aspects like change management, policy, processes, structures, as well as laws and regulations are also identified as important (Gant and Gant, 2002). A rather centralized approach is proposed to ensure that a program is implemented in a consistent way throughout various agencies (Rose and Grant, 2010; Ke and Wei, 2004). Consistency should also be based on a robust strategy (ibid.), including political and bureaucratic support and funding. Due to the numerous internal and external stakeholder groups with different agendas the issue of defining the program's goals, scope and outcome is cumbersome. Another CSF is the coordination of e-government programs on different levels (federal, provincial/state, and local level [Jaeger and Thompson, 2003; Rose and Grant, 2010]). To ensure privacy and security is also considered as a critical issue in the literature study (above).

3 Research Approach and Case Study Introduction

This is a qualitative, longitudinal, case study (Walsham, 1995). This paper reports an analysis of the first two years in a larger project focusing e-ID in a public e-service setting, that started in January 2011 and ends in 2014. The overall area of interest is to study policies, implementation and practice of e-ID in Sweden, including the key actors, important decisions and events (cf. Langley, 1999), challenges and limitations related to the governance, development and use of e-ID. The analysis below is structured based on the different stages in an e-government system life-cycle described by Heeks (2006), and on challenges to e-government identified by Gil-García and Pardo (2005), introduced above. These theories have been used as guides for structuring and analysing (Walsham, 1995) empirical data from the national e-ID program studied and the documents describing the initiative. The aim of explicitly using the concepts from Heeks (2006) and Gil-García and Pardo (2005) as lenses is also to contribute to that body of knowledge. At the same time the analysis tries to discover new concepts, areas and issues in the empirical material in an explorative matter as a part of a reflexive (Van de Ven, 2007) research approach. Important empirical sources have been 11 interviews with different actors deeply involved in the e-ID process, different kind of forums for presentations and discussions such as hearings arranged by authorities, meetings with the e-ID Board, practitioners' networks events and documents. The respondents (described above) were identified by *snowball sampling* (Patton, 1980) and represent e-service providers such as central government agencies, local authorities and health care regions as well as the provider of the e-ID solution itself.

The emergence of the present national public e-ID policy in Sweden can be traced back to the end of the 1990s, when the government started to investigate the future use of public e-services. The need for secure and coordinated solutions for identification was pinpointed in this work. Internet banking (e-banking) was already well established by then as a channel for delivering banking services and had an installed base of solutions for identification. In 2000/2001, The Swedish Tax Agency got the commission to investigate a national e-ID solution for the public sector, resulting in the first set of frame agreements with the actors delivering secure e-ID to the banking sector. Frame agreements that agencies need to follow during a certain period of time. This was the starting point of the public e-ID of today (Grönlund, 2010; Söderström and Melin, 2012). The market driven e-ID delivery model was chosen for several reasons; 1) to support competition among providers, 2) to promote e-IDs as an important driver for further e-service development, and 3) to avoid investments in e-ID (Grönlund, 2010). Grönlund (ibid., p. 196) describes the market driven model as advanced: "Not only the e-IDs themselves but also the control structure, the certification system, was left to the providers." The Insurance Claim Agency and The Swedish Board for Study Support also adopted e-ID solutions for their high volume secure public e-services. In 2012 the banking sector had approximately 4.2 million identified customers/users. Approximately 80 % of the e-ID use in Sweden is currently related to e-banking services (provided by the BankID consortia) and 20 % is related to public e-services.

