Organizing safe on-line interaction and trust in governmental services.
A case study of identification channels for public e-services in schools.

Mariana S. Gustafsson*, Elin Wihlborg**

* PhD-candidate, Department of Management and Engineering, Linkoping University, Sweden.
mariana.s.gustafsson@liu.se

** Professor, Department of Management and Engineering, Linkoping University, Sweden.
elin.wihlborg@liu.se

Abstract: There is an increased use of public e-services integrating citizens into public administration through electronic interfaces. The relation among parents and public schools is a daily and important relation that has to be trustworthy. On-line interaction among public organizations and citizens can be seen as e-government, indeed embedded into daily practices. A safe entry into such systems is essential for security and trust in the e-governmental systems and schools as well as public services in general. This paper addresses how electronic identification has been used for access to public e-services in schools in a Swedish municipality. The aim of the paper is to present a case study on how electronic identification is used and implemented in ICT platforms in schools. The analysis focuses on information security, organization and potential development of the platforms. The main finding in the case study is that there was an un-organized presentation of information in the system; both general and personal information had to be accessed with the same level of security (identification systems). The organization of identification and access to public e-services seemed highly dependent of the organizational structure of the public schools. The more general implication is that safe and well organized identification systems that are considered as trustworthy and useful among citizens are essential for increased use of the services and legitimate public e-services in general.

Keywords: electronic identification, e-government in public schools, case-study, eID

Acknowledgement: This project is part of the research project FUSe (Future secure electronic identification - emergence and use of e-identification), hosted by Linköping University, managed by Prof. Karin Axelsson and financed by The Swedish Civil Contingencies Agency. We also express thankfulness to our informants - school principals, teachers and pupils from the five participating schools, as well as the officials at Linköping municipality, who made this study possible.
1. Introduction

Identification is a crucial part in all relations and it becomes even more important as societies develop into more complex, integrated and globalized networked relations (Giddens, 1990). This also relates to the risks in the settings of the digitalized society (Castells, 1996 and 2011 Beck, 1992). In citizen-government relations the identification confirms citizenship and thereby it gives access to welfare and social services. This is at the core of e-government (Heeks & Bailur, 2007). In an increasingly digital society where e-government develops and becomes more integrated into citizens’ daily practices and activity patterns, needs arise for safe and trustworthy arrangements of identification. Electronic identification (eID) confirms and verifies the identity of a person and is related to the citizenship. The electronic identification thus plays a fundamental role when relations among citizens and the government are transferred into e-governmental relations (SOU 2009:86 and SOU 2010:62). Electronic identification is essential for providing public e-services that are individual and related to the individuals’ personal information (Taylor & Lips, 2010, Söderström, 2011, Axelsson & Melin, 2012).

Identification systems are designed and managed by each state and its government. The Swedish system of electronic identification was initiated in the early the 1990s by the Swedish Tax Agency (STA). They saw a potential for improved efficiency in creating links between systems containing tax information and civil registration data (Soderstrom & Melin, 2012). A common practice is that eID is downloaded as a security-software on the user’s computer and/or available on-line. Identification devices are used to confirm the identification by a unique signature when accessing the e-service (Grönlund, 2010).

In mature welfare states, as Sweden, where citizens express high trust towards the state (Rothstein, 2009) there is also a high level of interaction among the state and its citizens. There is also a high and clear policy ambition to reach an almost complete coverage for public e-services (Grönlund, 2010). The government aims to develop a modern and efficient public administration at all levels. Improved e-government is highlighted in several policy documents, among other in the National Digital Agenda and the issue is made explicit in the state budget. Sweden also stands out for its high access to computers and internet access; about 97% of the households have access to Internet (Eurostat 2011).

