JeDEM 5(2): 155-173, 2013
ISSN 2075-9517
http://www.jedem.org

Safe Online e-Services Building Legitimacy for E-government

A Case Study of Public E-services in Education in Sweden.

Mariana S. Gustafsson*, Elin Wihlborg**

**Department of Management and Engineering, Linkoping University, Sweden. mariana.s.gustafsson@liu.se, +46 13 281582*

***Department of Management and Engineering, Linkoping University, Sweden. elin.wihlborg@liu.se, +46 13 281578*

***Abstract**: There is an increased use of public e-services integrating citizens into public administration through electronic interfaces. On-line interaction among public organizations and citizens is one core relation in e-government that hereby becomes embedded into daily practices. A safe entry into e-governmental 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. This paper draws on a case study of use of ICT platforms in education administration in order to study the implementation of secure login process and factors that may have implications upon trust in-and legitimacy of public e-services at local e-government level. Besides describing the implementation process and analyzing security and organizational arrangements connected to the use of the platform, the paper address the argument that secure identification tools are essential for increased use of e-services and lead to greater legitimacy of the public (e)services. The analysis focuses on information security, organization set-up and potential development of the platforms, contributing with empirical findings and conceptual applications. A key finding was that 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 of the findings was that safe and well organized identification systems that were considered as trustworthy and useful among citizens were essential for increased use of the services and legitimate public e-services in general.*

Keywords: local e-government, public e-services, education administration, legitimacy, electronic identification, information security

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, parents and pupils from the seven participating schools, as well as the officials at Linköping Municipality, who made this study possible.

There is no doubt any more that information technologies and Internet affect how governmental authorities, organisations and citizens interact. E-government has become a pervasive reality in which society is governed and organized. Citizens', companies' and other societal actors' expectations of 24-hour, fast, efficient and flawless governmental and public services are high (Evans & Yen, 2005). These are matched by goals and strategies for governing using information and communication technologies in response, and have led to the emergence of 'information government' (Mayer-Schönberger & Lazer, 2007), 'virtual state' (Fountain, 2001) or, more commonly, e-government.

The Swedish Government has an extensive policy on e-government and so do most local governments as well. The main aim of the national e-government policy is to make on-line public services and administration as simple as possible for as many as possible to exercise their rights and obligations and take part of governmental services. The policy for e-government has been further developed in a Digital Agenda (2011) that focuses on the citizen's needs of interaction with the government and emphasizes the importance of transparency, quality, efficiency and innovation

of governmental and public services, as well as the need for cooperation between the governmental agencies at different levels of government (Ministry of Enterprise, 2011).

Being ranked as 7th among the leaders of e-government development in the world and 5th in Europe (United Nations, 2012), 74% of the Swedish governmental agencies provide about 640 e-services for the citizens. The introduction of electronic identification (eID) in accessing these services is advancing rapidly, 20% of the e-services require identification by eID/BankID, while still 59% of the e-services require identification by id and passwords, 15% of the services require e-signature (E-Delegationen, 2011).

A critical issue for further development of extensive and integrated e-government is citizen identification and security connected to use of governmental e-services that aims to build trust and legitimacy. 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). But the risks in the settings of the digitalized society are also high (Beck & Ritter, 1992; Castells, 1996, 2011). At the same time, electronic identification is essential for providing public e-services that are individual and related to the individuals' personal information (Axelsson, Melin, & Lindgren, 2013b; Söderström & Melin, 2012; Taylor & Lips, 2008). All this said, however a recent survey on Swedish population use of IT has revealed that information security was not 'high on the agenda' when it comes to the user-behaviour. According to the survey 95 % of the respondents[1] did not use any service to anonymize their computers and almost everybody (97%) used passwords. However 94% saw some kind of risk in using internet, with the highest being personal data being accessed by unauthorised people (SIFO, 2012; Statistics Sweden, 2013).

Legitimacy of government based on citizens' trust in state institutions and agency has been an issue for political science research for decades (Easton, 1957). Legitimacy of governments is essential, but it has to be further developed in the e-government context and there are demands for new approaches due to changing technological and organisational arrangements characterising the technological society of today (Wihlborg, 2014). 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 there is a need for safe and trustworthy arrangements of identification. The Swedish welfare state has been enjoying a high level of legitimacy due to the close communication between citizens and public service through indispensable and high quality services (Kumlin & Rothstein, 2005) and this now has to be enforced even in relation to e-governmental arrangements.

Security of personal data emerges as an important issue when the interaction between citizens and governmental agencies is increasingly carried online though diverse e-services. Citizen's trust in e-government and its connection to the security of personal data stored in- and handled through technologies is an important question for researchers, policy makers and technology developers. More recently, the importance of trust and safety has been emphasized in policies and design of eID, along with the need to analyze its practical outcomes and how it is embedded into organizational practices (Melin, Axelsson, & Söderström, 2013; Söderström & Melin, 2012).

This paper analyses the introduced issue on safe log-in to e-governmental services through a case study in the education area in Sweden, at local government level. Education, up until the age of fifteen is compulsory and free in Sweden. The national government regulates and funds all education. But the 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 and they get the same public funding as schools managed by the municipality. 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

[1] 1000 telephone interviews were conducted.

a long history of use of ICT in education in Sweden. The access to computers has increased considerably, both in schools and in society as a whole in Sweden. Almost all teachers on the upper secondary school level and two thirds of the teachers at the ground school level have access to an individual computer. Pupils' access to computers has doubled since 2008. But at the same time there is a large need for competence development among the teachers concerning security on the net and use of digital tools in teaching (Skolverket, 2013). With the new Education Act (Government, 2009) 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 secure 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 therefor developed rapidly and has become an important aspect of public e-services in the context of e-government. We have here chosen to focus on two ICT platforms used mostly in all schools (to different degrees) in one Swedish medium sized municipality.