Several governmental actors have been active in developing e-ID. The Agency for Administrative Development managed the development of the secure electronic exchange of information and safe handling of electronic documents between 2006 and 2008. In its final report (VERVA R 2008:12a, b), the agency pinpointed the need for: 1) a distinct definition of the Swedish e-ID and 2) a central coordinating body. As a result of this and other actions the e-Government Delegation (e-Gov Delegation) was created in 2009. Their role was to strengthen national inter-organizational development of e-government including e-ID. As a part of the coordination, a technical infrastructure based on a solution where the government should act as a central node towards the issuers (e.g. the banks) was suggested. According to the e-Gov Delegation, this solution should serve as a basis for the technical interoperability for electronic identification and facilitate further diffusion and development in the area (SOU 2009:86; 2010:62). Later on the commission was appointed to investigate the next generation of inter-organizational e-ID solution (SOU 2010:104). This initiative was driven by the fact that the current procurement model was outdated, without any option of renewal. The investigation resulted in a report, dominated by a technical oriented blueprint. In January 2011 another authority named The Swedish e-ID Board was created, with a mandate to centrally manage and develop sustainable e-ID solutions. Grönlund (2010) compares the historical Swedish e-ID development with other EU countries, and characterizes the Swedish approach as a fairly complex, and market driven, solution, with multiple contracted private e-ID providers, no centralized e-ID identity management system, and several e-ID card solutions in parallel. One has also to keep in mind that Sweden has a governance model with strong, rather independent, public agencies and relatively weak Ministries; at least historically, and policies are more negotiated than implemented top down (ibid). The National Audit Office in Sweden regards the political leadership as weak in this sense. As reported above, the Cabinet are more in control, however, since 2009 (Grönlund, 2010; SNAO, 2009). The proposal, above, by the e-Gov Delegation is a step towards a centralized e-ID infrastructure focused in this paper. This includes aspects such as standardization, usability, privacy, and costs focus (ibid.).

4 Analysis and Findings

The analysis below is structured according to the life-cycle perspective on development followed by a challenge and CSF perspective on program management introduced above.

4.1 Managing e-ID Development – A Life-cycle Perspective

A life-cycle perspective is introduced in section 2.2.1, above, and the different stages suggested by Heeks (2006) are utilized below to assess the e-ID development initiative.

Project assessment – E-government projects are typically oriented towards pragmatic problem solving (Heeks, 2006); the studied e-ID initiative is no exception. The current procurement model (and the frame agreement) was outdated, so an explicit need for a new e-ID solution was present. Opportunity seeking (ibid.) is another orientation. From a political perspective the e-ID initiative was a way of trying to stimulate competition among e-ID providers. The initiative had scarce resources (deadline was postponed) which as described above also influenced the next step below.

Analysis of current reality – The analysis of the current reality in the e-ID initiative was extremely forced and temporarily staffed. The initial intention was to anchor the plan in different stakeholders' views, but the report describing the current reality and the design has, instead, been developed in a more isolated way. The report as such contained a blueprint of the next generation technical solution of the e-ID, based on a market driven approach. The contextual analysis (e.g. to different governmental levels), an important part of this stage (Heeks, 2006), were put in the background and the technology in the foreground. A SWOT analysis that can, for example, be completed at this stage (ibid.), was first operationalized in a referral process (below).

Design of the new system – important activities in this stage is the setting of objectives related to dimensions of the new system (including hardware and software). Organizational processes are also necessary to take into account from a design perspective. No IT artefact design took place at this stage; instead more conceptual design of the system was made. The model proposed in the report was based in multiple contracted private e-ID providers and a federated e-ID solution with the e-ID Board acting as a central coordinating contractor versus the e-ID suppliers. The Board also delivers and maintain a central technical base structure (an Identity Federation) for the public sector. Several e-ID solutions were suggested in parallel. Important design issues (e.g. digital signing) were not solved in detail at this stage. To collect feedback on the future e-ID report, the managing ministry initiated a referral process in the spring of 2011. Critique from actors in the public and the private sector were frequent.

System construction – this stage consists of the process and activities in acquiring any new IT, undertaking detailed design of the new e-government system, building it, testing it, and documenting it (ibid.; Melin and Axelsson, 2009). In the present case no IT artefact is constructed; the conceptual infrastructure is instead in focus at this stage. The main purpose with the infrastructure for the national e-ID is to conceptually design secure e-ID solutions, to provide an infrastructure for identification, and to provide services for signing. Time consuming building of trust was made during dialogue.

Implementation and beyond – the last stage, implementation and beyond, includes the planning of implementation processes introducing the new e-government system; monitoring and evaluating performance and context (Heeks, 2006). In the focused plan there are a number of activities such as changes in the constitution, preparation of agreements, technological development, and the establishment of frameworks for security and trust related to this stage. A transition plan can also be seen as a critical part of the work to ensure a smooth transition from the current to future model. The latter aspect is an important issue for implementation and beyond (future use; i.e. how the suggested federated national e-ID solution will affect the current one) together with the intention that the model for e-ID should be sustainable and flexible (SOU 2010:104); which is a challenge in itself.

