Constructing Security: Reflections on the Margins of a Case Study of the Use of Electronic Identification in ICT Platforms in Schools

Mariana Gustafsson

Constructing Security: reflections on the margins of a case study of the use of electronic identification in ICT platforms in schools

Mariana S. Gustafsson

Department for Management and Engineering,
Political Science Unit, Linköping University, Sweden
mariana.s.gustafsson@liu.se

Abstract. This paper addresses how people construct meanings regarding "the concept of security", based upon the descriptions collected from participants in a case study of the use of electronic identification in ICT platforms in schools. The aim of the paper is to reflect on the concept of security by identifying and analyzing how people build their own understanding of security when using ICT platforms in schools. The analysis identifies three ontological instances of security: security as an ideal state of affairs, security as a value and information security. The analysis also clarifies the difference between the objective and subjective nature of security, as well as the differences between factual and perceived information security. As a result, I raise several research questions concerning "security", and identify common assumptions with regard to constructing the concept of security.

Keywords: security, ontological, epistemological, construction, meaning, empirical

1 Introduction

Secure identification plays a crucial role in the relations between citizens and public authorities, and it becomes even more important as societies become more complex, integrated and globalized [1]. The process by which societies become increasingly technological and interconnected inherently involves multiple aspects of security [2] owing to the increased use of digital applications and tools [3-5]. The e-government environment is increasingly the forum for interaction between citizens and the state [6]. Identification through digital systems becomes a structural condition when societies build their electronic governments, as well as an issue affecting personal relations that govern daily practices [7-9]. The increasingly digital society within which e-government develops and becomes more integrated into citizens' daily practices raises the need for safe and trustworthy arrangements in relation to the use of ICT.

In a mature welfare state, where citizens express a high level of trust toward the state [10], there is also a high level of interaction between the state and its citizens. As

a result, this type of state experiences increasing demands for more and comprehensive public e-services and an increasing density of interactions between citizens and authorities. The context of the Scandinavian welfare state is interesting for the purpose of analyzing the construction of security in this sense, firstly because there is a high level of basic trust among citizens toward the state and secondly because there are clear policy ambitions to reach an almost complete coverage for e-government.

The use of ICT in education in Sweden has a long history and access to computers among teachers, pupils and parents is constantly increasing, approaching full population coverage, 94 percent in 2012, [11, 12]. A number of school reforms - and notably the new Education Act (2011) - demand increased and systematic reporting of pupils' school progression, which will lead to an increased use of ICT in education administration. In this context, systems for secure log-in and identification become essential and emerge as a commonly used platform within the local citizens - public authorities interaction. In this interaction, essential information, including sensitive information, is transferred among several user groups. The pupil's privacy, autonomy and integrity are ultimately at stake. Teachers, pupils and parents have to communicate on a variety of more or less sensitive issues including the study progression of the pupil, individual assessments and learning goal achievement. Teachers also have to report potentially sensitive data to head teachers, mentors and other administrative authorities. There is a general high demand on the teachers' professionalism and the standardization of pupil assessment tools and procedures in order to maintain a high quality of education and learning target achievement in schools. The use of ICT systems in teaching and in the administration of education is therefore developing rapidly and involving an array of security-related issues.

The aim of the paper is to reflect on the concept of security as the object of study by identifying and analyzing how people build their meaning regarding security when using ICT platforms in schools. In the following text, I present an account of 'security' from a constructivist perspective. I start with a clarification of the research design, where I present some analytical tools and assumptions within the constructivist approach and show how this case opens up to a reflective study. This is followed by a short presentation of the case study on use of ICT platforms in schools, which represents our empirical data source on the margins of which I build my reflections. Then, I engage in a reflective analysis to clarify the concept of security from ontological and epistemological perspectives. The reflective analysis is central in understanding the object of study, constructing further research questions and choosing frameworks for analysis and argumentation [13, 14]. Finally, I close with a few concluding remarks where I ask myself: what was the meaning of the argument, what can be learnt from it, and how can it be used in further research.

