Electronic Identification as an Enabling or Obstructive force
The general public’s use and reflections on the Swedish e-ID

Author: Annie Göransson
Supervisor: Behrooz Golshan
Examiner: Päivi Jokela
Date: 2018-06-01
Course code: 5IK50E, 30 credits
Subject: Informatics
Level: Master Thesis
Department of Informatics
Abstract
This thesis is an exploration of the general public's use and reflections on electronic identification (e-ID) tokens, in Sweden. Based on the researcher’s own experiences, the aim was to understand how the current e-ID scheme was enabling or obstructing the interaction with public agencies, etcetera. The thesis has a qualitative research design and is situated within the interpretivist paradigm. The data was collected through semi-structured interviews and the analysis of three documents, published by three different public agencies in Sweden. The data was analyzed through the vehicle of thematic analysis, which engendered four themes. These were 1. e-ID definitions, 2. the personal identity number as enabler and obstruction, 3. banks as the major e-ID issuer in Sweden and 4. security, skepticism and trust. The findings indicated that the e-ID was associated with convenience and security risks, which were brought up by the interviewees as well as the analyzed public reports. Furthermore, one of the public reports argued that the e-ID should be separated from the notion of having authority, through re-baptizing the Swedish term for e-ID, in Swedish 'e-legitimation' to electronic identity document ('elektronisk identitetshandling' in Swedish).

Keywords
electronic identification, BankID, frauds, personal identity number, convenience, trust, skepticism, security, general public
Table of contents

Abstract........................................................................................................................................ i
List of tables and figures.................................................................................................................. iii

1 Introduction .................................................................................................................................. 1
1.1 Background ............................................................................................................................. 1
1.2 Motivation ............................................................................................................................... 3
1.3 Purpose and Research Questions ............................................................................................ 5
1.4 Scope and Limitations ............................................................................................................. 5
1.5 Outline structure ..................................................................................................................... 6

2 Literature review ....................................................................................................................... 8
2.1 Defining electronic identification ......................................................................................... 8
2.2 Scientific literature about e-IDs .......................................................................................... 10
2.3 Conclusion of literature review ........................................................................................... 17

3 Methodology ............................................................................................................................. 19
3.1 Research Paradigm ............................................................................................................... 19
3.2 Data Collection ..................................................................................................................... 20
3.3 Data Analysis ......................................................................................................................... 25
3.4 Establishing trustworthiness ................................................................................................. 28
3.5 Ethical Considerations ......................................................................................................... 29

4 Empirical findings ..................................................................................................................... 31
4.1 Theme 1: Definitions of the e-ID .......................................................................................... 31
4.2 Theme 2: The personal identity number as a precondition and obstruction ......................... 33
4.3 Theme 3: Banks as the main issuers of e-IDs ...................................................................... 34
4.4 Theme 4: The security aspect, trust and skepticism ............................................................. 36

5 Discussion ................................................................................................................................ 40
5.1 Interpretations of the e-ID ..................................................................................................... 40
5.2 People's trust in societal institutions .................................................................................... 41
5.3 The personal identity number as an enabler and obstruction ............................................. 43
5.4 Security and skepticism ...................................................................................................... 43

6 Conclusion ................................................................................................................................. 45
6.1 Conclusions ......................................................................................................................... 45
6.2 Contribution ........................................................................................................................ 45
6.3 Future Research .................................................................................................................. 46

7 References ................................................................................................................................. 47

Appendices .................................................................................................................................... 53
Appendix A - Informed consent form (in Swedish and English) .................................................. 53
Appendix B - Interview guide non-e-ID users (in Swedish and English) ..................................... 56
Appendix C - Interview guide e-ID users (in Swedish and English) ............................................ 57
Appendix D - Interview guide Anders Henriksson (in Swedish and English) .............................. 58
List of tables

Table 1. 9
Table 2  18
Table 3  22
Table 4  22
Table 5  24
Table 6  26
Table 7  26
Table 8  28
Table 9  29

List of figures

Figure 1  7
Figure 2  39
Figure 3  40
1 Introduction

In Sweden people are increasingly choosing to adopt and use electronic identification systems of varying kinds. E-ID tokens are used for identifying and signing digitally in matters related to the bank, public agencies, payments, etcetera. In Sweden, the adoption and use of the banks’ e-ID solution (BankID) is solid and it became exceedingly popular as the real time payment system Swish was launched in 2012 (Eaton, Hedman, and Medaglia, 2017). On the surface, e-ID tokens may seem unproblematic or as useful enablers. However, my own experiences from working on a BankID issuing bank challenges this interpretation.

Below the history of electronic identification in Sweden is succinctly presented. After this historical review, the motives for choosing the topic are presented. This is followed by the thesis’ purpose and research questions. Lastly the thesis’ scope and limitations are conveyed.

1.1 Background

In Sweden, the population has been nationally registered since the 17th century. The foundation to public agencies’ administration is the personal identity number. This number consists of ten to twelve digits, with the first six to eight digits indicating date of birth and the rest indicating geographical area, as well as gender. Further, the personal identity number is issued to both native Swedes and immigrants (who are registered in the population register) by the tax agency. The personal identity number is used within both the public sector and the private sector. This number is the identifier in the Swedish e-ID solutions. Those who are residing temporarily in Sweden (up to a year) will instead of receiving a personal identity number, get a unique (coordination) number, which is also issued by the Swedish tax agency (Söderström, 2016; Skatteverket.se, 2018).

The developing of e-IDs began in the middle of 1990s, a process facilitated by the organized population registration system, which was well established. By this time, nearly every person living in Sweden had a personal identity number. The public agencies in Sweden had a well-functioning back-office administration and there was an ambience of acceptance in society towards being put in a population record. Although the public agencies had a large and stable administration, identity documents such as ID cards were to some extent issued by private institutions, for instance by Swedish banks (Grönlund, 2010).

In the year of 2001, Sweden held the presidency of the European Union. By this time, public agencies were considering making their services available around the clock for citizens, an idea being conceptualized as the ‘24-hour agency’, where increased interactivity with the citizens was one of the objectives (Söderström, 2016). Simultaneously, electronic signatures were given the same status as written signatures by the European union. It was against this background that the Swedish e-ID scheme began to materialize. The plan was from the very beginning to have a market solution and thus letting Swedish banks be the identity providers, since they had a large volume of customers. The government’s responsibility was to govern through legislation and requirements in procurements, known in Sweden as ‘frame agreements’ (Melin, Axelsson and Söderström, 2016). Grönlund (2010) argued that apart from the fact that banks had many customers, the economic argument was emphasized by the government. Further, the market governance of e-IDs was framed as prosperous, since it would create competition between private sector e-ID providers and thereby minimize the costs (which were transaction based). Another argument, which was appealing to bank customers, was that the acquisition and use of the banks’ e-identification tokens were free of charge. The trust people had particularly in the
banking system, was also stressed as an important variable in choosing banks as the e-ID issuers (Grönlund, 2010; BankID.com, 2018).