4.2 Managing e-ID Development – A Challenge and CSF Perspective

This part of the analysis is based on challenges to e-government identified by Gil-García and Pardo (2005), introduced above (Section 2.2.2). The findings regarding these challenges and success factors are used to assess the e-ID initiative and summarised below. Some of the empirical examples have also been used when discussing the life-cycle perspective above. Below, input from the theoretical section looking at the e-ID initiative from a program perspective (Section 2.2.2) is integrated. The reasons for failure in this area are multifaceted (Kubicek and Hagen, 2000; Sarantis et al., 2011). Several challenges are present also in the e-ID development program. Related to the e-ID initiative ownership is a key issue within the Swedish model for governance (Section 2.2.2). The untested, conceptual, infrastructure for e-ID is also a challenge from a program management perspective.

Information and data – this category covers the capture, management, use, dissemination, and sharing of information. There are also aspects of data quality and data accuracy in this category (Gil-García and Pardo, 2005). The federative solution in the suggested e-ID infrastructure demands data interchange between different actors (e.g. identity providers, e-service providers, attribute issuers, registrar). Data interchange is complex and a multi actor arrangement is also complex (cf. Jaeger and Thompson, 2003; Rose and Grant, 2010) from an information and data management perspective.

IT – the technological conditions for the program are based on different existing e-ID artefacts on the market (installed base; widespread solutions from e.g. Swedish banks with many users). There is also a situation where the infrastructure and application are conceptually designed in parallel – resulting in an untested, conceptual, e-ID infrastructure. One must also consider that there is no detailed IT artefact designed at this stage – this is also a possible risk (e.g. unprecedented technological constraints) and multiple standards coexist. Several issues, considered as challenges by Gil-García and Pardo (2005), are thus present; technological incompatibility and complexity and, to some extent, innovation.

Organizational and managerial – the role of the e-Gov Delegation is perceived as unclear. This is a major challenge based on the need for strong and active program leadership that is placed at the top of the list of CSF's by Rose and Grant (2010). The size and scope of the e-ID development program is also perceived as unclear, so is the ownership of the program (Sarantis et al., 2011). Taking into account the time limit and the time pressure described above, this must be perceived as a high risk program. This interpretation is also in line with e.g. Kubicek and Hagen's (2000) reasoning. Due to the numerous internal and external stakeholder groups, with different agendas, the issue of defining the program goals, scope and outcome is cumbersome. Dawes and Pardo (2002) also address the existence of multiple, and partially conflicting goals in the public sector, which is critical for e-government initiatives. Based on the analysis and findings in the present case above, e-ID development is no exception. Adding a complex infrastructure with relationships between technology, law and business model makes it even harder to communicate with different stakeholder groups. The latter aspect is highlighted in literature reviews as a major issue to succeed in (Rose and Grant, 2010; Schierholz, et al., 2007). If we look at the total scope of the program and the embedded projects, IT design issues are placed in the foreground while organizational and user/using issues are put in the background.

Rose and Grant (2010) and Ke and Wei (2004) propose a rather centralized approach to ensure that a program is implemented in a consistent way throughout various agencies. Consistency should also be based on a robust strategy according to Rose and Grant (2010), consisting of political and bureaucratic support and sufficient funding. As mentioned earlier the national context and history for the e-ID has to be considered here. Sweden has a governance model with strong, rather independent, public agencies and relatively weak Ministries (Grönlund, 2010; SNAO, 2009). However, as reported above, the Cabinet is more in control, since 2009 and the creation of the e-Gov Delegation is a step towards a more centralized development of a national e-ID infrastructure. This includes standardization, usability, privacy, and costs focus. When the Swedish e-ID Board was created in 2011, with a mandate to centrally manage and develop sustainable e-ID solutions, this was a step towards a more centralized approach, in line with consistency proposed by Rose and Grant (2010) and Ke and Wei (2004).