2 Research Design

As the title of this paper implies, this is a reflective account on the margins of a qualitative case study on the use of ICT platforms and secure log-in. 'On the margins' means that I engage in reflections on 'the concept of security', dialoguing with the

empirical material from the case study, rather than using it to explain the theory [15]. 'On the margins' also means that I oscillate in my reflective constructions [15] between the theoretical realm and the empirical realm, viewing them as connected to each other. In my reflections, I use different names for the same things depending on whether I use them in the abstract, theoretical sense or in the empirical, practice-related sense. For example, I use in my analysis 'FRONTER-ICT platforms-platforms-technical artifacts' and 'teachers-participants-users-people' interchangeably depending on the level of reflection (i.e. closer to the theory or closer to the empirical material).

A methodological implication of this approach (experienced during the process of analysis) is that, when the analysis lies close to the theoretical realm, it is difficult to pinpoint specific quotes in the interviews and focus groups (as it is required in the conventional qualitative data analysis [16, 17] and expected by the reader). This is due to the fact that there are several complex layers of analysis and interpretation between what was actually said and my reflections on it. To a certain extent, the references used below will not be extracted directly from the raw interview transcripts, but those constructed in the process of dialogue with the empirical data. Reference is then made to the entire interview or focus group. The resulting critique is that the participant and the personal character of the qualitative data disappear when the reflections become more abstract. Apart from that, the analysis is based on a primary and classical structuring and systematization of data in categories (in this case: participants' use of notions, assumptions, functions, attitudes, beliefs and actions on security) and patterns (in this case recurring themes on security), followed by a 'dialogue' with the data using analytical tools from the constructivist approach and the distinction between ontological and epistemological stances. The questions that guide my dialogue with the empirical material are thus: how do people perceive 'security' in the context of their work in school; what is security believed to be, what are the assumptions, the attitudes and the actions involved.

For a more detailed account on the methodology of the empirical case study itself, I am compelled to refer the reader to two other papers that focus to a larger extent on the empirical level [18, 19].

2.1 Short presentation of the case study

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'[1]. We focused both on the municipality administration, which is responsible for education and schooling, and on the platform use at 5 schools. The sample choice was based on a preliminary mapping of the 'history of use' of ICT platforms by all 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 five schools were at compulsory and upper secondary level, one of the schools was a 'free school' publicly-funded but

[1] Project financed by the Swedish Civil Contingencies Agency

run by a private organization. Seven interviews and 9 focus groups, involving forty-four participants (school principals (4), teachers (17), schools' platform administrators (2), pupils (13)[2] and municipality officials - users of platforms (8)) were the main sources of primary data[3]. 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. In addition, local policy documents were analyzed 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.

2.2 The ICT Platforms

In the analysis of the constructions of meaning on 'security', we draw on the empirical findings regarding the use of ICT platforms in schools. The two widely used ICT Platforms in schools are DEXTER and FRONTER, and SKOLA 24, which is used in the free school in our sample. Alternative platforms are not offered by the municipality. The municipality statistics show a constant increase in the use of the platforms, from 338 active users in September 2005 to 6865 active users in September 2012 [18]. The primary schools use the attendance function and the grading function offered by DEXTER. FRONTER is used both as a learning-teaching platform and as an administrative tool for managing work-tasks like pupil documentation (pupils' individual development plans (IUPs) and individual assessment (SOs), goals, portfolio and attendance records), administration and planning. All three platforms provide similar functions in the administration of education. The schools differ in their frequency and range of use of the platforms. FRONTER and SKOLA 24 have been used primarily as learning and teaching tools. They are now being considered for their administrative functionality in schools. As these platforms will be increasingly used in the administration of education, secure log-in solutions to access them are currently being considered. eID is presently considered as the most secure identification tool that can be used to log-in to the platforms.