Education is compulsory and free in Sweden. The Government regulates and funds all education and schools are managed by the municipalities. In line with new public management models, private companies and foundations can also run schools. These schools are called as ‘free schools’ and provide education at all levels and follow the same laws and regulations as the public schools. The municipality has the main responsibility to allocate pupils and resources also to the free schools. Hereby, the schools make up an essential part of the local government service to citizens. There is a long history of use of ICT in education in Sweden and with the new Education Act (2011) that demands increased and systematic reporting of the pupil’s school progression, use of ICT in education administration will probably increase. In this context systems for safe log-in and identification become essential and have developed as a commonly used local citizen - public authorities’ interaction. Here essential information, including sensitive information is transferred among several actor groups. The pupil’s integrity is at core. Teachers and parents have to communicate both about the progress of the pupils and the general schedules in the school. Teachers also have to report to head teachers and other administrative authorities. There is a general high demand on teacher’s professionalism, quality of education, pupils learning target achievement and their eligibility for further education. Use
of ICT-systems for teaching and administration of education has therefore developed rapidly. We have here chosen to focus on two ICT platforms used mostly in all schools (to different degrees) in one Swedish medium sized municipality.

1.1. Aim of the paper

The aim of this paper is to present a case study of use of electronic identification to access ICT platforms in schools in order to analyze security aspects, organization and potential development of the platforms.

1.2. Case study methods

The general processes of policy development and design of eID highlight the importance of trust and safety (Soderstrom & Melin 2012; Melin, Axelsson & Soderstrom 2013), but there is also a need to analyze its practical outcomes and how it is embedded into organizational practices.

This case study focuses on use and implementation of secure log in to ICT platforms in five schools in a Swedish municipality – Linköping – focusing both on the central administration and schools’ practice. As an example of e-government this analysis applies a public administrative focus. All five schools are at primary and secondary level, one of the schools is a ‘free school’ publicly funded but run by a private organization. The case study material consists of nine in-depth interviews and eight focus groups, involving in total forty-one informants (school principals, teachers, pupils and municipality officials). Semi-structured interviews were made with school principals and the schools’ IT- or Fronter-administrators. The school principal was a key person with an overview of the school organization and the strategy and priorities for school development. Beside his/her leadership function, the principal held administrative responsibility at the school and was key decision-maker with regards to allocation of resources inside the school.

The research design strived to reach key informants who could inform us about the school organization and their experience with using the platforms Fronter, Dexter and other ICT-systems in their work. In addition local policy documents have been analyzed, to get a background of the processes and policy statements made both regarding these specific systems and municipal e-government in general. A limitation of the study is that we have not at this stage made any formalized interviews with parents. The schools are not willing to provide contacts with parents. However, in some of the interviews and focus groups the informants provided information in their role as parents, although tangentially.

2. Identification in on-line relations and local organization of e-ID

Identification can confirm citizenship and as such it is related to a complex web of relations. Identities are transformed and given other meanings in a globalized information society (Castells, 1997/2010). The development of electronic identification refers both to a technical solution and social and organizational arrangements (Axelsson & Melin, 2012). It is a socio-technical system, but as such it is limping. There is a mismatch of social and technical innovations that can challenge legitimacy of e-government (Wihlborg, 2012, Söderström, 2011) and electronic identification in particular and e-government in general (Axelsson & Melin, 2012).
In order to form legitimate e-governmental systems there has to be a balanced and high level of actual and perceived security. Actual information security is a factual, objective state of the information security in a system and it includes all aspects of security arrangements. Perceived information security is a subjective interpretation made by a single individual in his/her context and is based on personal knowledge and experience. There is always a difference between actual and perceived information security, since people never can reach a complete knowledge about the degree of actual information security at a specific point in time. The perceptions of information security can differ among different subjects who act in the same organization, as these are influenced by the nature of their work, the knowledge they possess, experience, own analysis and judgment (Oscarson, 2007).

The perceived security is highly related to the organizational setting that the ICT-system is contextualized into. E-government is based on political institutions and thus legislation and policy decisions are framing the IS-system (Hardy & Williams, 2011). In this case the national legislation clearly defines the role of the schools in the municipality and their local action spaces. There is a strict legislation on communication and transparency on pupils and their results.

3. e-ID as the way into e-services - The case study

This case study is based in Linköping, a Swedish municipality with 145,000 inhabitants. The municipality has been a forerunner in applying a functional organization, with internal procurement also in the educational sector. There are today a total of 84 schools, whereof 66 are primary schools (55 public and 11 free-schools) and 18 are secondary schools (5 public and 13 free-schools). In this section we present the two ICT platforms – Dexter and Fronter – used in schools and demanding eID.