Östgöta Enskilda bank announced in November 1996 that they had created an internet bank, through which the bank’s customers could pay their bills and transfer money between their accounts (Eaton, Hedman, and Medaglia, 2017). Within the next 400 days, all the major Swedish banks had launched their own internet banks. Further, banks (i.e. Danske Bank, Handelsbanken, Ikano Bank, Länsförsäkringar Bank, SEB, Skandiabanken and Swedbank) built a consortium and formed a company in September 2002, named Financial ID-Teknik BID AB, which became the certificate authority and the e-ID issuing banks consequently became the identity providers (Eaton, Hedman, and Medaglia, 2017; Bankid.com, 2018; Söderström, 2016). In 2003, the banks began issuing so-called BankIDs to their customers. The first customer who used a BankID was a customer in Skandiabanken and this person used the BankID to sign with, in a change of address (via the tax agency). By the end of 2003, over 100,000 people used the BankID. In 2005, BankID had 500,000 users in Sweden. Two years after that (in 2007), a survey showed that 95 % of the Swedish population was familiar with BankID (Bankid.com, 2018). Further, the e-ID solutions offered by the banks could be described as soft and hard, with BankID available either as a downloadable file (soft), which could be moved between computers, and the other alternative being a plastic card with a chip on it (hard). Several years after launching the e-ID on file and plastic card, BankID was introduced on mobile (in 2010). In this project, the mobile operators Telenor and TeliaSonera were involved, since the BankID was placed on the mobile telephone’s SIM-card. However, this solution was phased out and replaced with the mobile BankID, which was introduced in June 2011. In 2017, 90 % of those possessing a smart phone used the mobile BankID and the growth of use has for several years been 10 % a year. The use is distributed across all age groups who qualify for having an e-ID. Most frequent is the use among people who are between the ages of 26 and 35, with 96 % of those owning a smart phone using a mobile BankID (Davidsson and Thoresson, 2017). As the BankID use has been steadily rising, more banks have joined and begun to issue (mobile) BankIDs, some of them being Icabanken, and Nordea (Bankid.com, 2018).

Several governmental agencies have been given the commission of developing a national e-ID scheme and they have since the early 2000s been running multiple projects. What has characterized these projects is that the leadership has shifted between different public agencies such as the Swedish Agency for Public Management and the now closed down public agency of Verva. Although the designated project leaders have varied throughout the years, the tax agency and the social insurance agency have always been highly involved in the projects, since most transactions have occurred within these two public agencies (Grönlund, 2010). Further, the projects have been the following: SAMSET (2000-2003), E-Board (2003-2005), 24th Delegation (2003-2006), Verva (2006-2008), E-Government Delegation (2009-2015) and the e-ID Board (2011-). In these projects the issues have been, for instance, to define electronic identification, develop guidelines, stimulate public sector use of e-identification, secure exchanges of information, strengthen e-government and make technical infrastructure suggestions (Grönlund, 2010; Söderström, 2016). After having dealt with a number of issues in different constellations, the e-ID Board was formed and given the commission of centrally coordinating and supporting secure e-identification and e-signing, essentially for the purpose of enhancing the e-government. Moreover, the e-ID Board’s main mission has been to develop an updated Swedish e-ID model (in Swedish ‘Svensk e-legitimation’). This has been a challenge, as different variables such as time constraints, technical, commercial and legal issues have been causing more work than was initially anticipated. Further, the e-ID solution in
Sweden is a federated solution and the role of the e-ID Board is considered to be a central node. Those issuing e-IDs in Sweden must follow the requirements known as trust frameworks, that the e-ID Board has developed (Grönlund, 2010).

Apart from BankID, there are and have been additional efforts in providing electronic identities, from agencies as well as from the private sector. The tax agency started offering e-IDs on their identity cards in 2009, making it possible for non-citizens (who were registered in the population register) to carry an e-ID. The age limit for this e-ID token was 13 years. The e-ID was originally from the network operator Telia, but since 2017 it is Svenska Pass who provides the e-ID (Skatteverket.se, 2018). The Swedish network operator Telia is also an e-ID issuer, offering e-IDs on card, both to private customers and companies (Telia.se, 2018). Verisec’s e-ID solution Freja eID was launched in 2017. This e-ID offers electronic identification on several trust levels. Freja eID is marketed as more secure than BankID, with a mobile application protection against intrusions of different kinds, such as injections of malwares. Moreover, Freja eID is alternating the personal identity number, which is the classic identifier in Swedish e-IDs. The company which owns Freja eID questions the personal identity number as the only identifier, with the motivation that this number should not be stored in e-commerce companies’ databases (Verisec.com, 2017; E.J, 2018).

1.2 Motivation

The interest for this subject began in 2017 when I was employed on a Swedish bank which issued BankIDs. During my employment, my understanding was that banks served their customers with BankIDs for the sole purpose of internet banking. That is why I began to question the citizen-bank-government relation, since people had to go through the private sector (mainly banks) to access public agencies’ web-based services. I met bank customers who were disappointed over the fact that they had got requests from public agencies to start identifying themselves electronically, in order to manage different issues such as claiming tax refunds. Previously, this had been solved through filling in forms. By this time, I started wondering how the technically sceptic or inexperienced part of the population would, in the future, work their way around electronic identifying and signing, which have “lock-in” effects (Melin, Axelsson and Söderström, 2016).

It was brought to my attention during the fall of 2017 that there was a large number of mobile BankID frauds in Sweden, which had been occurring and accelerating during the last couple of years (with several people a day being targeted in mid-December of 2017). Bank customers, particularly older men living in affluent neighborhoods, had been victims of the frauds and their bank accounts had been emptied (Thelocal.se, 2018). These frauds occurred without any advanced hacker techniques, but instead these calculating and well-orchestrated attacks used for instance the technique of caller ID spoofing, i.e. when a person (with a malicious agenda) is calling from a telephone number resembling for instance the police’ or the bank’s telephone number (Lotsson, 2018). One Swedish police detective investigating the BankID frauds referred to the BankID as the “devil’s invention” (Johansson, 2018, p.6). According to the public service television station, SVT, the BankID deceivers may have made over 50 million Swedish crowns (approximately 4.7 million Euro) in six months until April 2018 (SVT Nyheter, 2018). There have been slight differences in the deceptive strategies, but one of them is calling a person via telephone and claiming to be working for the Swedish police agency. The targeted victim is alerted by the deceiver that someone has been hacking his or her bank account. After this, the victim is informed that his or her bank will call him or her up a while after the first telephone call. Thereafter, another person calls and is claiming to be a bank employee from the victim’s
The alleged bank employee encourages the victim to open his or her mobile BankID app for logging in to the internet bank. The deceiver has via his or her own computer by now already typed in the victim’s personal identity number in the field where it is supposed to be and clicked on the “login” button before the victim has had a chance to press it him- or herself (directly after the password was typed in the mobile BankID app). On the victim’s smart phone an error message surfaces. To empty the accounts, the deceiver needs the mobile BankID to be used one more time and the victim is instructed to press the password again to achieve the login (to the internet bank). After this instruction has been followed, lifelong savings have disappeared for a considerable number of people. One daughter to a deceived mother questioned the system as whether people are supposed to be proficient in security and technical issues, so that this crime never would occur. Further she claimed that her mother would have been helped if she was robbed on the street, but in this case, she was not helped or compensated by her bank (SEB), her insurance company or from the National Board for Consumer Disputes (ARN). This wave of BankID attacks would eventually, as the daughter predicted, end up with people putting their money under their mattresses instead of being increasingly digital (Aftonbladet, 2018). Shortly before the thesis was submitted, the local newspaper, SMP, published a news article stating that the BankID frauds and the bank’s responsibilities and potential compensation will be audited by ARN in May, 2018 (Cato, 2018). Further, it was revealed in the article that for instance one individual with 40 years of experiences as a bank employee had been deceived, among many other people. What was also noticed shortly before the thesis deadline, was an article which conveyed that Finansiell ID-Teknik Bid AB are with an application update trying to combat the BankID frauds through encouraging their users to share their location on their mobile devices (Nilsson, 2018). Moreover, the article had an embedded survey of whether the readers used a BankID. After 1117 votes were registered, the result was that 4 % did not, 17 % did and thought it was a fantastic system, 4 % did without any opinion about it and overwhelmingly 74 % had chosen the alternative of “yes, against my will”.