3 A constructivist perspective and analytical tools

In my reflection on the concept of security, I borrow some analytical tools from Searle's theory on construction of social reality [20]. As a result, I embrace some of the assumptions that he makes concerning sense-making of reality, namely that there is a reality out there that is totally independent of people. According to this theory, people understand social reality – 'social facts' through their purpose for the human activity. For example, 'Cars are for driving, dollars for earning, spending and saving,

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

[3] In the accomplishing stage of this paper, some additional 11 interviews with parents have been carried out, but have not been included in the analysis.

bathtubs for taking a bath' [20]. The reality of everyday life is constantly interpreted by people and presents itself as meaningful to them. Berger and Luckmann differentiate between different spheres of reality, among which, one is chosen to be 'the reality of everyday life' - the reality that is most ordered and most meaningful to the consciousness of the person [21].

3.1 Assignment of function, objectivity, institutional facts

It lies in the human nature, or in our experience of the world, to assign functions to objects or phenomena, 'we do not experience things as material objects, much less as collections of molecules. Rather, we experience a world of chairs and tables, houses and cars, lecture halls, pictures, streets gardens, houses, and so forth' [20]. Sense-making and construction of social reality depends on our concept of objectivity and the difference between objective and subjective. Epistemologically speaking, 'objective' and 'subjective' are primarily predicates of judgment [20]. In the ontological sense, 'objective' and 'subjective' are predicates of entities and types of entities and they ascribe modes of existence [20]. Searle distinguishes between brute and institutional facts. Brute facts exist independently of any human institution, including language. Institutional facts require special human institutions for their existence. Language is one such institution, but there is a whole set of other institutions. I will not focus on the institution of language in this paper. 'Institutional facts' are dependent on collective human agreement or acceptance in contrast to 'brute facts' [20]. It is in these terms that I am interested to study the concept of security and its meaning in the 'reality of everyday life' of people. I proceed to do this by analyzing and interpreting people's understanding of security in connection to their use of the platforms. The concept of security can thus be considered as built on institutional meaning [21] or 'institutional facts' [22], as it is a result of institutional arrangements among people.

3.2 Actual and perceived security

Concurrently, I make use of Oscarson's [23] concepts of actual and perceived information security in order to clarify the distinction itself and generate further reflections on the construction of security as an institutional fact. Actual information security is a factual, objective state of information security in a system, including all aspects of security arrangements [23]. Perceived information security is a subjective interpretation made by a single individual in his or her context and 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. Even events outside one's organization or fields can influence one's perception, for example media representations, rumors, incidents in other organizations [23].

4 An ontologic and epistemologic account on security

The ontology of 'security' in this study is inevitably colored by the people, the schools' organizational set-up, and their actual use of a number of specific ICT platforms in their work. These people are active in the education system, which is within the authority of the state, and have specific roles as pupils, teachers, principals, coordinators, etc. This fact presents both the context and the active environment where, through their work and use of ICT platforms, they form and categorize their perceptions of security based upon their assumptions, beliefs and attitudes with regard to security and technologies in general.

4.1 Security in terms of categories used

Security appears to be a current and relevant issue in the overall workings of the school system, specifically in the public administration of education as a whole. Two aspects appear to be central in the participants' systems of categories, beliefs, assumptions and actions: a) the nature of work in the school that continuously produces a large amount of information about the pupil; and b) the increasing use of electronic platforms for teaching, learning and the administration of pupil data. The security of pupil-related information thus emerges as a central concept in the interviews. Protecting sensitive data about the pupils and ultimately protecting the child is defined as an essential role assumed by the interviewees.

Due to successive reforms in the Swedish school sector, reflected also in the Education Act (2001), teachers are required to document and follow up each pupil in every subject. These legal requirements impose a change in work methods in schools so as to provide SOs for the pupils and thoroughly informed IUPs. Due to the thoroughness and systematic character of the process, the nature of this information is becoming increasingly sensitive, as more and more specific data about the pupil will be documented. Consequently, increasing administrative burden induces the use of ICT in the administration of education in schools. Thus, security implications lie in the potentially sensitive nature of pupil-related information per se and are further complicated by the digitalization of this information through the use of ICT platforms. While the fact that pupil-related information produced in schools is potentially sensitive, being often a gray area, and may lend itself to subjective evaluation is a serious issue, the confusion among the teachers concerning whether SOs and IUPs are subject to the principle of public access to official records is a fundamental problem.