3.1. Municipal policies on eID and education

The municipality has, in line with national and European policies, a local policy –“eVision”, with the aim that ‘e-Service shall make it easier to live and work in the community’ (eVision and eProgram for the Municipality 2006, p. 4). This policy, implemented during 2007-2010, focused on the three key areas: e-democracy, e-service and e-administration. The Digital Agenda adopted in 2012 made trust and safety of digital systems more explicit.

The ICT platforms in schools are a key area of implementation, where the pupils’ ‘individual development plans’ (IUP, legally demanded documentation) will be managed digitally and allow the parents to get access to the IUP (Municipal Digital Agenda 2012, p. 3). Information security was a fundamental precondition for this implementation and was given specific focus in the Digital Agenda. A joint log in function for easier access in the education area was to be developed, with a pilot on eID being conducted in spring 2012. The piloted systems included: Skola 24 (access to records on pupils attendance), Fronter (access to digital IUP) and Dexter (registration of supervision hours within childcare) (Municipal Digital Agenda 2012, p. 8). Fronter and Dexter are the most used systems and will be the focus here.

3.1.1. Dexter

Dexter is widely used in the municipality’s e-services towards citizens. Primary schools are using the attendance function and the grading function offered by Dexter. Through Dexter pupils and their parents can choose and apply for childcare, where the parents can follow up
their place in queue and report their income (to calculate fees). There are several alternative ways to log in to Dexter. Teachers are using their intranet password while parents can log in by a personal ID and password or their eID provided by banks (See Figure 1, where the blue boxes are translation of Swedish text). The former alternative is encouraged, but a pilot is running currently to investigate solutions for a wider use of the latter alternative.

Figure 1. Dexter snapshot, log in view at Linköping municipality webpage

Figure 1. shows different types of log-in opportunities for different user-groups. The main impression of the first page into the system is the focus on the three core actor-groups: parents, pupils and teachers. The parent-school relation is encouraged already here and the potential of the e-service is clearly pointed out.

3.1.2. Fronter

The program Fronter is both a learning/teaching platform and an administrative tool for managing work-tasks like pupil documentation (IUP, goals, portfolio and attendance records), teaching administration and planning. Linköping municipality started to implement it in 2007, and today most schools are included, but some still lag behind of local organizational reasons. The teaching functions are the mostly used and the communication between parents and schools is not yet fully implemented. Teachers and pupils are seen as internal users and they log in to the platform using a personal password. Teachers are using their intranet password and the pupils are using intranet password or a single-use password (See Picture 2). Parents are logging in by the external electronic identification system. Parents can- and have logged in by
using the pupils log-in. But they are supposed to use a personal eID to reach a higher level of security.

In contrast to the Dexter login-page the eID has a much more apparent role on this first page of the Fronter system. Login for parents are described as “For citizens” and requires an eID, provided by the private banks or national post.

The Figures 3 and 4 illustrate the increasing activity in Fronter, showing the amount of active users and total log-ins to Fronter per month. The dips in both pictures are illustrating the use during summer vacations. This development is grounding for our analysis focusing on security, organization and potential developments.

Figure 2. Fronter log in snapshot at the webpage at Linköping municipality

Figure 3. Total logins Fronter 2001-2012 (Linköping Municipality)
4. e-ID in practice - Results and Analysis

This paper is based on an in-depth single case study. The analysis of the use of eID and different platforms for interaction between parents and schools can be taken even further. Here we focus on information security, organization and potential developments of the systems with the certain eye for safe electronic identification.

4.1. Reach of information - security in focus

Our case study indicates a diverse range of thoughts and experiences of security aspects connected to secure log-in among the key actors. The informants highlight issues regarding both actual and perceived security of the system and the organization of work methods. The most common discussion is the management of personal and sensitive information.

Two important security aspects connected to the system’s factual security are operational reliability and data security. Fronter is considered as a stable platform, fulfilling these technical dimensions, according to the IT-coordinators (interview 12-10-22). Secure log in for legal guardians, on the other hand, is an actual and complex issue since these are unique users who have to manage several related issues of identification and rights. External electronic identification, eID, is a solution that the municipality plans to use so as to allow legal guardians’ access to the platform. However, the primary problem is connected to client support in diverse problems connected to the e-services. Since eID is administered by several agents (BankID, Telia, SEB, Posten, Nordea etc) the municipal administrative officials can only help partially if at all (interviews 12-10-23, and 12-10-22).