Legal and regulatory – this category represents the formal rules that government organizations operate upon. Restrictive laws and regulations must be taken into account when developing e-government in general (Gil-García and Pardo, 2005) and secure e-ID in particular. If we take a look at the studied e-ID initiative changes in law and regulation are needed to implement and use the suggested e-ID infrastructure in practice. A public sector procurement model needs to be more flexible and allow parallel agreements with several suppliers (multiple sourcing); described as a system of choice.

Institutional and environmental – challenges in the institutional framework in which governments operate (Gil-García and Pardo, 2005) and policy environment is included here. Norms and actions are also examples of the policy environment which is important for the success or failure of e-government development initiatives. As reported above, the Cabinet are more in control now. This is obvious a step towards a more centralized and consistent e-ID infrastructure (Rose and Grant; 2010; Ke and Wei, 2004) and a changed set of norms compared with the previous more decentralized national approach. This is challenging the norms and power structures. Another aspect taking the environmental issues into account is the business model of the Swedish e-ID's intention to create a model that works effectively with benefits and incentives for different operators. It is also highlighted that the model should be evolutionary and adaptable to new conditions (SOU 2010:104). However, a balance between robustness and flexibility is hard to achieve in practice implementing e-ID solutions.

If we analyse the e-ID initiative from a program perspective (Rose and Grant, 2010) we can see that several aspects highlighted by Gil-García and Pardo (2005) above is overlapping. The contribution of management to the overall success of a program is one aspect; a strong and active leadership, change management, a contextual view of technology, laws and regulations are other important aspects.

5 Conclusions and Further Research

The purpose of this paper has been to present a program level analysis of the contemporary management of e-ID development in Sweden from: a) an e-government systems development life-cycle perspective, and b) a project challenge and CSF perspective including a program perspective. As reported in Section 4 several challenges are present. Conclusions are that the initiative is oriented towards pragmatic problem solving (an outdated procurement model that needs to be replaced) and an explicit demand from public agencies (secure e-ID solutions for e-services). However, the problem solving and implementation process is forced in time and scarce available resources. The fact that the program scope is unclear and that the relation to the existing and dominating e-ID solution (BankID) is unclear and hard to coordinate from a governmental perspective puts further pressure on the national e-ID program. Above, the national e-ID initiative is analysed as a program and from a challenge and CSF perspective. Important conclusions based on this analysis is that there is a significant challenge in the designing of the infrastructure for e-ID (conceptually and applying it in parallel) and at the same time taking existing e-ID solutions into account. Even if there is a more robust strategy (cf. Rose and Grant, 2010) as a baseline now, there are significant challenges related to organization and management of the program (scope, ownership, time, resources, governance structure, and design issues on a conceptual level). The involved actors are also heterogeneous and with different sets of expectations. The critique against the program putting the technological artefact in foreground, and the user setting (e.g. citizens and professional users) together with the link to e-services provided in the background, are other major challenges for the program.

The e-ID development program in Sweden is facing some of the challenges reported in Denmark and Finland (Hoff and Hoff, 2010; Rissanen, 2010) concerning e.g. privacy concerns, a lack of inter-governmental and public-private coordination. This is important to learn from for practice and research. Despite the more centralized approach, within the Swedish model of governance nowadays and the creation of the e-Gov Delegation and the e-ID Board, inter-governmental coordination is still a major challenge. This is also an example of path dependency (Kubicek and Noack, 2010a). Therefore we conclude that the centralized approach suggested by Rose and Grant (2010) can be questioned; at least it is no silver bullet in managing successful e-ID development. The relation to the widespread existing solution for e-banking (issued by the banks), the installed base, is also a challenge. Coordinating an area that is partially market driven is highlighted by the e-ID Board as a major challenge. This is an issue challenging the CSF literature within e-government (Rose and Grant, 2010; Ke and Wei, 2004). We have also identified that the management of e-ID development shares the challenges and possibilities in relation to e-government management in general (cf. Irani et al, 2007).