This paper draws on a case study of use of ICT platforms in education administration in order to study the implementation of secure login process and factors that may have implications upon trust in-and legitimacy of public e-services. Besides describing the implementation process and analysing security and organisational arrangements connected to the use of the platform we will also address the argument that secure identification tools are essential for increased use of e-services and lead to greater legitimacy of the public (e)services

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 analyse security aspects, organization and potential development of the platforms. More specifically:

- The first research question refers to a case of implementation of e-government in Sweden:
- How is secure log-in actually arranged and perceived among key groups of users (administrative staff, teachers, pupils, school principals and parents) of the ICT platforms organized in the municipality and at the schools? (section 4)
- The case study will be analysed trough three main perspectives:
    - How is information security arranged? (section 5.1)
    - How is the organisation in the schools and the relations between the schools and home, influenced by the use of the platforms? (section 5.2)
    - What potential for change and development are discussed among the key user groups? (section 5.3)
- Finally, the general conclusion and discussion returns to whether there is any connection between secure log in and increased use leading to greater legitimacy of public e-services in the e-government context (section 6)

1.2. Outline of the Paper

This article proceeds in several steps by introducing the methods and the sample of the case study in section 1; by framing and anchoring the study in institutional theories and information systems theories in section 2; by shortly presenting the two platforms, FRONTER and DEXTER, that were the focus of the study in section 3; by presenting the experiences of the key user groups

in section 4; by analysing information security, organisation sat-up and potential development of the platforms in section 5; to finally provide concluding analysis of implementation challenges and implications for the legitimacy building in section 6.

1.3. Case Study Methods

The qualitative case study on the use of ICT platforms and secure log-in was conducted in the Linköping municipality (150 000 inhabitants) in the framework of the nationally-funded project 'Future Safe Electronic Identification', funded by the Swedish Civil Contingencies Agency. We focused both on the municipality administration, which is responsible for education and schooling, and on the platform use at 7 schools. The sample choice was based on a preliminary mapping of the 'history of use' of ICT platforms in 56 schools in the municipality, the inclusion of both public and private schools and the inclusion of large (more than 300 pupils) and small (less than 300 pupils) schools. All 7 schools were at compulsory and upper secondary level, one of the schools was a 'free school' publicly-funded but run by a private organization. 18 semi-structured interviews and 9 focus groups, involving 55 participants (school principals (4), teachers (17), schools' platform administrators (2), pupils (13)[2], parents (11) and municipality officials - users of platforms (8)) were the main sources of primary data.

The research design strived to reach key participants who could report to us about the school organization and their experience with using the platforms FRONTER, DEXTER, SKOLA 24 and other ICT systems in their work and studies. The school principals were key persons with an overview of the school organization and the strategies and priorities for school development. Beside the leadership function, the principals held administrative responsibility at the schools and were key decision-makers with regards to allocation of resources in their respective school. The IT- or FRONTER – administrators were key informants with regards to practical implementation of the platforms and held important knowledge on their functioning and teachers' perceptions of the platforms. Teachers, pupils and parents were holding important information about the functionality and usability of the platforms and could give insight about their experience with using them in their work and in interaction with each other. In addition, local policy documents were analysed in order to learn about the background of the processes and policy statements made both regarding these specific systems and the municipal e-government in general.

This case study and the analysis presented here builds on an abductive approach (Alvesson & Sköldberg, 2009). The ambition is to strive for a preformative interpretation of the case by focusing on themes and concepts, emerging in the empirical material, that are subsequently consulted with the existing theories, in order to return to the next level of interpretation that can eventually lead to problematisation or further development of the theoretical concepts. The analysis is thus not restrained by a specific theoretical framing. Instead we anchor our interpretation in a number of theories or theoretical concepts used in political science and information systems.

2. Theoretical Framing of the Study

In this section we will present the theoretical concepts that we guide the analysis of the case study. By this framing we defined and limited our main perspectives applied in the latter analysis of implementation of secure login to education administration platforms and the implication of their use upon legitimacy of public e-services. This section ends with a conclusion of the main theoretical concepts.

2.1. Legitimate e-Government

Legitimacy of government has been described in terms of acceptance it received by the citizens. According to the acceptance principle, political legitimacy is built on the coherence between values and norms among the electorate that correspond to those of the elected. Legitimacy is a two

[2] Grade 9 in compulsory school and grade 1 in upper secondary school

dimensional concept, consisting of inputs and outputs of the political system (Easton, 1957; Scharpf, 1997, 2010). Legitimacy in this sense entails democracy, accountability and effectiveness of governments. In terms of input to the political systems legitimacy derives from the government decisions based on preferences of the citizens. In terms of output of the political system, legitimacy derives from the effectiveness of goal achievement of governmental policies and activities. Consequently, we could consider that e-government activities that are democratic and accountable, but result in ineffective e-services, as well as effective e-services that are employed by non-democratic and unaccountable governments will cease to be legitimate.

This view has been challenged to state that democratic, accountable and effective government activities were not enough to build legitimacy. The quality of government activities is at least as essential in building legitimacy as the other elements (B. O. Rothstein & Teorell, 2008). In mature welfare states with extensive public services there has been an increased focus on the processes where legitimacy is gained on the output side of the political system when public services are used to improve the quality of life among citizens. Furthermore, at the input-side of the political systems public services for welfare and other aims are primarily provided by street level bureaucrats. Street level bureaucrats are the public servants meeting the citizens in daily interaction providing services as for example education, care, and social services. They most often have face-to-face interaction and frequent meetings with citizens (B. Rothstein, 2009). Through their continuous interaction they build up trust both in personal relations and towards the governmental system as such, thereby contributing to building legitimacy.