At my workplace I helped many customers manage their internet bank applications. We as bank employees became their technical support and helped them with finalizing account registrations on their smart phones and downloading mobile applications. We helped customers type in the requested information into the different applications, and so on. There was, to the best of my recollection, sometimes an ambience of confusion and resentment in the bank office. The Swedish librarians’ trade union, DIK, has also reacted towards being the IT support of those needing to acquire and use e-IDs, arguing that this is a notable shift of responsibility. Librarians have to help people with acquiring e-IDs, paying invoices and filling in different forms. The reason for this is said to be that the offices of public agencies and banks are closing down rapidly, because of digitalization (SVT Nyheter, 2018).

During my bank employment, I also observed that the BankID was shared among family members during the acquisition phase, with for instance the husband holding his wife’s telephone and requesting to manage the whole procedure of the BankID acquisition. This was strictly forbidden, as the e-ID token from the bank’s point of view was considered to be a valuable document (i.e. as a regular ID card), which is not meant to be shared with family members or friends. This was sometimes experienced as problematic, as most of the individuals who wanted to manage the acquisition for their family member asserted that it was merely to help out with a somewhat difficult task.
1.3 Purpose and Research Questions

In this day and age, when public agencies in the name of “eGovernment” are increasingly digitalizing their operations, people become more or less obliged to begin identifying themselves electronically. The efforts of bringing in more market actors into the marketplace as e-ID issuers are not ebbing away. However, there seems to have been some kind of ambiguity from the governmental side. Although the public agencies request from people that they should use e-IDs to access their e-services, their own e-ID issuing is marginal. The quote below conveys the vagueness in the Sweden’s e-ID scheme, as it was perceived in 2016.

“The future e-ID solution is still heavily dependent on the market actors, i.e. the banks, still being willing to support the national e-ID. As far as we have seen, a scenario where the banks are opting out of the e-ID scene has not been accounted for by the e-ID Board, but still is a possible outcome because of development costs and a potentially less profitable business model.” (Melin, Axelsson and Söderström, 2016, p. 90)

As the current e-ID scheme in Sweden is dominated by Swedish banks and premised on the general public’s willingness to acquire e-IDs in order to interact with public agencies, the objective of this thesis was thus to find out more about the general public’s reflections and use in relation to electronic identification tokens. Further, the purpose was to better understand how the current e-ID scheme is enabling or obstructing people, through their reflections and use of the current e-ID supply.

The research questions are:

1. How does the general public interpret electronic identification in terms of their use and reflections?

2. In what ways does electronic identification enable or obstruct when the general public use their e-ID tokens?

1.4 Scope and Limitations

The general public’s expressions of confusion, resentment or optimism for that matter in relation to electronic identification is an issue that needs to be more thoroughly explored. Is the e-ID token to be taken for granted and conceived as something unproblematic, or as a mere back-office enabler (Melin, Axelsson and Söderström, 2016)? Or, could it be regarded as a symbol for dissension? The studies done on user perceptions in the field have been preoccupied with implementation and adoption of e-IDs in workplaces. Further, they have mostly been targeting employees in the public sector, such as nurses, teachers, politicians and so on. I attempted with my thesis to find out more about e-identification, which is used by millions of residents in Sweden and hence make an empirical contribution through the targeting of the general public.

The issue of electronic identification has been presented through many technical terms and related suggestions. However, this study will not contain any detailed accounts of the technical
facets of e-identification, because it would be out of the scope of this this, which has the objective of mapping out people’s use and reflections of electronic identification.

This thesis has its base in Sweden and therefor the generalizability to other countries may be limited. In Sweden, the banks’ solution BankID is the solution mainly used by private persons, in contrast to for instance the tax agency’s e-ID solution. However, the academic literature included in this study has been published in many different countries and creates together with my results a conceptualization, which may be applicable to other contexts beyond Sweden.

1.5 Outline structure

Chapter 1. Introduction

In the first chapter the background of e-identification, motivation for the chosen topic, research purpose and research questions as well as scope and limitations were presented.

Chapter 2. Literature review

The literature review was divided in two main sections, the first being e-ID definitions and the other one being the literature review as such. Further, the literature review was split into three aspects, that is technical, legal and social aspects. Each aspect contains a variety of different topical subjects being presented in scientific articles centered around electronic identification.

Chapter 3. Methodology

In this chapter the methodological decisions, which have been made, are described. First the design of the study is explained. After this, the thesis is situated within a paradigm. Then, I describe the data collection, data analysis, the thesis’ trustworthiness and lastly, ethical considerations.

Chapter 4. Empirical findings

In chapter 4, the empirical findings (based on interview and document data) are presented through the vehicle of thematic analysis. This chapter contains four broad patterns (themes) observed during the data analysis. They are: Definitions of the e-ID, The personal identity number as a precondition and obstruction, Banks as the main issuers of e-IDs and The security aspect, trust and skepticism.

Chapter 5. Discussion

The discussion is based on the four concepts defining the e-ID by Söderström (2016), as well as the topical discussions found in the scientific articles about e-IDs. Further, these theoretical elements are compared to the findings presented in chapter 4.
Chapter 6. Conclusion

The last chapter is divided in three headings where I succinctly answer my research questions. Further, the contribution of this study is explained and lastly, my ideas of future research is shared.