The participants' perceptions of 'security' seem to be rooted in the two aspects described above. This fact explains the categories, the assumptions and the attitudes they have about security in connection to the use of and log-in to the ICT platforms. I intentionally chose to approach 'security' openly and not limit it to 'information security', or 'operational security' or 'individual's security', and thus followed openly the ways in which people expressed their thoughts, attitudes and assumptions by sharing and discussing their experience of using ICT platforms in schools. Based on my interpretation of- and dialogue with the participants' categories, assumptions and attitudes,

I identified three ontological instances of 'security': security as a desired state of affairs, security as a value and information security. Each of these are explained below.

Security as a state of affairs and an aim to be reached.

On a very basic level, security is perceived as a state of affairs or a position that people desire and want to achieve in their organizations [24-27]. Security is in this respect an ideal situation that is intentionally sought and it seems to imply protection of the group and stability in the organization. Analytically, it appeared more relevant to refer to the systems of categories used, the logic of argument and the participants' assumptions rather than specific words, quotations, or categories that they used in the interviews. I observed intentionality in the individuals' understanding of security. This was expressed in their perceptions of what should be done to ensure security, in their emphasis on assuming a careful attitude in handling sensitive information and in their worries regarding negative effects in the eventuality of insecurity within the platform [28-31]. 'If more personal information will be stored there (ed. FRONTER), then it should be made more secure' [25]. 'There are always (ed. security) shortages with everything that is stored on the internet. Things that are too sensitive, that others shouldn't get access to, should not be stored there… Things get more secure apparently, but it is safest outside internet, outside the computer… You wouldn't even notice the intrusion.' [32]. At this fundamental level it is difficult to see any differences between the participants, and the citations presented above show just a glimpse of the entire picture that emerged from the interviews. Intentionality lies in the assumptions of participants, where it is implied that security is something desirable and necessary.

Security as a value.

Again, on a fundamental level, security seems to be a value that is inherent to human activity. The value of protection of the person's integrity, autonomy and privacy seem to be fundamentally connected to the (assumed) virtues of democratic forms of organization. It was expressed, for example, in a focus group with pupils that: 'If the SOs will be more specific, then one needs to have more secure channels to store them… But if somebody gets access to your password and all your stored information, then it is not good' [25]. 'If somebody got access to my logbook (in the platform), then I would be hated in my class' [32]. In the same context, a school principal stated: 'From a security point of view, it feels really good to not need to e-mail things (ed. sensitive information) among us' [28]. A fact that is specific to the organizations in this study is that the subjects of these security concerns are children, who are considered vulnerable per definition and whose protection and security is seen to be at the center of their activity, next to education and socialization. A teacher in an interview described the situation: 'I create a room on FRONTER for the pre-school class where I want to show what we have done in different contexts. I must ask the parents to approve my use of the pictures. Then I have to make sure that those children whose parents didn't approve do not appear there. It's a lot like this today, if we shall film or not the Lucia parade. Unfortunately, we live in a society today where we have to be careful with these things' [30]. Another teacher specified a related aspect: 'Another

question of pupil integrity is when parents get the opportunity to control the child through their access to the school platform, for example when you have honour-related conflicts in the family'. In this sense, security was often perceived in terms of the need to protect children as vulnerable persons, the need to protect and handle carefully sensitive data that could affect a child's integrity, autonomy or privacy. A common assumption that is observed here is that a person's integrity, autonomy and privacy are secured through democratic institutions, where these are part of fundamental human rights.