The municipality deals with large sets of sometimes personal and sensitive information regarding citizens, raising the demand for secure channels of handling this information. The demands for secure management of information are increasing in on-line systems, even if the security level was lower before these systems were put into use, as one of the administrative officials admitted:

“You can never be sure that the person calling is indeed the personal who he says he is” (interview 12-10-23).

There is a much lower actual security when calling, but it appears to be paradoxically interpreted as more secure among at least some end-users.

The system administrators also emphasized that it was still indefinite how different types of personal information would be managed and exposed to the users. One of the principals (School 1) also questioned what type of information was stored and securely managed in
Fronter. His school was running a project that was investigating the issue of digitalization of all registered files and was going develop security requirements on the system (interview 12-10-30).

Another finding concerns the different value of the information stored in Fronter for the different users. Information, for ex. logbooks written by the pupils, can be sensitive for the specific pupil or teacher who have logged a conflict during a project, while be totally non-sensitive for the rest:

“… if somebody logged in and read my logbooks, I would be hated in my class”
(Focus group 12-12-04).

The different value of information for the users has important implication for factual- and perceived security relation, meaning that the sensitivity of data and the security needs can be relative and relational.

Perceived security builds importantly on trust. The key actors seem to be the teachers who do or do not trust in their own IT-skills, the IT-systems themselves and the organization support. This system strives to include everyone and the differences regarding competences and experiences of competence was highlighted in the focus groups as the main constraint for common trust and organization.

4.2. Schools on-line a new setting – New organizational forms are emerging

Fronter and Dexter are implemented to improve organizational efficiency and quality both regarding pedagogics and administration. The schools are autonomous organizations, where the school principals have a large degree of independence. Based on their professional competences the teachers are entrusted to manage their daily work independently. In this context Fronter and Dexter are supposed to be implemented and used in flexible ways and the identification systems have to support this. The municipality cannot force the teachers to actually use the systems

“… they (ed. school principals) decide in the school, but it is the teachers who have the final responsibility (ed. to actually use the system)” (interview 12-10-22),

The municipal IT-coordinators have noticed the importance of the school principals’ personal engagement and interest in the systems for successful implementation and high interest in login to- and using of the systems. The principals have to prioritize the implementation and allocate time and money in the budget. But it is also about Fronter-administrator and skilled IT-teachers who understand its potential and who can show and inspire their colleagues’, as was explained by the IT-coordinators (interview 12-10-22).

A teacher (in focus group 12-11-05) described the organizational set up around Fronter as: ‘quite loose’. The users in some schools perceived no directives concerning how to use Fronter while in others it occurred naturally. The teachers who had used Sharepoint (a similar platform) a lot changed to Fronter much easier than other teachers, for example. It wasn’t organized specifically, but it happened naturally due to skilled IT-interested teachers, as one of the principals described:
Almost all informants pointed out that this relation was unclear and loose today. If a user (teacher, pupil or parent) encountered problems with Fronter or Dexter, the organization and support of the login possibilities was unclear.

Consequently, the organizational setting is important for the implementation of secure login and identification. Since the organizational setting in general was decentralized it was difficult to reach coordinated and standardized use of the information platforms and identification to it.

### 4.3. It is good, but can be better

Ideas of potential development of secure login to the platforms abounded in the interviews. These differed among the informant groups and related clearly to their focus and interests. The administrative officials had more of a system focus and parents and teachers had more ideas relating to their own use of the system. In spite of this the ideas on potential development can be categorized in two types, regarding organisation and regarding trust.

A combination of a shortage of IT-competence and infrequent use had a negative influence for the implementation and use of eID for ensuring secure IT-systems and e-services, which also implied less usability and weaker impact on target achievement. One of the teachers considered that

> “There should be a critical mass, that a majority of the teachers are using it. Maybe it should be 85% of the teachers who are using it, in order for it to be meaningful” (interview 12-11-06),

There is a long way to go in development and organisation of public e-services and electronic identification arrangements connected to them. Most of the ideas focused on the relationship and coordination among the schools, the municipality and the technical developers. As shown by the interviews, reliance and trust in the e-services depend on a range of factors and conditions, such as development of support structures with clearly defined roles of the agency, users’ skills and attitudes towards use of IT-systems in schools and competence development measures targeting the different groups of users in and outside the schools.