Hereby also public e-services have to be considered in relation to legitimacy building on the output side of the political system. If public e-services are considered as safe and trustworthy they will contribute to the continuous building of sustainable legitimacy (Wihlborg, 2014). We will focus on two core aspects of legitimacy in the following analysis of secure log-in. Firstly security is a core aspect of e- in e-government and if security issues are trustworthy among the users both in actual and perceived terms it will contribute to legitimacy. Secondly, the organizational arrangements of the services indicate how and by whom legitimacy can be gained.

2.2. Security as a Core Aspect of Legitimacy

Security is a basic pre-requisite for legitimacy. Safety and security make the citizens to trust the state in a very basic meaning. When adding “e-“ to governmental activities, new forms of security and safety arrangements are demanded. There are two main reasons for this improved demand for security. Firstly, there is a decreasing degree of face-to-face interaction in on-line communication that poses demands for new forms of trust and thereby for legitimacy (Turkle, 2012). Secondly, there are increased risks of profiling citizen information and tracking personal information through the increased use and storage of personal data and the evolving capacity of data aggregation by new information technologies (Bannister, 2005; Ciborra & Navarra, 2005).

Information security of citizen data becomes an important aspect when e-government is carried out on electronic platforms and e-services. The focus on security regarding e-government, has mainly been addressed by theories and concepts emerging from an information system perspective. A model addressing this aspects is distinguishing between actual information security and factual information security (Oscarson, 2007). 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 (Gustafsson, 2013; Oscarson, 2007). Furthermore, the perceived information security should be assessed in relation to

the citizens' perceptions of security at a more basic level, where security is valued and desired and involves a coveted state of affairs (Gustafsson, 2013).

2.3. Organization as a Core Aspect of Legitimacy

This is mainly based on a more political science perspective that do not primarily pay any attention to the e- part of e-government. However, it is indeed important to extend the knowledge on the use of and implications from IT-platforms into the analysis of legitimacy. Jaeger argues that e-government from a democratic perspective can be analyzed using three approaches: liberal individualist, communitarian, and deliberative" (Jaeger, 2005). All these indicate that the use of e-government can be embedded into different approaches of democratic legitimacy. In this case the use of ICT-platforms for education administration presents a case of e-government legitimacy focusing on individual and organizational perspectives, where the deliberative aspect involves that more information and transparence can lead to more informed participation in e-government. Thus the organization of e-government can support legitimacy from different democratic perspectives and here both the individual and deliberative approach has to be considered.

Technologies are commonly enacted in social and organizational contexts, giving rise to complex interplays between the technical artifacts and their users, but also influencing organizational structures, work methods and cultures (Fountain, 2001; Kling, 2000; Orlikowski, 2000). Employment of technologies result in certain organizational outcomes such as efficiency, effectiveness, quality, transparency and legitimacy, while organizational forms include structural characteristics such as centralization, formalization, and communication channels (Luna-Reyes & Gil-Garcia, 2011). The enacted technology and the subsequent organizational results have also an impact on the organizational forms and the institutional arrangements (Fountain, 2001). ICTs are commonly embedded in the work processes and methods and are usually part of the organizational infrastructure (Fountain, 2006).

In order to understand how technology design, implementation and use are influenced by the organizational context and structures and vice versa, as well as capture the transformative nature of the technology enactment process, the institutional approach provides analysis models such as 'technology enactment framework' that focuses on the interplay between technology, bureaucratic structures and institutional arrangements (Fountain, 2001, 2006; Luna-Reyes & Gil-Garcia, 2011). According to this model, technological artifacts become 'enacted' when shaped by organizational forms and institutional arrangements which in their turn are affected by use, design and choice of ICT.

The interplay between the ICT, the organizational structures and the institutional arrangements is our main interest in terms of reaching legitimacy of public e-services through implementation and use of ICT in schools. In our study the technological artifacts are the electronic platforms used in education administration and the eID as secure login to them, the schools and the municipality represent the organizational context and rules and regulations among which The School Act (Government, 2009), but also the emerging identification rules and procedures connected to e-services present the institutional arrangements.

2.4. Identification in Online 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, 2011). The development of electronic identification refers both to a technical solution and social and organizational arrangements (Axelsson, Melin, & Lindgren, 2013a). 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 and electronic identification in particular and e-government in general (Axelsson et al., 2013b; Söderström & Melin, 2012; Wihlborg, 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.

2.5. The Three-armed Anchor

Taking an abductive and interpretative approach (Alvesson & Kärreman, 2011), and using theoretical concepts from institutional theories and information security systems theories presented above, our analysis of legitimacy of public e-services in the education administration will thus focus on three core perspectives, that represent our three-armed theoretical anchor: the information security, the organization process and the potential development as perceived by the key user groups. We mean that these perspectives are essential in understanding how legitimacy for e-government is build.

3. e-ID as the Way into e-Services – The Case Study

This case study is based 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, but the analysis will also include SKOLA 24, as it was the platform used in the free school in our sample.

3.1. Municipal Policies on e-ID 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' (Linköping Municipality, 2006). 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' 'written assessments' and 'individual development plans' (IUP, legally demanded documentation) will be managed digitally and allow the parents to get access to the IUP (LK, 2012). 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) (LK, 2012). 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 the platform. Through the platform 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 the platform. 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.