As an important implication of this research we would like to broaden the scope based on the analysis above; in digitizing Europe for example, e-ID is regarded as an important back-office enabler for launching e-services and transforming government (European Commission, 2010). Yes, e-ID can be considered as a back-office enabler for launching e-services, but it also needs to be managed as an *integral part of e-service development* because it is intertwined with the *use of e-services* from a user perspective. Thus, e-ID is more than a back-office enabler – it is an integrated part of successful e-service management and use. This conclusion calls for future studies moving away from only focusing the technical artefact (Halperin and Backhouse, 2008), and instead opening up the setting and context for the e-ID artefact in order to deal with implementation issues, governance structures, multifaceted user and organizational settings and challenges, and life-cycle related issues described above. The present study is an attempt to learn from e-ID development initiatives. We regard that this is essential also for future e-government development (cf. Irani et al., 2007) in general. Further research can address the paradoxical situation that e-ID can contribute to security and at the same time may become a threat to privacy (Kubicek, 2010; Halperin and Backhouse 2008); this issue is not addressed in this paper but an important aspect in future research. We would also like to address the need for future contextual studies of e-ID in order to generate more knowledge on the issue of e.g. national differences, governance structures, IT and e-ID user maturity and diffusion.

References

Avison, D.E., Fitzgerald, G. (2003). Information Systems Development: Methodologies, Techniques and Tools, 3rd Edition, McGraw-Hill, London.

Barnard-Wills, D., Ashenden, D. (2010). Public sector engagement with online identity management, Identity in the Information Society, 3(3), 657-674.

Collings, T. (2008). Some thoughts on the underlying logic and process underpinning Electronic Identity (e-ID), Information Security Technical Report, 13, 61-70.

European Commission (2010). Digitizing Public Services in Europe: Putting ambition into action, 9th Benchmark Measurement, Dec 2010, Directorate General for Information Society and Media.

Gant, J. P., Gant, D. B. (2002). Web portal functionality and state government eservice, Proceedings of the 35th Annual Hawaii International Conference on System Sciences, IEEE, 1627-1636.

Gil-García, J.R., Pardo, T.A. (2005). E-government success factors: Mapping practical tools to theoretical foundations, Government Information Quarterly, 22(2), 187-216.

Grönlund, Å. (2010). Electronic identity management in Sweden: governance of a market approach, Identity in the Information Society, 3(1), 195-211.

Halperin, R., Backhouse, J. (2008). A roadmap for research on identity in the information society, Identity in the Information Society, 1(1), 71-87.

Heeks, R. (2006). Implementing and Managing eGovernment – An international text, SAGE, London.

Heeks, R., Stanforth, C. (2007). Understanding e-Government project trajectories from an actor-network perspective, European Journal of Information Systems, 16(2), 165-177.

Ho, J., Pardo, T.A. (2004). Toward the Success of eGovernment Initiatives: Mapping Known Success Factors to the Design of Practical Tools, In: Proceedings of the 37th Hawaii International Conference on Systems Sciences, IEEE, 1-6.

Hoff, J.V., Hoff, F.V. (2010): The Danish e-ID case: twenty years of delay, Identity in the Information Society, 3(1), 155-174.

Irani, Z., Love, P.E.D., Jones, S., Themistocleous, M. (2005). Evaluating e-Government: learning from the experiences of two UK local authorities, Information Systems Journal, 15(1), 61-82.

Irani, Z., Love, P.E.D., Montazemi, A.R. (2007). e-Government: past, present and future, European Journal of Information Systems, 16(2), 103-105.

Jaeger, P.T., Thompson, K.M. (2003). E-Government around the world: Lessons, challenges, and future directions, Government Information Quarterly, 20(4), 389-394.

Jiang, J., Klein, G. (2000). Software development risks to project effectiveness, Journal of Systems and Software, 52(1), 3-10.

Ke, W. Wei, K.K. (2004). Successful E-Government in Singapore, Communications of the ACM, 47(6), 95-99.

Kotlarsky, J., Oshri, I. (2005). Social ties, knowledge sharing and successful collaboration in globally distributed system development projects, European Journal of Information Systems, 14(1), 37-48.

Kubicek, H., Hagen, M. (2000). One Stop Government in Europe: An Overview. In: Hagen, M., Kubicek, H. (Eds. 2000). One Stop Government in Europe, University of Bremen, 1- 36.

Kubicek, H. (2010). Introduction: conceptual framework and research design for a comparative analysis of national e-ID Management Systems in selected European countries”, Identity in the Information Society, 3(1), 5-26.