Figure 1. The disposition of the thesis is shown in the process flow above.
2 Literature review

The e-ID token is the object needed in order to access (from the public protected) web-based services offered by the private sector, e.g. Internet banking, or the governmental sector, e.g. filing taxes or applying for financial support (Söderström, 2016). In Sweden, electronic identification has rapidly become integrated into the population’s lives, with an exponential growth in adoption and use, since the introduction of mobile BankID, in 2011. The use of mobile BankIDs among adults in Sweden has more than doubled from 34 % users in 2014 to 73 % users in 2017 (Davidsson and Thoresson, 2017).

This chapter has been divided into two sections. First, I attempt to bring clarity in how electronic identification is conceived in this study, because there is no consensus reached in the academic community regarding what constitutes electronic identification (Söderström, 2016). This description will be more conceptual in nature. Secondly, I present common elements found in the body of scientific literature, which is focused on electronic identification. The reviewed body of literature is further divided into the subsets of technical aspects, legal aspects and social aspects. Moreover, the conceptualization of electronic identification together with the three aspects in e-ID literature will be applied in chapter 5 (Discussion).

2.1 Defining electronic identification

There is a tendency in the academic community to overlook or to over-simplify the issue of identifying oneself electronically (Söderström, 2016). This is considered to be a weakness. Söderström argued that different latent conceptualizations of the e-ID may generate misapprehensions and further misleading research results. Further, Söderström argued that there are significant differences in the conceptualizations of the e-ID. As an example, Kubicek (2010) makes no distinction between the abbreviation of e-ID and digital identity. By contrast, Söderström claimed in his dissertation that his empirical findings had indicated a weak connection between e-IDs and digital identities, as the e-IDs (smart cards) in his case were regarded as isolated entities. Although being critical towards lumping together e-IDs with digital identity (with digital being perceived as more significant than merely a plastic card with a chip placed on it), Söderström acknowledges the rapid pace of technological innovations being launched every day on the market. Therefore, he encouraged further research, which would explore how people’s identities are increasingly becoming digital.

The e-ID exists in a number of different forms, such as on plastic cards, files on the computer, on sim-cards in mobile phones and as mobile applications. A tendency which was common in the scientific literature about electronic identification was to instantly refer the e-ID token to one specific form, for instance the smart card. In for instance Söderström’s (2016) study, the e-IDs were placed on plastic cards, which may or may not have impacted on his results indicating that nurses saw little or no connection at all between the e-ID and digital identity.

Kubicek (2010) made an ambitious attempt to define the e-ID. He argued that the e-ID begins with the notion of entity, which is anything that is characterized from a set of attributes. An entity could for instance be a person, a company or a computer. Further, identity is the dynamic totality of the attributes, belonging to the entity. Moreover, the entity can only have one identity, but several digital identities, because they are subsets of specific attributes. Attributes could be either distinct or abstract, measurable properties of identity, and some of the attributes are identifiers. Finally, the identifier is one attribute or a set of attributes of an entity, which identifies the entity within a specific context.
Different researchers have had different levels of abstract theorizations about electronic identification. Söderström (2016) who studied e-ID implementations in healthcare, gathered four sub-concepts in his dissertation, which together defined electronic identification. The concepts are identity, identification, authentication and authorization. Tsakalakis, Stalla-Bourdillon and O’Hara (2016) defined the first three sub-concepts (going backwards) in their study as: authentication being the process in which an individual proves a claim to an entity, i.e. individual number 1 proves to individual number 2 that she is, for instance, a grown-up. Further, identification is a subdivision of authentication. This means that identification attaches the individual to an identity. The identity itself holds several attributes, such as name and date of birth. Furthermore, Söderström (2016) argued that “the identity is in fact based on attributes unique to the individual while identification, authentication and authorization are related to the process of requesting and acquiring access to something protected from public access” (Söderström, 2016, p. 4-5).

Finally, Söderström (2016) defines the concept of authorization (which was highly relevant to his healthcare case) as granting permission, which is based upon different attributes. The permission granting means that an authenticated (e.g. when the person has proven to be who he or say is said to be) entity has the right to perform a certain task, or to use some kind of service or resource (Kubicek, 2010). Söderström (2016) made a table (see Table 1) on the four sub-concepts and their characteristics.

Table 1. A modification of Söderström’s (2016) matrix on the four concepts defining the e-ID.

<table>
<thead>
<tr>
<th>Concept</th>
<th>Typification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identity</td>
<td>Unique combination of attributes</td>
</tr>
<tr>
<td>Identification</td>
<td>Representation of attributes</td>
</tr>
<tr>
<td>Authentication</td>
<td>Assessment of attributes</td>
</tr>
<tr>
<td>Authorization</td>
<td>Permission based on attributes</td>
</tr>
</tbody>
</table>

The e-ID Board (2016) described e-identification and the basic principle of it in four steps, namely: the user indicates that he or she wants to use a certain e-ID to login to a service (1), the service sends an identity certificate-query to the e-ID issuer (2), the e-ID issuer checks who the user is and sends an identity certificate back to the service (3) and through this exchange the service has identified the user (4).

Moreover, the processes in which we are authenticating, i.e. when we are proving that we are who we claim to be, differs. There are different methods which differs in terms of the security level, and two common concepts are two-factor authentication and strong authentication. Two-factor authentication (in short, 2FA) denotes that we are using two things, one thing we know and one thing we possess. One example of this is withdrawing money from the automatic teller machine. The thing we know is our pin code and the thing we possess is our bank card. In the popular Swedish e-ID solution mobile BankID, the mobile phone (and the mobile BankID application) is the thing we possess, and the password is the thing we know (Lotsson, 2018). Further, authentication can also be based on something we are, and this is known as biometrics, i.e. our fingerprints, voices, faces, and so on. The concept of strong authentication was also
discussed in the academic literature. This is a concept without a clear definition. Verisec (2015) used the triad of knowledge, ownership and inherence to describe strong authentication. Further, strong authentication is when two or more of the following things are used: something the user knows (e.g. a password, personal identification number), something the user “owns” (e.g. a mobile phone, or a smart card) and finally, something which the user inherits (biometrics). The e-ID, Mobile BankID, also supports biometrics with Touch ID or Face ID on newer mobile devices (from version 7.8 and onwards), as alternatives to passwords, although the service currently used could require only using a password (Bankid.com, 2018).

Lastly, the four concepts of identity, identification, authentication and authorization are generic concepts occurring frequently in literature published about e-identification. As was argued before, these are defined differently, depending on each researcher’s motivations. However, the main conceptualization of the e-ID chosen in this study is the one put forward by Söderström (2016), as it offers a clear and holistic model on the comprehensive and intricate area of electronic identification.

2.2 Scientific literature about e-IDs

Most scientific articles used in this thesis were found through using the search terms eID or electronic identification, sometimes in combination with words such as token, or eServices. Further, the articles were found in databases such as Emerald and DIVA, which the Linnaeus university subscribes to. I narrowed the literature search, by choosing scientific articles from the year of 2013 and onward. This measure was taken in order to make sure I was using articles which featured relatively new discussions about the e-ID. Further, studies about e-IDs which were published earlier than 2013 were added if they offered key historical insights or other interesting angles catering to the study’s aim.