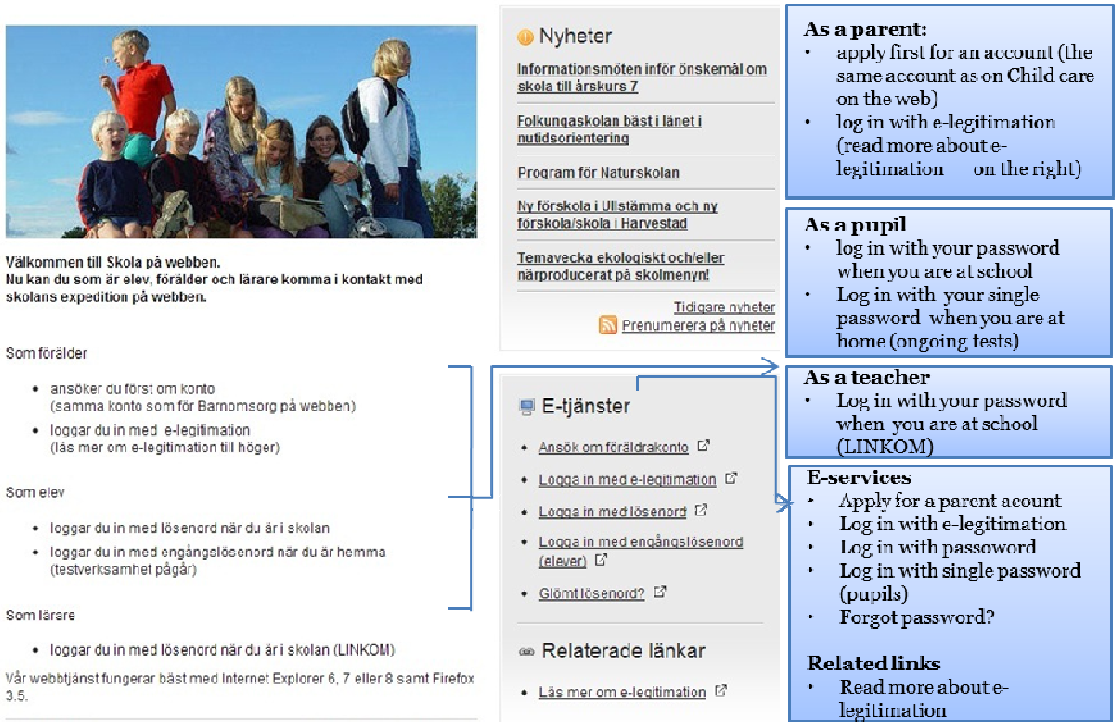

Figure 1. DEXTER snapshot, log in view

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

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. The 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 Figure 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.

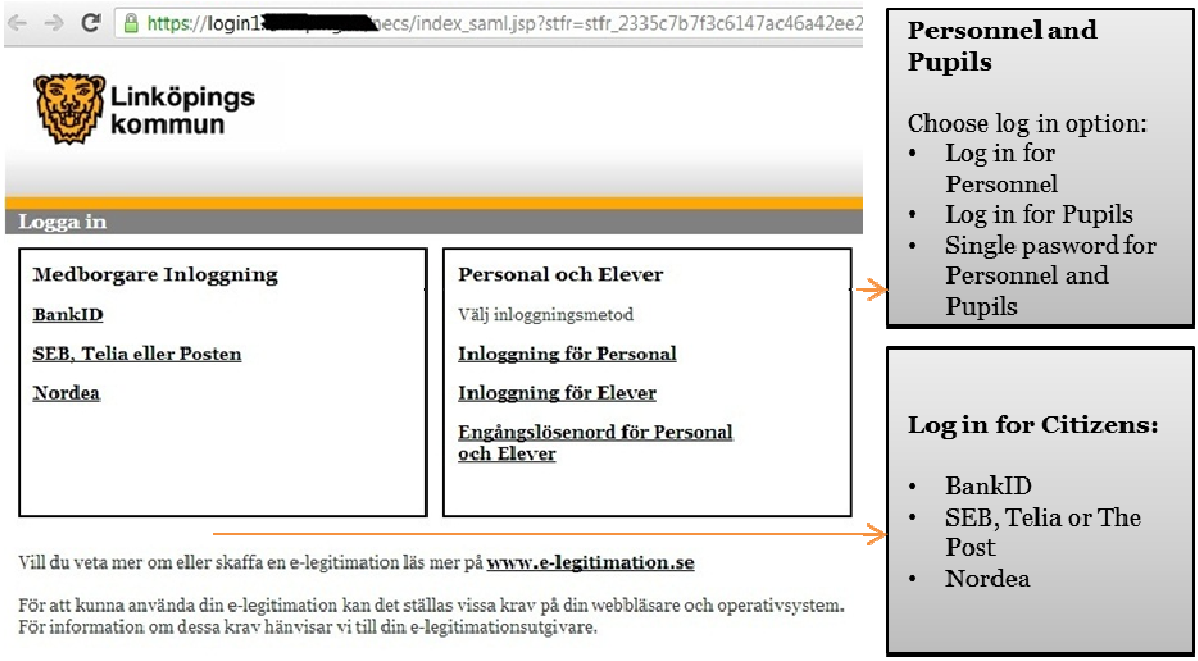

Figure 2. FRONTER log in snapshot

In contrast to the DEXTER login-page the eID has a much more obvious role on the front page of FRONTER. 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 the platform per month. Municipal monitoring of the platform use shows that there is an increasing number of users 6 865 and there is a steady increase in the frequency of use of the tool, with 48 000 unique log in registered in the end of October 2012. The dips in both figures are illustrating the use during summer vacations. This development is grounding for our analysis focusing on security, organization and potential developments.

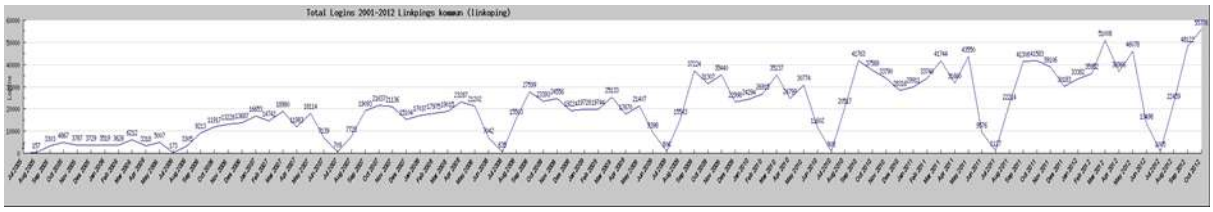

Figure 3. Total logins FRONTER 2001-2012 (Linköping Municipality)