The category 'sensitive information' was central at this level. Sensitive, but also longitudinal and systematic information about the pupil, as well as work-related assessments on sensitive cases provide critical information that can tragically affect the respective pupil autonomy, integrity and privacy in case of criminal intent and unauthorized use. The participants' experience shows that the area is gray and that there are no clear legal regulations or policies to address this new type of sensitive data produced in schools [26, 29, 30, 33]. The teachers agreed that: 'We are forced to write down a lot of things about the pupils that you assume will not come out. But if an interested person comes and requests that information… She has the right to get them. Just make a copy and take with you' [26] . A school principal pointed that: 'We produce public records that we give to the pupil who can lose them on the bus or store them in a digital system where it can go astray. But this is a public record and we can't write sensitive information in a public record' [29]. Awareness of this gray area and actions to address potential dilemmas also emerged as issues of concern among the participants. Another important issue that emerged from the study, was the participants' increased concern with the potential negative effects of excessive emphasis on security as a value in the e-democracy and electronic public administration, namely, with its tendency to result in overprotection and intrusion into personal privacy that could lead to control and surveillance of individuals [30, 34, 35].

Information security.

This is not a fundamental perception that is placed at the level of the two presented above. It is however obvious in our case that both the users and the schools are affected by the use of technical artifacts, in this case ICT platforms. Our participants need to use technical artifacts to manage their work and studies. They regard the platforms as tools to be used to achieve their primary goals of education and socialization. A school principal (backed by another principal in a different interview) emphasized that 'There is a tendency in the data system to impose requirements on how one should work. If it appears that FRONTER does not have the needed adaptability and presents too many demands to change the way we work, we will not use it or will use it sparely. We want a tool that fits our work and not vice-versa' [33]. They are also aware of the security risks involved with using electronic artifacts [26, 27, 30, 31, 33, 35]. The vocabulary and arguments used in this sense are more specific and have a clear message. At this level, there are plenty of concerns regarding operational security, secure log-in and advanced identification tools such as eID, privacy, unauthorized information access and differentiated information display, operability of the platforms, security risks, ownership of information, etc. These concerns are expressed

specifically by the camp comprised of IT coordinators, municipality officials and municipality system administrators, and even some FRONTER administrators in schools [24, 26, 27, 29, 31, 33-36].

As for the camp that represents the school system – principals and teachers, I observed a distance from the technicalities connected with security aspects of the ICT platforms that they use. It is either assumed among the principals that the platforms administered by the municipality meet the security requirements: 'I don't have that background and knowledge, I must rely on those who we buy the service from that they will take care of security' [28], or it is argued that the specific platform supposed to store and manage pupils IUPs and SOs, FRONTER, is not secure enough to contain sensitive information. Security risks and the reliability of the artifact belong to this discussion [24, 26, 27, 29, 31, 33-36]. As more and more sensitive information (pupil profiling) will be administered through more and more advanced ICT platforms, increasingly high demands will be placed both on the technical artifact itself and on the users of the artifact, i.e. teachers, pupils and parents. The platforms will have to meet high security requirements and will, at the same time, have to be simple and lend themselves to intuitive use, as expressed by the users: 'As more systematic and specific information will be shared at all levels..., it is important that sensitive information stays on the right side of the threshold… It will require the system to manage different types of information and at the same time be easy and functional for the different and frequent users' [27]. The users who will get administrative rights to change the content of the platform and even develop it through use will have a high burden of responsibility to manage sensitive pupil data accordingly. 'Responsibility' was thus another central category that fueled the participants' perceptions and assumptions with regard to achieving security through the use of ICT platforms in schools [28-31, 33, 37].

4.2 How do people construct security?

Once I de-construct 'security' and conclude that at the fundamental level security is an ideal state of affairs that people intentionally strive to achieve and to which people assign a fundamental value, I proceed to reconstruct the concept of security based on the participants' categories, attitudes, actions and rules pertaining to their use of ICT platforms in schools. The analysis below engages in ontological and epistemological rationalizations regarding the concept of security based primarily on some of J. R. Searle's concepts and analytical tools pertaining to the process of constructing social reality. Clarifying the ontological and epistemological stances in approaching 'security' as the object of study is an important platform, upon which interesting, non-evident research questions can be constructed or theories built [13, 15]. While doing this, I try to keep the focus on- and correlate between the three ontological instances of security, i.e. security as an ideal state of affairs, security as a value and information security.