Eaton, Hedman, and Medaglia, (2017) argued that earlier research on e-IDs have emphasized issues such as technological decisions, trust and public value, surveillance, legal frameworks, innovation processes, market governance, and life cycles. Applied theories have for instance been concepts of innovation and boundary objects. Common data gathering methods have been case studies and surveys. Further, the researchers argued that the published studies have neglected to study the interactions between different kinds of actors. Moreover, after I had gathered a satisfying number of articles, these were divided into three broad categories, because of the issues being expanded on in the topical literature. This was done in order to structure the analyzing of the available literature and also to enhance the presentation of the content in the gathered academic articles. The created categories were technical, legal and social aspects. Moreover, some of the found articles were one-sided and occupied with for instance technical solutions. However, a significant proportion of the found articles were broader and their content might be located under each of the constructed categories.

The topics put into the technical aspects section has primarily been centered around hard systems, i.e. to improve e-identification in order ensure secure identification and authentication in the future. The legal threads were mainly based on comparisons of different countries, their e-ID schemes and its effects on the e-ID use. Regulations, particularly eIDAS, have been scrutinized in some articles. The third thread found relating to legal issues was immigration and the highly desired “legal identity”, despite that there are negative factors associated with it. The elements which have been social, have almost entirely originated from research made in organizational contexts, such as in healthcare. These studies have predominantly conveyed issues such as user perceptions, policy, strategy, economy and so on. Further, the focus has
been put on the governing (in the public sector) of electronic identification and employees’ reactions towards the solutions being imposed on them. Moreover, social perspectives were mainly applied in Scandinavian research (by a few researchers). Although there are studies published exploring social issues, there is a void needed to be filled with research on social factors and in particular of ordinary civilians’ use- and perceptions of e-IDs. There is a shortage of studies showing how civilian populations use and reflect on the e-IDs, especially since this is not a new technology (in Sweden) and issues such as technology acceptance or adoption are therefore of less significance.

2.2.1 Technical aspects

In this category, articles with discussions about hard (IT) systems were organized. Common subjects were biometrics, authentication processes and security, among other things.

**Biometrics**

Tsakalakis, Stalla-Bourdillon and O'Hara concluded in their article from 2016 that “future work is needed to explore how additional attributes, such as biometric information and attribute providers, should be incorporated into the existing system in order to equate it to higher international Levels of Assurance.” (Tsakalakis, Stalla-Bourdillon and O'Hara, p.44).

Biometrics was a recurring theme in the literature about electronic identification. Turkey is one example where issues in this regard have been surfacing. The national e-ID consists of a plastic card with a chip, which is produced and issued by the state of Turkey. These cards reached the market before the card access devices were produced and disseminated by private companies (Bostan, Şengül, and Karakaya, 2017). Bostan, Şengül, and Karakaya argued that the biometric verification specifications are unclear in Turkey, and they therefore proposed letting the state run the verification algorithm and thereby keeping the people’s biometric data away from the companies who produce the access devices. More specifically, a major issue is the difficulty of revoking biometrics, in comparison to chosen passwords or tokens. The fingerprint is not possible for an individual to replace, as compared to a pin code. Furthermore, it has been argued that some individuals may have difficulties in providing the requested biometrics, for instance transgender persons have been mentioned in the questioning of the alleged unambiguous link between biometrics and a unique identity (Eaton, Hedman, and Medaglia, 2017).

**Authentication**

Another technical area being described in academic articles is the issue of authentication and adequate requirements for this. This area is growing, since people in Europe (among these Estonia is often held up as a prominent example), use e-ID tokens increasingly. They are used as public transport tickets, substitutes for driving licenses, for e-banking and access to libraries or swimming pools and many other things. Nyman, Ekberg and Asokan (2014) specifically proposed a new architecture based on the authorization model within the new Trusted Platform Module specification (TPM 2.0). This is to improve urgent concerns such as security and usability to ultimately be deemed trustworthy. Further, the researchers were not convinced that e-IDs in the form of smart cards (so-called “stand alone tokens”) was the best solution and suggested instead that e-IDs should be embedded in smart devices since they had a higher degree of usability. One conference paper (Hölzl, Mayrhofer and Roland, 2016, p.2) pointed out existing flaws in terms of privacy:
“A survey of available governmental eIDs in the European Union by Lehman et al. shows that none of them provides anonymous and privacy-preserving verification methods. Only the Austrian and German eID cards support notable features for protecting users’ privacy by pseudonym generation and selective attribute disclosure.”

Authentication is a comprehensive process which is discussed extensively in the literature, for instance through the example of the United Kingdom’s newly rolled out e-ID scheme (known as ‘Gov. UK Verify’), which has been launched as a “state-of-the-art-privacy-preserving system” (Tsakalakis, Stalla-Bourdillon and O’Hara, 2016, p.32). The state’s national ID cards efforts have bad connotations based on historical events, and a register (known as “NIR”, National Identity Register) which was setup in 2006 together with the launch of an ID card (containing biometric data and other identifiers such as name and date of birth). The register was eventually destroyed (2010) due to mass allegations of state surveillance. It is the first system in the UK, where the government does not act as an identity provider but have instead delegated this responsibility to competing companies on the market. The system encompasses correspondence between several parts and components, namely: the central hub, the service provider, the identity provider, the matching service as well as the e-ID user. In the authentication process, there are nine exchanges between these parts. Further, Brandão et al. (2015) compared the UK identification system (Gov UK Verify) with the United States Federal Cloud Credential Exchange (FCCX) and deduced that these systems, which are used by more than one hundred million users (who need to authenticate in order to access e-government services), have issues in terms of both privacy and security. The main message mediated in the article is that malicious forces could access information about users undetectably, with the worst-case scenario being mass surveillance.

Requirements

Since e-ID tokens exist in several different forms, Hölzl, Mayrhofer and Roland (2016) provided a requirements chart for e-IDs, in which the generic notions of functionality, mobility, security and privacy were included. These notions contained 3-4 requirements each. The goal of “real world identification” was envisioned as a mobile e-ID which for example would be equated with a typical ID document, instantiated through the “prover” (driver) showing the “verifier” (the police officer) his or her driver’s license. Further, the scheme should allow for using the same e-ID in different contexts. Under the notion on mobility, it was argued that one should for instance be able to have offline verifications and the e-ID should not depend on the mobile device’s battery, it should work without a charged battery. For security, the researchers suggested state-of-the-art cryptography. Under the notion of privacy, privacy-preserving signatures was included together with the three elements of anonymity, unlinkability and backward unlinkability, which covers that the user should not have his or her identity revealed, and it should not be possible to link an individual’s transactions across verifications. Under user-control it was argued that the user must be able to decide which attributes to share with the verifier, i.e. the user should authorize what data can be shared with the verifier.