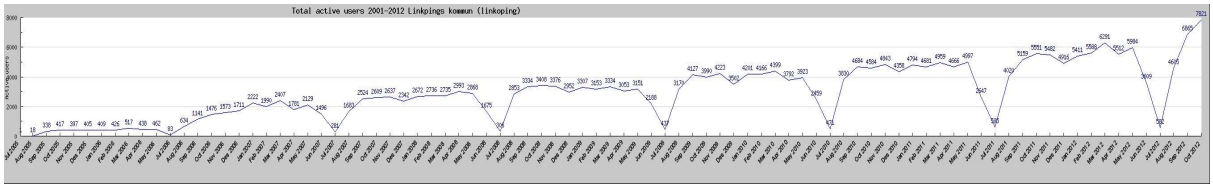

Figure 4. Total active users FRONTER 2001-2012 (Linköping Municipality)

4. e-ID in Practice: Perspectives of Key User Groups

In order to study how electronic platforms are implemented and how legitimacy was built through their use in the education area, we identified and approached several key groups of users of the education administration platforms in the municipality. These users were acting at two organization levels: at the municipality level and at school level. The participants in the interviews and focus groups were thus representing municipality bureaucrats, school principals, teachers, pupils and parents. A selective presentation of results per key group follows below.

4.1. Education Administration at Municipality Level

There are two important security aspects connected to the system's factual security: operational reliability and data security. According to the municipality IT-coordinators, FRONTER fulfills these technical dimensions per today. The system administration for FRONTER meets their expectations today. Compared with earlier systems, it is more stable. Data security is ensured by encrypted data transfers and secured log in. Secure log in becomes a concern especially when external users, i.e. parents, are invited to access and use the platform. Another security issue is raised by giving teachers administrative rights to modify the content in the platform, which urges for wide security set-ups, explain the IT-coordinators.

"We are working right now with two factors authentication, but this has not been applied in practice yet. We are discussing the issue of legal guardians as unique users, which poses a range of challenges (for the security of the system)' (I_10.22_LK, 2012).

Secure log in or eID is tested through pilots in the municipality and is considered as an alternative to replace the currently used log in through user name and password. Although eID has been used by different actors in Sweden during the last five years, the IT-coordinators consider it still being unripe for using it widely in different services. The central questions that arise from the experience of using eID in the municipality e-services is connected to the technical support and the agency responsible for it. Because there different forms of eID that operate on the market (BankID, Telia, SEB, Posten, Nordea etc), there are also different agents administering it, an issue that complicates the picture for the end-user in case of failed or problematic log-in, when the user does not know who to address with the problem, it was explained by the IT coordinators. By having a chain of different agents involved in the process the support becomes difficult, costly and time consuming, according to the experience gathered in the municipality.

'Such a support is much more complicated than a usual customer support service, it's not just about forwarding the different issues. It is depending on different authorities. ' (I_10.22_LK, 2012)

Information flow appears to have implications on secure log in that is connected to the work methods that the municipality employs in handling different types of information. There are several questions that result in connection with this: what type of information is transferred to which user and in by which methods. Taking in to consideration that the municipality deals with large sets of sensitive and less sensitive information about citizens and that it has different channels of receiving and sending this information to the citizens, there is a need for secure methods of handling this information. The interviewed administrative officials admit that although considerable work has been done to develop work methods that ensure that personal data is handled safely, some of the methods used today, for example telephone communication and even log in solution with id and password, cannot be considered totally safe.

'Today it is easy to get hold of somebody's personal security number or email password… You can never be sure that the person calling is indeed the personal who he says he is' (I_10.22_LK, 2012)

In these situations the responsibility lies on the public administration official to judge whether or not to release the information and what type of information to release. One the other hand, they all seem to be confident that an experienced professional making this judgment, can be as safe as other technical alternatives provided by the e-services.

Another side of the same issue concerns the type of information to be released or accessed through the e-service system. The municipality system administrators emphasize that it is still indefinite what type of personal information is to be shown to the user when the latter accesses it through the different e-services.

'It is not currently totally clear what type of information shall we show. What do one wants them (users) to access. For example in the secondary school the pupil becomes 18 years old and is major. In choosing the different programmes there is no need for parents' signature, it is the pupil who makes the choice. Then the question arises can we show the parents the pupils choices? It is this kind of questions that we work on now – what is a public record and what is work record – but we don't have the solution yet' (I_11.12_LK, 2012).

4.2. Teachers

Teachers had various experience of use of FRONTER or other platforms in teaching and administration and the same could be observed about their attitudes and thoughts about ICT in their work. It is obvious that the current implementation of the platform, the experiences of use and consequently the discussions concern usability, functionality and integration in the school's organizational structure and work methods, rather than a major focus on the informational security aspects of the platforms. It can clearly be observed that the use of the platform is very individual from teacher to teacher, at this implementation stage, based on the teachers' ICT competence, interest in the platforms and teaching and administration methods he or she uses in their classes.

Existence or lack of a clear policy or a decision coming from 'above' (i.e. the school principal, the municipality) concerning the use of the platform influenced teachers' motivation and how they used it. Existence or lack of teachers technology-impellers, interested in ICT and able to inspire the colleagues seemed also to have an influence on the use and enactment of the platforms at schools.

'In our working group there is nobody who drives FRONTER. There is nobody especially good on it. I thought to be myself that person and I am interested myself. But I do it mostly for my own sake, because there is no decision from the leadership that it (ed. the platform) shall be used. My role would be then to both promote the tool, learn how to use it and instruct others. That's too much job' (FG_11.27_IBR, 2012).

Interestingly the influence of the technology-impellers in these schools was positive in some schools and negative in others. Those of them who had a positive attitude towards the platform and trusted it inspired and taught others to use it. Those of them who considered it obsolete and inefficient and did not trust it influenced their colleagues to be critical to it as well.