In the context of transition from a verbal tradition to a written and digital documentation on schoolwork and pupils performance, a considerable amount of sensitive data needs to be handled. This urges for development of secure, flexible and at the same time simple and accessible IT-solutions, a point that is raised by teachers, school principals and municipality officials. IT-coordinators foresee that more specialised systems are under development for deeper information to be shared on different levels by different actors, which raises the demand on security (interview 12-10-22).

Trust in the IT-systems used by the municipality (and other authorities) seemed to be a core element for acceptance and use of the different IT-solutions, according to our interview data. More specifically, we can identify two dimensions of trust - trust in the security of the system itself and trust in the subject’s own capacity to deal with the system. In both these respects there are potentials for development.
5. Concluding remarks

From this single-case study we can draw some conclusions regarding development and use of secure log in solutions in education. Firstly, we will point out the need for improved work on secure systems and use of eID embedded into the practical policy areas. Electronic identification has to be suitably included as an essential part of all public administrative situations where identification is needed. New forms of trust and legitimate governance have to be promoted when public administration less and less takes place in face-to-face situations. This case study highlights two such basic aspects: the disparity of actual and perceived security and the organisational arrangements.

The main findings show that use of secure log in or eID is at its incipient stage in the education area in the municipality of Linköping. This is explained by the difference in factual- and perceived security among the different user groups. Low frequency of use, technical problems of the systems, lack of IT-competence and lack of trust in IT are several aspects that seem to influence the perceived security of the system among the users. Identification is not the primary focus of public e-services from a user perspective. However, when highlighted no respondent hesitated to its importance.

The general organizational arrangements and the decentralized management of schools muddle the trust in eID and the specific platforms with the trust in the educational system in general. These platforms had a standardized and coordinative function that did not fit into to the decentralized and flexible organization of the schools and their work methods. Private software companies have designed and provided all-inclusive platform solutions, especially in the case of Fronter, but the local implementation in schools was to different extent limited and opened for frustration. In addition the Swedish national eID connection to these systems presents a challenge. Thus there are laggards among potential users who might have problems accessing the external identification rather than the platforms themselves. Perceptions of security of the systems take place in the complex interplay of the providers of electronic identification and the services within the platforms.

There are several challenges of making these types of systems more secure and still keep them simple for the user and flexible for management. There are obvious needs for further technical development, improved competence and trust among users, and improved organizational set ups for implementation of these systems. This work is essential for security and trust in public e-services and e-government in general.

References


**Official documents**

SOU 2010: 62. Så enkelt som möjligt för så många som möjligt - framtidens e- förvaltning, [As easy as possible for as many as possible, Future e-administration], Statens offentliga utredningar/ Swedish governmental report.


Interviews
2012.10.22 Group interview with Municipality IT-coordinators (2 participants), Municipality
2012.10.23 Group interview with Administrative officials (5 participants), Municipality
2012.10.30 Group interview with System administrators (2 participants), Municipality
2012.10.30 Interview School Principal 1
2012.11.06 Interview Secondary School Teacher 2

Focus groups
2012.11.05 Focus group Primary School Teachers (5 Participants).
2012.12.04 Focus group Secondary School Pupils (4 participants)

Municipal documents
eVision och eProgram Linköpings kommun. Adopted by municipal council 2006-12-01.
Budgets and final account reports from Linköpings kommun, 2007-2012.

About the Authors
Elin Wihlborg
Elin Wihlborg is a professor in Political Science at the Department of Management and Engineering, (IEI) Linköping University, Sweden. Her research focuses on public administration, in particular regarding regional development, urban planning and e-government and implementation issues in general. Her research has been published internationally and in handbooks for policy makers in municipalities and regions in Sweden. She is a member of the faculty board and supervises a number of PhD-students in different areas.

Mariana S. Gustafsson
Mrs. Gustafsson is currently a PhD student at the Department of Management and Engineering, (IEI) Linköping University. She has worked in a number of FP5 and FP6 research projects in the area of innovation, labor market research and information society, based at Lund University. Subsequently she has joined Oxford Research to work with evaluations and consultancy in the areas of innovation and organization development. Her research interest is currently focused on politics and economy of high technology and consequences of these upon society.