Nyman, Ekberg and Asokan (2014) claimed that reducing passwords in user authentication (in online transactions) is a problem needed to be solved. The Fast Identity Online (FIDO) alliance is an industry consortium (held up as a prominent example), which offers specifications in authentication architectures which are backed by many industry players. These specifications are based on strong authentication and biometrics. Essentially, what differs from the user’s point of view, is the degree of privacy protection in FIDO’s protocol, which offers asymmetric keys for authentication. This means that different service providers cannot link the user’s activity, if they cooperate.
Another area where secure electronic identification and requirements for this was addressed, was in e-Voting. This is a complex area, as there are several variables which should be fulfilled in order to create secure e-Voting information systems (Zissis and Lekkas, 2011). Zissis and Lekkas, (2011, p.245) claimed that “e-Voting security is in effect a matter of trust”. Further, John et. al (2013) addressed the problem of merely using passwords for e-Voting, as malicious software programs could easily be used and make the process of electronic voting insecure. The researchers proposed a combination of smart cards and biometrics, which they called hybrid identification. The scheme entails three criteria, i.e. something the voter knows (a PIN code), something he has (a smart card) and lastly, what he or she is (biometrics, such as fingerprints).

2.2.2 Legal aspects

Legal frameworks in European states and their implications for the countries’ different e-ID schemes and use, was a common theme among the gathered scientific articles. Further, other matters which have been prevalent in the scientific articles are interoperability within the confines of the European Union, as well as the new e-ID legislation eIDAS.

Countries’ different legal frameworks

Lentner and Parycek (2016) conducted a comparative legal study, in which Germany, Austria, Lichtenstein and Canton of Zug were compared. They concluded that the differences in legislative culture and existing legislation had a big impact on which e-ID solutions were launched in the different regions. In countries where the ID card is obligatory to carry, the e-ID is offered in the form of a smart card. This was the case for Germany. In countries where ID documents were not obligatory, the e-IDs ranged from smart cards to mobile device solutions. Further, Lentner and Parycek noted a difference of usage, since the e-IDs in Germany and Canton of Zug were used to identify, whereas in Austria and Lichtenstein the e-ID was primarily used for signing electronic documents (i.e. e-signing).

Nyman, Ekberg and Asokan (2014) explored what was hindering the adoption of a pan-European e-ID scheme and found that it essentially legal aspects. Further, they claimed that the work towards achieving interoperability in the European Union has been complex, with having to incorporate the aforementioned notions of user-centricity, anonymity, pseudonymity, multiple identities, identity portability and unlinkability.

Regulations

The EU regulation eIDAS was frequently referred to in the scientific articles. This “new” law was adopted by the European commission in 2012, as a reaction on the current legal e-ID framework. The past law was deeply fragmented, meaning that each EU member state had its own specific e-ID solutions (Martin and Gomes de Andrade, 2013). In its core, the legislation means that EU citizens will be able to use their e-ID tokens in all EU member states. Further, the eIDAS legislation will be put into action in autumn, 2018. The European commission motivates eIDAS with claiming it means a higher degree of security and convenient interactions with public agencies, such as when filing taxes. Further, one can remotely open a bank account, start a company in another EU member state or make internet payments easier, etcetera (Digital Single Market, 2015). According to Tsakalakis, Stalla-Bourdillon and O'Hara (2016), eIDAS is a step in the direction towards creating a single market, for the states which are EU members. In this respect, the legislation is for ordinary citizens living in the confines of the European Union.
Union. A message the scientific articles sends is that this law will have to be followed-up, regarding the effects this will have on people’s levels of trust as well as privacy concerns, among other things. Further, the main aim of the legislation is explained as to “manage electronic seals, time stamps, certificate services for website authentication and electronic documents and their delivery” (Tsakalakis, Stalla-Bourdillon and O’Hara, 2016, p.35). Further, the eIDAS is meant to be an interoperability framework for national e-ID management systems. Further, the topic of pseudonymisation was discussed in detail in one of Tsakalis, Stalla-Bourdillon and O’Hara’s (2016) articles. This concept was put in relation to the EU regulation GDPR (General Data Protection Regulation) and eIDAS. One important aspect of pseudonymisation is its feature of reducing the risks of data breaches. However, the definition of pseudonymisation in GDPR was argued to be too strict in order for it to achieved. As a result, the researchers concluded that eIDAS datasets cannot comply with GDPR’s strict definition.

**Legal identity**

A topic which has been problematized in literature is immigrants and their requests of receiving legal identity. For instance, some governments do not register their populations as is done in Europe. Individuals immigrating from these countries (Peru is one example) are difficult to identify (Whitley, Gal and Kjaergaard, 2014). Whitley, Gal and Kjaergaard studied identity and identification. One of their objections to identification systems were that “If this legal identity is missing, people can find themselves effectively excluded from many of the basic activities in society and with a diminished base from which to form their social identity.” At the same time, there was an element of fear in their article, claiming that the registration of people could lead to a “govern by identity” (Whitley, Gal and Kjaergaard, 2014, p.25). Moreover, Eaton, Hedman, and Medaglia (2017) argued that academic literature about e-IDs generally is dismal and foresees massive state surveillance tendencies with identification systems being launched on the market. Despite this, it is contended that many immigrants aspire to receive a legal status, which means having certain rights (e.g. voting, welfare,) as well as responsibilities (e.g. paying taxes).

2.2.3 Social aspects

In the gathered literature about e-identification, a decent amount of the articles carried elements of softer issues, such as people’s adoption of newly implemented e-identification systems. Another angle was the intertwined nature of soft systems and hard systems (i.e. people and technology). Articles which had an outstanding focus on social perspectives were mostly published in Scandinavia and these were often published by the same researchers (in different constellations).

**The e-ID as a socio-technical system**

One researcher duo attempted to bridge the dominant technical and social perspectives, through viewing electronic identification as a socio-technical matter. In Lirginlal and Phelps article published 2012, the focus was on digital identities and their adoption in Arab countries (with Qatar as the selected case). The “digital identities” were issued for the purposes of managing e-government related tasks and e-payments. Lirginlal and Phelps applied the concept of Identity and Access Management (IAM) while arguing that digital identity issues is a complicated issue, with policy, technology, and supporting infrastructure being intertwined, which further implicates the deployment, control and maintenance of digital identities. Furthermore, the grip of ‘socio-technical’ entails bringing in factors such as technology, social matters, politics,
regulations and cultural dimensions which have a role in people’s usage of different technologies. Lirginlal and Phelps (2012) analyzed digital identity implementation in Qatar specifically with the concept of barriers, which are social, economic, technical, legal and policy in nature. The notion of religion was also discussed, as in Qatar Islam is the dominant belief system, which was perceived as a hefty factor in the adoption of digital identities. According to Lirginlal and Phelps, in Islam, the rule is that technological innovations cannot desacralize the tenets of Islam. This implies that religion will inform the implementation of digital identities, especially in terms privacy and data protection. The main message presented in the researchers’ article was that digital identities reflect social institutions, but also technical components, such as servers and readers. Further, local culture is stressed as an element worth more attention. What works in for instance Qatar may fail completely in another Arab state, which may share many similarities, but differences as well.