Information security aspects in using the platform in teaching and administration were linked to the usability of the platform. Teachers explained that if the platform was to be used frequently and actively, the log in to it should not be complicated to such an extent that it makes it difficult to perform their core activity of teaching. Security is also a matter of trust in IT systems, as it is uncovered by our interviewees. Teachers' trust in their own ability to deal with different IT-systems and understand how to use them is connected to more frequent use of the platform and vice versa.

Consequently, there can be observed a difference among the teachers in schools, but also among parents, concerning use and trust in secure IT-systems.

'If you work with one system and understand how it works, you can change to another system and be able to work in it quite fast', concluded a teacher (FG_12.04_lFK, 2012).

In another school the reactions differed:

'that information disappears from FRONTER is a severe stress moment for the teachers, especially under time press' (I_11.06_rAT, 2012).

Consequently, it can be the case that this also may lead to teachers' and parents' insecurity and unreliability for the tool.

4.3. Pupils

The pupils regarded the platform as useful and secure, but a bit old-fashioned. They were satisfied with those teachers who used the platform actively in some subjects and desired that more teachers used it and filled it with content. According to them their use of the platform was greatly dependent on the teachers' use of the platform. At the moment of the interviews most of them did experience that information stored and handled in the platform had a sensitive character. According to them not even the pupil documentation ('written assessment' and 'individual development plan') contained sensitive data, as most of these had information of general character about the pupil (FG_11.27_eBR, 2012). However, they agreed that the more specific documentation that is stored in the platform is, the harder the requirements for information security should be. They also agreed that current login with id and passwords was not secure enough if systematic and more specific pupil data should be stored on the platform.

Out of these observations, it can be concluded that it depends on the user, i.e. the teacher and the pupil who create the information the extent to which an information becomes sensitive. Furthermore, what is sensitive for one pupil or teacher may not be perceived as sensitive for the other pupil or teacher. For example one student explained that:

'…if somebody should come over my logbooks, then I should definitely be hated in my class. I have recently changed classes and have written everything I think and believe about the subject and the situation. I didn't keep anything. It's quite sensitive'(FG_12.04_eFK, 2012).

4.4. Parents

The parents' use of the platform differs in accordance to how long the school and the individual teachers have come in using FRONTER. Their use ranges from once per week in connection to the weekly letter and once or twice per school term in connection to access to the pupil's IUP before the individual meeting. The parents are positive in principle to using electronic platforms for accessing their children's school data. However, currently the schools still use paper documentation in contact with the parents in order to reach complete coverage of the concerned. Most of the interviewed parents consider the written assessments and the IUPs as sensitive data that should be protected. A parent reflected for example:

'One can ask oneself about everything that is stored in there – how damaging can it be? I believe in the good human. I praise openness and consider dialog with the teacher as being important. But the information that is stored there is not relevant other than for the involved parent, teacher and pupil. If a pupil needs special support, than it would be sensitive for him or her if the classmates knew about it.' (I_03.09_f3FK, 2013)

Most interviewed parents trust in that there is a practice and regulation on what information the teachers should store on the platform. Since most of the information already is registered in the

municipality databases there would not be much difference with the use of the platforms (I_26.08_fVD, 2013). In terms of trust in the platforms' security one of the parents motivated:

'Yes I do. Because it has existed for such a long time, I believe that they have developed the system and minimized the risks for unauthorized login. And it is somebody else is behind the program. Were it the school that owned the platform, then I would have been doubtful. The school should do teaching, not security, their main activity is teaching. So, I think that FRONTER has anyway developed in the direction to make it easier to login and ensure the security of information stored there' (I_03.09_f3FK, 2013).

Some parents have experienced difficulties with eID login to the platform, which made them give up this alternative in favor of the simpler one, the id and the password. They have discovered that it works to login in with the id and password and so far the content for these two login alternatives has been the same. Other parents, on the other hand have had no problems using eID and considered it as a natural higher security measure, but started questioning it when both login alternatives were actively used. The parents as the teachers stressed the importance of the platforms combining both security requirements for certain stored information and usability of the platforms if these are to be used frequently.

4.5. School Principals

The school principals proved to be concerned with the type of information to be stored on the platform. While a considerable part of the school information (eg. grades) is public there is still a part of information that is connected to the personal integrity of the pupil - usually containing psychological, medical and pedagogical records on pupils' behavior, abilities, choices and attitudes towards studies.

'The system should be much safer technically if we are to store this kind of information in it. As it is today, the pupils have their own passwords, but this is not safe either, as it can land in somebody else's hands… In parallel the school is running a project that investigates the issue of digitalization of all registered files and there is going to be a secrecy requirement on the system. And then there should be a much higher security requirement on FRONTER as it is today.' (I_11.06_rAT, 2012).

Another implication for the use of eID lies in the nature of work at school, where different types of information are transmitted among teachers, among the teachers and pupils and among the teachers and parents. The school information ranges from weekly newsletters that are typically public in nature to work material concerning a pedagogical investigation of the pupil that is highly sensitive and confidential. The point that the school principals, along with the teachers and the IT-coordinators raised concerning this was that it was still unclear about the technical set-up for accessing such heterogeneous information through using eID. This issue can pose challenges in terms of hindering daily use of the platform by the teachers, parents and pupils given that eID keeps to be perceived as a difficult login by the users, as it seems to be the case from the interviews. As one of the school principals explained:

'It's still an open question what one wants to achieve with eID. Maybe we'll have to live with a double system, where the sensitive information is stored in a secured system with secure log in and that doesn't need to be accessed so often, while the daily information lies more openly on the website', was the suggestion of one of the school principals (I_11.27_rBR, 2012).

5. Legitimacy Building in Process

We proceed in this section with further analysis of the interview data based on the three aspects: information security, organization set up and potential development in our aim to study how local e-government legitimacy is built through the use of the education platforms.