As discussed above, security exists at least in three different instances and the first question to ask is what kind of entity is security – is it something that is 'out there'

independent of human perception, something like the rocks or the sun or is it something that exists only because we have created it and once the last human perishes it disappears from existence. That is to ask whether security has an objective or a subjective existence in the first place. It seems that security is both, based on an important distinction between ontological and epistemological stances that Searle helps clarify [22]. In the ontological sense, i.e. as a form of existence, security at the most fundamental level seems to be an entity dependent on the fact that people feel it, desire it and need it. That means that without people, security does not exist. In contrast, without people the sun or the rocks would exist; that makes them ontologically objective entities or facts. Therefore in ontological terms security is always subjective.

An interesting thing happens when I take the epistemological stance. That is, to judge whether security is a subjective or an objective fact. Through sense-making and judgment people make true or false statements about security. The truth and falsity of the judgments on security appear to depend on the attitudes, beliefs, and assumptions of the same or other people. Thus, from the epistemological point of view, security is subjective, but only *to a certain degree* [22]. Namely, if the same subjective judgment on security is made by a large part or an entire group of people, then this subjective judgment will objectivize the object of judgment, which is security in this case. From the epistemological perspective, I can thus say that security as an ideal state of affairs and security as a value presents objective judgments or objective facts (using Searle's terms) that are independent of individual attitudes, beliefs and feelings. The objectivized judgment about security (that needs further reflection) will thus be that regardless of individual culture, organizations, religions or beliefs, security in terms of protection and stability (i.e. security as a state of affairs and a value) is something that people need in order to live.

4.3 Perceived and factual security

What about information security, i.e. the third ontological instance identified in this case? Also from an epistemological perspective, I concentrate on the factual security and perceived security suggested by Oscarson [23] in his analysis of security of information systems. Factual security in this sense is the totality of people's judgments on whether an information system is secure, thus making it an objective fact. However, what I find in our case, when it comes to ICT platforms, people consider themselves as not having enough technical knowledge of FRONTER or other platforms in order to judge how secure they actually are [26, 29, 34, 35, 37]. There is thus a variety of judgments on the security of the platforms based mainly on the participants' actual use of these platforms in school, i.e. based on how they function, as well as on their beliefs and attitudes toward information technology in general.

The perceived security of the platforms is thus based on the people's experience and knowledge of them though practical use. And their experience as users shows clearly that the platforms are perceived as not secure [26, 29, 30, 33, 35, 37]. An epistemological question arises regarding what kind of knowledge and how much knowledge is needed so that a judgment on the security of an information system is

objectivized? Lack of technical knowledge among the users of the platforms (all our participants are users of the platforms) appears, in our case, to be substituted with reliance on the authorities' (i.e. the municipality) knowledge and responsibility to ensure the security of ICT platforms. 'The municipality is considering a tool for digitalizing sensitive information. Then I assume that they have taken the responsibility to ensure that there is a sufficient level of security in it. This means some form of two-step log-in [29]', a school principal said. This substitution of knowledge seems to be enough for at least some of the users in order to assume that the platforms are secure [26, 29, 30, 33, 35, 37]. This substitution also implies trust in the authorities and their role in ensuring the security of the platforms.

However, this substitution does not seem to be sufficient to provide a base for all the users to judge the platforms as secure, since there are grounds to question whether the authorities indeed have the knowledge or take the responsibility to ensure the security of the platforms. This is also the case in our empirical study [29, 30, 37]. The question is then: when there is a perceived lack of technical knowledge about the platforms among the users, can they objectivize their judgments on the security of the platforms through mere use of the platform? The assumption would be that, if people use the platform long enough to see it function securely, they will eventually objectivize their judgment about it and perceive it as secure, i.e. achieve factual security. However, testing this assumption appears problematic as the ICT platforms' lives (and existence) are short, which means that in practice there will never be enough time to gather enough knowledge and experience enough use in order to objectivize a judgment on their security.