Present in the articles with a socio-technical viewpoint was the use of various theories to describe e-identification as a system both dependent on human and non-human actors, where technology and social aspects are seen as intertwined, which informs how the designated technology is perceived and used by people. Hedström et al. (2015) aspired to find out how identities were constructed when implementing e-IDs on cards and why different job roles meant different use of electronic identification. The researchers used Actor-network theory (ANT) to compare two e-ID implementation processes in Sweden. One of the cases was an elementary school context and the other one was in a public healthcare context. Further, the ANT was used as a tool in addressing both human and nonhumans actors (such as the e-ID), which together form a network. Furthermore, technology (i.e. the e-ID) carries meanings and values within itself. Through the human and non-human interplay, meanings are translated, which will eventually change the network. The element of so-called translation is defined by new emerging relations between human- and non-human actors. In Hedström et al.’s study, it was found in the healthcare case that there were two distinct human actors with different ideas in the network, which they labeled project initiators (information security manager) and users (nurses). From the project initiator’s point of view, the e-ID was necessary to implement, in order to ensure strong authentication and thereby secure the patient data. However, some users regarded the e-ID card as a constraining commodity, which had to be used throughout the workday. Moreover, it was found that the e-ID card was not handled properly by the users in order to secure the patient data. As a reaction to this, the project initiators wanted to make the e-ID token more integrated into the nurses’ workday. Functions were added to the e-ID card, such as making it a payment card, which could be used during coffee breaks for purchasing snacks, etcetera. However, most nurses regarded the e-ID card merely as a professional token, with a fixed meaning. Moreover, in the school area, teachers were not allocated e-IDs (from the municipality). Instead, the management was discussing the option of teachers using their own personal e-IDs for authenticating in the various digital educational platforms. This option was rejected by the teachers as their own e-IDs were used to manage personal things such as “pay my bills or buy something on the internet” (Hedström et al., 2015, p.153). Gustafsson (2017) cited Hedström et al.’s. (2015) research (which she was a part of) and applied the notion of trust, because the school case demonstrated a lack of this element. Further the problem was also related to attitudes, lack of skills, and lack of backup from the municipal IT administration. Instead of using the suggested e-ID solution, i.e. the teachers using their own e-IDs (to authenticate themselves in the digital platforms), they created back-up systems and worked in a more analogues fashion (i.e. printing information which was needed). Further Gustafsson (2017) argued that people working in healthcare and in schools had a somewhat shared picture of the problems related to the e-ID implementations. The problems were essentially related to the blurring of private and public spheres. It was found that fear of intrusion by unauthorized
users, threats to the integrity and surveillance from public agencies (or the market actors) caused the hostility towards using e-ID tokens on the workplace. Gustafsson (2017) regarded the governing of e-IDs and their perceptions between different actors as processes of translation. In the translation process, teachers, healthcare personnel, school principals, politicians, municipal IT staff and so on, were involved. Further, the tensions were emerging when networks were overlapping. Gustafsson (2017, p. 95) explained that e-IDs are made obligatory passage points (OPP):

”In terms of our tension, the struggles and resistance occur when networks from these different translations overlap and as a result, new parts of their identities, interests and activities are revealed by a digital tool that is made an OPP for both. This generates a new condition for the networks. It triggers a new problematisation, where again the identities, interests and roles need to be clarified and new associations in terms of rules and modes for action need to be negotiated.”

Söderström (2016) explored electronic identification in Sweden with a soft systems-oriented approach, merging and developing sociological and institutional theory. Similarly, as Hedström et al. (2015) and Gustafsson (2017), he researched implementation of electronic identification tokens in the public sector. Söderström (2016) applied Actor-Network theory as a part of the sociological perspective (‘sociology of translation’), with the motivation that ANT is an elucidatory framework for studying entities which are hybridized and thus difficult to separate from each other. Moreover, Söderström researched e-ID card implementations in several organizational settings, exploring how e-IDs were “translated” within the Swedish healthcare system and in three Swedish public agencies. He concluded that there were overwhelmingly negative translations of the e-IDs cards, partly due to the coordinating actors’ ways of handling institutional barriers. A paradox was evident in both cases (i.e. eHealth and eGov), as the users of the e-IDs were not using them as was anticipated. Söderström (p.316) concluded that “The introduction of the public sector eID, with the aim of increasing security, results in decreasing security levels”. Furthermore, Söderström emphasized the importance of realizing that there are more aspects than the merely the technical part of an e-ID. One conclusion drawn was that the function of the e-ID is unique, and it is an important enabler in the public agencies’ web-based services offered to citizens and businesses. Further, he claimed that the e-ID is a necessary and important prerequisite in the development of e-Government services.

Path dependency and CSF’s

Although there were several published studies emphasizing the user experience in relation to electronic identification, these studies have mostly been targeting the population of employees in the public sector. Further, this research has been preoccupied with the governing of e-IDs, so as to create an understanding of why the e-ID implementations in for example the health care sector has not been successful (Melin, Axelsson and Söderström, 2016). The economic concept of path dependency was applied in order to comment on the present as well as future actions and decisions, by looking in the rear-view mirror. There are four interrelated causes in the concept of path dependency, which are: increasing returns, self-reinforcement, positive feedbacks and lock-in effects. Melin, Axelsson and Söderström (2016) addressed the governing of e-IDs in Sweden, through using the economic concept of path dependency. Serious challenges where detected, such as a narrow understanding of electronic identification in itself. The researchers contended that e-identification had been reduced to a back-office enabler, implying that it was a component which has been neglected (Melin, Axelsson and Söderström, 2013). Further, the researchers argued that electronic identification was underestimated in terms of its contextual and organizational intricacy. Melin, Axelsson and Söderström applied in their
article from 2013 both a life-cycle and a critical success factor (CSF) perspective, in order to elucidate the challenges in managing e-government and e-identification, particularly in Sweden. Common life-cycle variables that were used were project assessment, analysis of present reality, designing the new system and implementation (and beyond). The CSFs were related to information and data, IT, organization/management, regulation and institutions/environment. What was extracted from the applied frameworks was that there were challenges in designing the e-ID infrastructure, while taking the current e-ID solutions into account. Also, the e-ID projects have had organizational and management problems. The problems have essentially been that the professionals involved in the projects have had a myriad of roles and consequently different expectations on the projects’ outcomes. Moreover, one suggestion which was put forwards was a more integrated view of electronic identification, implying that one has to leave the notion of e-IDs as mere back-office enablers (in the launches of eServices). Furthermore, it was concluded that electronic identification is intimately associated with the use of e-services from the user’s point of view and therefor the public agencies need to widen their horizon (Melin, Axelsson and Söderström, 2013).