5.1. Challenges of Information Security

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 (I_10.22_LK, 2012). 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 (FG_10.23_LK, 2012; I_10.22_LK, 2012).

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. 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 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. Another finding concerns the different value of the information stored in the platform 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 (FG_12.04_eFK, 2012). 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.

5.2. Changing and Emerging Organizational Arrangements

The platforms 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 the platforms 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)" (I_10.22_LK, 2012).*

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 platform-administrators and skilled IT-teachers who

understand its potential and who can show and inspire their colleagues', as was explained by the IT-coordinators (I_10.22_LK, 2012).

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 the platform 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:

> *"There was a teacher in each work group who had the competence and the will to test FRONTER" (I_11.06_rAT, 2012).*

Almost all informants pointed out that this relation was unclear and loose today. If a user (teacher, pupil or parent) encountered problems with the platforms, 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.

5.3. 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 organization 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" (I_11.06_rAT, 2012)*

There is a long way to go in development and organization 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 specialized systems are under development for deeper information to be shared on different levels by different actors, which raises the demand on security (I_10.22_LK, 2012).

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.

6. 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 is increasingly included as an essential part of all public administrative situations where identification is needed. This results in new arrangements of trust and legitimate governance when public administration provides welfare services by electronic means. This case study highlights two such basic aspects that appear characteristic for these new forms of arrangements: the disparity of actual and perceived security of the information systems and the importance of organizational 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. 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

Alvesson, M., & Kärreman, D. (2011). Qualitative research and theory development : mystery as method / Mats Alvesson, Dan Kärreman: Thousand Oaks, CA : Sage Publications, 2011.

Alvesson, M., & Sköldberg, K. (2009). Reflexive methodology : new vistas for qualitative research / Mats Alvesson and Kaj Sköldberg: Los Angeles ; London : SAGE, 2009, 2. ed.

Axelsson, K., Melin, U., & Lindgren, I. (2013a). Public e-services for agency efficiency and citizen benefit-Findings from a stakeholder centered analysis. Government Information Quarterly, 30(1), 10-22.

Axelsson, K., Melin, U., & Lindgren, I. (2013b). Public e-services for agency efficiency and citizen benefit — Findings from a stakeholder centered analysis. Government Information Quarterly, 30(1), 10-22. doi: http://dx.doi.org/10.1016/j.giq.2012.08.002

Bannister, F. (2005). The panoptic state: Privacy, surveillance and the balance of risk. Information Polity: The International Journal of Government & Democracy in the Information Age, 10(1/2), 65-78.

Beck, U., & Ritter, M. (1992). Risk society : towards a new modernity. London: Sage.

Castells, M. (1996). The information age : economy, society and culture. Vol. 1, The rise of the network society / Manuel Castells. Malden, Mass.: Blackwell.

Castells, M. (1997). The information age : economy, society and culture. Vol. 2, The power of identity. Malden, Mass.: Blackwell.

Castells, M. (2011). Communication power. Oxford: Oxford Univ. Press.

Ciborra, C., & Navarra, D. D. (2005). Good governance, development theory, and aid policy: Risks and challenges of e-government in Jordan. Information Technology for Development, 11(2), 141-159. doi: 10.1002/itdj.20008

E-Delegationen. (2011). Uppföljning av myndigheternas arbete med e-förvaltning och e-tjänster 2011.

Easton, D. (1957). An Approach to the Analysis of Political Systems. World Politics(3), 383. doi: 10.2307/2008920

Evans, D., & Yen, D. C. (2005). E-government: An analysis for implementation: Framework for understanding cultural and social impact. Government Information Quarterly, 22(3), 354-373. doi: http://dx.doi.org/10.1016/j.giq.2005.05.007

Fountain, J. E. (2001). Building the virtual state : information technology and institutional change: Washington, DC.

Fountain, J. E. (2006). Enacting Technology in Networked Governance: Developmental Processes of Cross-Agency Arrangements. NCDG Working Paper No. 06-003, Paper 16.

Giddens, A. (1990). The consequences of modernity. Cambridge: Polity in association with Blackwell.

Government, T. S. (2009). Den nya skollagen : för kunskap, valfrihet och trygghet. Del 1. (9789138232347). Stockholm : Utbildningsdepartementet, Regeringskansliet : Fritze [distributör], 2009 (Stockholm : Edita Sverige) Retrieved from https://lt.ltag.bibl.liu.se/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=cat00115a&AN=lkp.521337&site=eds-live

http://www.regeringen.se/content/1/c6/12/82/90/322ec0b0.pdf.

Gustafsson, M. (2013). Constructing Security - reflections on the margins of a case study of use of electronic identification in ICT platforms in schools. Paper presented at the The 8th International IFIP Summer School on Privacy and Identity Management for Emerging Services and Technologies, Berg en Dal, the Netherlands.

Hardy, C. A., & Williams, S. P. (2011). Assembling e□government research designs: A transdisciplinary view and interactive approach. Public Administration Review, 71(3), 405-413. doi: 10.1111/j.1540-6210.2011.02361.x

Heeks, R., & Bailur, S. (2007). Analyzing e-government research: Perspectives, philosophies, theories, methods, and practice. Government Information Quarterly, 24(2), 243-265. doi: http://dx.doi.org/10.1016/j.giq.2006.06.005

Jaeger, P. T. (2005). Deliberative democracy and the conceptual foundations of electronic government. Government Information Quarterly, 22(4), 702-719. doi: http://dx.doi.org/10.1016/j.giq.2006.01.012

Kling, R. (2000). Learning About Information Technologies and Social Change: The Contribution of Social Informatics. Information Society, 16(3), 217-232. doi: 10.1080/01972240050133661

Kumlin, S., & Rothstein, B. (2005). Making and breaking social capital: The impact of welfare-state institutions. Comparative Political Studies, 38(4), 339-365. doi: 10.1177/0010414004273203

Digital Agenda för Linköping 2012-2015 (2012).