Kubicek, H., Noack, T. (2010a). Different countries-different paths extended comparison of the introduction of e-IDs in 11 European countries, Identity in the Information Society, 3(1), 235-245.

Kubicek, H., Noack, T. (2010b). The path dependency of national electronic identities - A comparison of innovation processes in four European countries, Identity in the Information Society, 3(1), 111-153.

Langley, A. (1999). Strategies for Theorizing from Process Data, Academy of Management Review, 24(4), 691-710.

Lyon, D. (2009). Identifying citizens: ID cards as surveillance, Polity Press, Cambridge, UK.

Melin, U., Axelsson, K. (2009). Managing e-service Development – Comparing two e-Government Case Studies, Transforming Government - People, Process and Policy, 3(3), 248-270.

Modinis Study (2005) On Identity Management in eGovernment. Common terminological framework for interoperable electronic identity management, E.C./University of Leuven.

Patton, M.Q. (1980). Qualitative evaluation methods, Sage Publications, Beverly Hills.

Price, G. (2008). The benefits and drawbacks of using electronic identities, Information Security Technical Report, 13, 95-103.

Rissanen, T. (2010). Electronic identity in Finland: ID cards vs. bank IDs", Identity in the Information Society, 3(1), 175-194.

Rosacker, K.M., Olson, D.L. (2008). Public sector information system critical success factors, Transforming Government: People, Process and Policy, 2(1), 60-70.

Rose, W.R., Grant, G.G. (2010). Critical issues pertaining to the planning and implementation of E-Government initiatives, Government Information Quarterly, 27(1), 26-33.

Rössler, T. (2008). Giving an interoperable e-ID solution: Using foreign e-IDs in Austrian e-Government - Interoperability in electronic identity management, Computer Law & Security Report, 24(5), 447-453.

SNAO (2009). E-legitimation – en underutnyttjad resurs, Riksrevisionen (The Swedish National Audit Office) Rapport RiR 2009:19, November 23, 2009 [In Swedish].

Sarantis, D., Charalabidis, Y., Askounis, D. (2011). A goal-driven management framework for electronic government transformation projects implementation, Government Information Quarterly, 28(1), 117-128.

Seltsikas, P., O'Keefe, R.M. (2010). Expectations and outcomes in electronic identity management: The role of trust and public value, European Journal of Information Systems, 19(1), 93-103.

Schierholz, R., Kolbe, L. M., Brenner, W. (2007). Mobilizing customer relationship management: A journey from strategy to system design, Business Process Management Journal, 13(6), 830-852.

SOU 2009:86 (2009). Strategi för myndigheternas arbete med e-förvaltning, Betänkande, E-delegationen, Stockholm [In Swedish].

SOU 2010:62 (2010). Så enkelt som möjligt för så många som möjligt - Under konstruktion - framtidens e-förvaltning, Betänkande, SOU 2010:62, E-delegationen, Stockholm. [In Swedish]

SOU 2010:104 (2010). E-legitimationsnämnden och Svensk e-legitimation, Betänkande av Utredningen om bildandet av en e-legitimationsnämnd, Stockholm. [In Swedish]

Söderström, F., Melin, U. (2012). The Emergence of a National e-ID Solution – an Actor-Network Perspective, Presented at the 35th Information Systems Research Seminar in Scandinavia, Sigtuna.

Van de Ven, A.H. (2007). Engaged scholarship – A guide for organizational and social research, Oxford University Press.

VERVA R 2008:12a (2008). Slutrapport om säkert elektroniskt informationsutbyte och säker hantering av elektroniska handlingar, Verket för förvaltningsutveckling, Stockholm. [In Swedish]

VERVA R 2008:12b (2008). Elektronisk identifiering och underskrift i Sverige, Särtryck ur 2008:12, Verket för förvaltningsutveckling, Stockholm. [In Swedish]

Walsham, G. (1995). Interpretative case in IS research: nature and method, European Journal of Information Systems, 4(2), 74-81.

Whitley, E.A., Hosein, I. R. (2007). Policy Engagement as Rigourous and Relevant Information Systems Research: The Case of the LSE Identity Project, In Proceedings of the 15th European Conference on Information Systems (Österle, H., Schelp, J., Winter, R. Eds.), 1301-1312.