The next interesting question is then: can people, through their practical use of different technical artifacts, over time objectivize their judgments – and thus arrive at (construct) objective facts – regarding the security of these technical artifacts? Or, considering the fact (and this seems indeed to be an objectivized judgment) that all the information technology in the internet age involves security risks of different natures (and existences), security through technical artifacts is not possible in the epistemological sense. Furthermore, I may continue this thought and argue that through the perceived and actual security risks that are connected to technology, there is a possibility that information technologies can endanger the first two ontological (and fundamental) instances of security - i.e. security as a value and security as an ideal state of affairs.

5 Concluding remarks and further research

What can then be concluded from these arguable accounts on security? Where and how can I use them? Where did they bring me? Have I brought you anywhere? Looking back at them, these are reflections on the nature of security driven by curiosity to learn about- and understand 'security' as object of research. I oscillate between different levels of abstraction and keep my case study in one hand (and Searle's book in the other), in order to keep me on the ground.

Making a difference between ontological and epistemological natures of objects is fundamental in understanding what I am studying. Through these accounts I have clarified some basic questions that need to be asked before building more meaning and argument about them through academic endeavors. The study presents some value for the information systems research by reflecting on the difference between factual and perceived security using the ontological and epistemological stances, opening thus further questions, such as - what kind of knowledge and how much knowledge is needed so that a judgment on security of an information system is objectivized; can people through their practical use of different technical artifacts over time objectivize their judgments in order to arrive to (construct) objective facts of security, is security possible to achieve through use of technical artifacts. The study presents also a contribution to the e-government research in terms of approaching security as an issue of e-government developing and integrating into citizens' daily lives. The study opens for further reflection on institutional arrangements, such as eID, that are currently created in the context of e-government.

References

1. Giddens, A., *The consequences of modernity*. 1990, Cambridge: Polity in association with Blackwell.
2. Beck, U. and M. Ritter, *Risk society : towards a new modernity*. Theory, culture & society (London), 99-0948605-9. 1992, London: Sage.
3. Castells, M., *The information age : economy, society and culture. Vol. 1, The rise of the network society / Manuel Castells*. 1996, Malden, Mass.: Blackwell.
4. Castells, M., *The information age : economy, society and culture. Vol. 2, The power of identity*. 1997, Malden, Mass.: Blackwell.
5. Castells, M., *Communication power*. 2011, Oxford: Oxford Univ. Press.
6. Heeks, R. and S. Bailur, *Analyzing e-government research: Perspectives, philosophies, theories, methods, and practice*. Government Information Quarterly, 2007. **24**(2): p. 243-265.
7. Axelsson, K., U. Melin, and I. Lindgren, *Public e-services for agency efficiency and citizen benefit-Findings from a stakeholder centered analysis*. Government Information Quarterly, 2013. **30**(1): p. 10-22.
8. Melin, U., K. Axelsson, and F. Söderström, *Managing the Development of Secure Identification – Investigating a National e-ID Initiative within a Public e-service Context*, in *ECIS 2013. European Conference on Information Systems*. 2013: Utrecht.
9. Wihlborg, E., *eID (electronic identification) as an Innovation in the Interface of Politics and Technology*, U. Symposium, Editor. 2012.
10. Rothstein, B., *Creating Political Legitimacy: Electoral Democracy Versus Quality of Government*. American Behavioral Scientist, 2009. **53**(3): p. 311-330.
11. Skolverket, *IT-användning och it-kompetens i skolan*, Skolverket, Editor. 2013, Skolverket: Stockholm.
12. Sweden, S., *Use of computers and the Internet by private persons in 2012*. 2013: Stockholm.
13. Alvesson, M. and J. Sandberg, *Constructing research questions : doing interesting research / Mats Alvesson, Jörgen Sandberg*. 2013: London : SAGE, 2013.
14. Alvesson, M. and J. Sandberg, *GENERATING RESEARCH QUESTIONS THROUGH PROBLEMATIZATION*. Academy of Management Review, 2011. **36**(2): p. 247-271.