Luna-Reyes, L. F., & Gil-Garcia, J. R. (2011). Using institutional theory and dynamic simulation to understand complex e-Government phenomena. Government Information Quarterly, 28(3), 329-345. doi: http://dx.doi.org/10.1016/j.giq.2010.08.007

Mayer-Schönberger, V., & Lazer, D. (2007). Governance and information technology [Elektronisk resurs]: from electronic government to information government / edited by Viktor Mayer-Schönberger and David Lazer: Cambridge, MA : MIT Press, c2007.

Melin, U., Axelsson, K., & Söderström, F. (2013). Managing the Development of Secure Identification – Investigating a National e-ID Initiative within a Public e-service Context. Paper presented at the ECIS 2013. European Conference on Information Systems, Utrecht.

Ministry of Enterprise, E. a. C. (2011). ICT for Everyone - A Digital Agenda for Sweden. Stockholm: Government Offices of Sweden.

Nations, U. (2012). E-Government Survey 2012. E-Government for the People. In U. Nations (Ed.). New York

Orlikowski, W. J. (2000). Using Technology and Constituting Structures: A Practice Lens for Studying Technology in Organizations. Organization Science, 11(4), 404-428.

Oscarson, P. (2007). Actual and perceived information systems security. Linköping: Department of Management and Engineering, Linköping University.

Rothstein, B. (2009). Creating Political Legitimacy: Electoral Democracy Versus Quality of Government. American Behavioral Scientist, 53(3), 311-330.

Rothstein, B. O., & Teorell, J. A. N. (2008). What Is Quality of Government? A Theory of Impartial Government Institutions. Governance, 21(2), 165-190. doi: 10.1111/j.1468-0491.2008.00391.x

Scharpf, F. W. (1997). Games Real Actors Play: Actor-centered Institutionalism In Policy Research: Westview Press.

Scharpf, F. W. (2010). Legitimacy in the Multi-level European Polity: Oxford University Press.

SIFO. (2012). Konsumentundersökning om Internetsäkerhet. In PTS-ER-2012:3 (Ed.).

Skolverket. (2013). IT-användning och it-kompetens i skolan. In Skolverket (Ed.), (Vol. 386). Stockholm: Skolverket.

Sweden, S. (2013). Use of computers and the Internet by private persons in 2012. Stockholm.

Söderström, F., & Melin, U. (2012). The Emergence of a National eID Solution – an Actor-Network Perspective. Paper presented at the IRIS 2012. The 35th Information Systems Research Seminar in Scandinavia, Sigtuna, Sweden.

Taylor, J. A., & Lips, A. M. B. (2008). The citizen in the information polity: Exposing the limits of the e-government paradigm. Information Polity: The International Journal of Government & Democracy in the Information Age, 13(3/4), 139-152.

Turkle, S. (2012). Alone Together: Why We Expect More from Technology and Less from Each Other: Basic Books.

Wihlborg, E. (2012). eID (electronic identification) as an Innovation in the Interface of Politics and Technology.

Wihlborg, E. (2014). Legitimate e-Government – Public e-Services as a Facilitator of Political Legitim. Paper presented at the Hawaii International Conference on System Sciences (HICSS), Hawaii.

Municipal Documents

DEXTER. Brochure, un-dated.

eVision och eProgram Linköpings kommun. Adopted by municipal council 2006-12-01.

FRONTER Learning Platform. Brochure, un-dated.

Budgets and final account reports from Linköpings kommun, 2007-2012.

Municipal Digital Agenda – action plan 2012 (In Swedish: Kommunens Digitala Agenda, handlingsplan 2012). Adopted by municipal council 2012-04-05.

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.

SOU 2010:104. E-legitimationsnämnden och Svensk e-legitimation, [The Swedish e-Identification Board and the Swedish e-Identification], Betänkande av Utredningen om bildandet av en e-legitimationsnämnd, Statens offentliga utredningar/ Swedish governmental report on building of the Swedish eIdentification Board.

SOU 2009:86. Strategi för myndigheternas arbete med e-förvaltning, [Strategy for the government agencies' work on eGovernment], Statens offentliga utredningar/ Swedish governmental report, Summary in English available at: http://en.edelegationen.se/sites/default/files/SOU2009_86_Summary_0.pdf

Interviews

I_03.09_f3FK. (2013). FUSe - Framtidens säkra elektroniska identifiering – framväxt och användning av e-legitimationer

I_10.22_LK. (2012). FUSe - Framtidens säkra elektroniska identifiering – framväxt och användning av e-legitimationer

I_11.06_rAT. (2012). FUSe - Framtidens säkra elektroniska identifiering – framväxt och användning av e-legitimationer

I_11.12_LK. (2012). FUSe - Framtidens säkra elektroniska identifiering – framväxt och användning av e-legitimationer

I_11.27_rBR. (2012). FUSe - Framtidens säkra elektroniska identifiering – framväxt och användning av e-legitimationer

I_26.08_fVD. (2013). FUSe - Framtidens säkra elektroniska identifiering – framväxt och användning av e-legitimationer

Focus Groups

FG_10.23_LK. (2012). FUSe - Framtidens säkra elektroniska identifiering – framväxt och användning av e-legitimationer

FG_11.27_eBR. (2012). FUSe - Framtidens säkra elektroniska identifiering – framväxt och användning av e-legitimationer

FG_11.27_lBR. (2012). FUSe - Framtidens säkra elektroniska identifiering – framväxt och användning av e-legitimationer

FG_12.04_eFK. (2012). FUSe - Framtidens säkra elektroniska identifiering – framväxt och användning av e-legitimationer

FG_12.04_lFK. (2012). FUSe - Framtidens säkra elektroniska identifiering – framväxt och användning av e-legitimationer

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.