15. Alvesson, M. and D. Kärreman, *Qualitative research and theory development : mystery as method / Mats Alvesson, Dan Kärreman*. 2011: Thousand Oaks, CA : Sage Publications, 2011.
16. Bryman, A., *Social research methods / Alan Bryman*. 2012: Oxford : Oxford University Press, 2012 4. ed.
17. Creswell, J.W. and J.W. Creswell, *Qualitative inquiry and research design : choosing among five approaches / John W. Creswell*. 2013: Thousand Oaks : SAGE Publications, c2013. 3rd ed.
18. Gustafsson, M. and E. Wihlborg *Organizing safe on-line interaction and trust in governmental services. A case study of identification channels for public e-services in schools*. JeDEM. The eJournal of eDemocracy and Open Government, 2013.
19. Wihlborg, E. and M. Gustafsson, *Electronic identification in practice – a case study of the use and organization of eID in public e-services in schools*, in *SWEG 2013. 10th Scandinavian Workshop on E-government*. 2013: Oslo.
20. Searle, J.R., *The construction of social reality / John R. Searle*. 1996: London : Penguin, 1996.
21. Berger, P.L. and T. Luckmann, *The social construction of reality : a treatise in the sociology of knowledge*. 1966, Garden City, N.Y.: Doubleday.
22. Searle, J.R., *The construction of social reality*. 1995, New York: Free Press.
23. Oscarson, P., *Actual and perceived information systems security*. Linköping studies in arts and science, 0282-9800 ; 412. 2007, Linköping: Department of Management and Engineering, Linköping University.
24. FG_10.23_LK, *FUSe - Framtidens säkra elektroniska identifiering – framväxt och användning av e-legitimationer* L. Universitet, Editor. 2012.
25. FG_11.27_eBR, *FUSe - Framtidens säkra elektroniska identifiering – framväxt och användning av e-legitimationer* L. universitet, Editor. 2012.
26. FG_11.27_lBR, *FUSe - Framtidens säkra elektroniska identifiering – framväxt och användning av e-legitimationer* L. universitet, Editor. 2012.
27. I_10.22_LK, *FUSe - Framtidens säkra elektroniska identifiering – framväxt och användning av e-legitimationer* L. Universitet, Editor. 2012.
28. I_11.14_rBJ, *FUSe - Framtidens säkra elektroniska identifiering – framväxt och användning av e-legitimationer* L. universitet, Editor. 2012.
29. I_11.27_rBR, *FUSe - Framtidens säkra elektroniska identifiering – framväxt och användning av e-legitimationer* L. universitet, Editor. 2012.
30. I_12.04_FFK, *FUSe - Framtidens säkra elektroniska identifiering – framväxt och användning av e-legitimationer* L. universitet, Editor. 2012.
31. I_12.05_rFK, *FUSe - Framtidens säkra elektroniska identifiering – framväxt och användning av e-legitimationer* L. universitet, Editor. 2012.
32. FG_12.04_eFK, *FUSe - Framtidens säkra elektroniska identifiering – framväxt och användning av e-legitimationer* L. universitet, Editor. 2012.
33. I_11.06_rAT, *FUSe - Framtidens säkra elektroniska identifiering – framväxt och användning av e-legitimationer* L. universitet, Editor. 2012.
34. FG_11.14_lBJ, *FUSe - Framtidens säkra elektroniska identifiering – framväxt och användning av e-legitimationer* L. universitet, Editor. 2012.
35. FG_12.04_lFK, *FUSe - Framtidens säkra elektroniska identifiering – framväxt och användning av e-legitimationer* L. universitet, Editor. 2012.
36. I_11.12_LK, *FUSe - Framtidens säkra elektroniska identifiering – framväxt och användning av e-legitimationer* L. universitet, Editor. 2012.
37. FG_11.05_lAT, *FUSe - Framtidens säkra elektroniska identifiering – framväxt och användning av e-legitimationer* L. universitet, Editor. 2012.