The e-ID adoption in two countries

The theme of implementation and e-ID adoption has been explored with the general public as a targeted group. One study compared the two countries of Bangladesh and Nigeria. McGrath, (2016) showed that the e-ID adoption processes varied in these two different countries, partly because of the trust existing between governments and their citizens. The relation between state and citizen were divided into two concepts of ambivalence and suspicion. Ambivalence denotes a coexistent trust and distrust towards one target. Suspicion is a general negative sentiment, with elements of skepticism, cynicism and distrust. McGrath illustrated in her study that implementations and people’s use of e-IDs (identity smart cards) was more successful in regions characterized by government-citizen ambivalence, such as in the United Arab Emirates or Bangladesh. Further, it was argued that the ambivalence emerged from the tensions of security and privacy concerns and the positive sentiment in the government’s campaigning for public awareness, trust in institutions, etcetera. In Nigeria, there were lower levels of trust between the government and citizens, because of corruption and incompetence, where previously failed ID card implementations were not evaluated, etcetera.

2.3 Conclusion of literature review

It can be deduced from the theoretical discussions rendered above (the school case being a good example) that the e-ID token is understood as a personal or private object, which to a large extent is used by people in their daily lives, for their own purposes. My targeted population and the previously conducted studies differ because most researchers have been targeting workers from different sectors such as the public healthcare, where the nurses are obliged to use the e-ID (in the form of smart cards). This disrupts their well-established work routines, with having to walk around and remember to bring the e-ID token with them and use it every time they are logging in on their computers (Söderström, 2016). It cannot be easily concluded for this reason that the e-ID is a considerable issue for private persons, since they presumably have a higher degree of voluntariness in choosing to adopt and using e-ID tokens, than when e-IDs are imposed on the working place.

The gathered literature has included different aspects and topics which could be related to the chosen e-ID framework of identity, identification, authentication and authorization (Söderström, 2016). The technical and legal literature were to some extent based on private
persons with discussions on for instance secure and privacy preserving authentication. Further, these topics lie mostly under the concepts of identity, identification or authentication. The social thread, however, most often had the organization and its constituent parts as a unit of analysis, which means that the issues would fit into the concept of authorization. In healthcare, for instance, the nurses needed to prove they were authorized to access patient’s journals. However, this process is not isolated to authorization, rather it is a mixture of, for instance, authentication and authorization. Below, in Table 2, is an attempt to fit in the gathered literature in a matrix with Söderström’s (2016) four sub-concepts. The matrix contains concepts which are present and emphasized in the reviewed literature and most of them are included in chapter 5. Moreover, the definition of the e-ID as four distinct areas may be debatable, as the topics discovered in the body of scientific literature could fit into several sub-concepts.

Table 2. Söderström’s four sub-concepts and topics from the scientific articles

<table>
<thead>
<tr>
<th>e-ID concepts</th>
<th>Technical</th>
<th>Legal</th>
<th>Social</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identity</td>
<td>Biometrics, privacy security unlinkability, state surveillance</td>
<td>legal identity identity portability, governing by identity, social identity</td>
<td>adoption of digital identities, barriers, job identity, translation, ambiguity, trust</td>
</tr>
<tr>
<td>Identification</td>
<td>Hybrid identification</td>
<td>e-ID cards for identifying vs. e-ID cards for signing, massive state surveillance</td>
<td>e-ID as a back-office enabler</td>
</tr>
<tr>
<td>Authentication</td>
<td>requirements, functionality, mobility, security, reducing passwords, strong authentication, biometrics</td>
<td>–</td>
<td>tension of security and privacy</td>
</tr>
<tr>
<td>Authorization</td>
<td>–</td>
<td>–</td>
<td>protection of patients’ journals and pupils’ data,</td>
</tr>
</tbody>
</table>
3 Methodology

3.1 Research Paradigm

According to Guba and Lincoln (1994) there is one basic distinction made between quantitative and qualitative research. The first-named approach is referred to as “hard” and it has a determined objective of quantification of findings, and the qualitative approach is described as “soft”, because of the position that for instance social sciences are less precise than quantitative research, such as mathematics. Moreover, Biggam (2008) claims that quantitative research usually answers the how-questions, while qualitative research usually goes more in-depth and tries to answer the why-questions. Further, Biggam adds that the qualitative researcher is attempting to interpret phenomena through people’s meaning making. Moreover, the view held by Creswell (2014) about the qualitative research design broadly describes the choices made in this study, regarding the data analysis and the presentation of the findings. Creswell (2014, p.32) states that:

“Data typically collected in the participant’s setting, data analysis inductively building from particulars to general themes, and the researcher making interpretations of the meaning of the data. The final written report has a flexible structure. Those who engage in this in this form of inquiry support the way of looking at research that honors an inductive style, a focus on individual meaning and the importance of rendering the complexity of a situation.”

The researcher conducts his or her research with fundamental beliefs about principles. These are known as paradigms or worldviews, which guide the researcher in how he or she views the world, knowledge and methodology (Lincoln and Guba, 1994). There are three dominant paradigms within the scope of information systems research. These are known as the positivist, interpretive and critical paradigms. Their main differences are their ontological and epistemological assumptions, that is, their ways of viewing the world and their ways of viewing knowledge (Orlikowski and Baroudi, 1991).

The positivist researcher believes in objective reality, which exists irrespective of human beings. Further, it is contended that phenomena can be gauged, and the researcher is supposed to be neutrally or passively approaching the chosen area of interest. Conflicts and contradictions are not matters of interest, but if these things surface, they are approached as things to correct. Moreover, in terms of epistemology, positivists argue for testing theories, for instance through applying the ‘hypothetico-deductive’ model. Moreover, this model is applied in order to predict patterns of behaviors in different situations (Orlikowski and Baroudi, 1991).

The interpretivist regards reality as a social construction by human actors (Walsham, 2006). Human actors construct and reconstruct their social realities through symbolic action. The interpretive research therefor rejects the positivist credo of objectively accounting for events and situations. In the interpretive worldview, reality is social and filled with subjective meanings, which informs not only language, but how people act as well. Further, the epistemology differs from the positivist research, since the interpretivists enter a world of those creating it. Further, the interpretivist researcher tries to understand social reality, by studying language and implicit norms (Orlikowski and Baroudi, 1991).

The critical researcher perceives social reality as contingent upon history and with a profound understanding about history, people have a certain capacity to better their situations. However, they are constrained (“alienated”) by strong economic, cultural and political systems. As the
interpretivist paradigm, the critical paradigm entails regarding reality as something produced and reproduced by people. The epistemological position taken is that knowledge is contingent upon historical and social practices (Orlikowski and Baroudi, 1991).

I am intending to conduct research which falls into the category of interpretive research. In this stream of thought, reality, i.e. ‘social reality’, is seen as a social construction by human actors (Walsham, 2006). Klein and Myers (2011) nuanced this argument a bit, by stressing that interpretivism does not define dependent and independent variables beforehand, instead the focus lies on the complexity of human sense making as a situation is dawning. Further, there are critical elements embedded in my research, specifically in my questioning of the current e-ID scheme, its intricacies and exclusion of several groups in society (see Discussion, caption 5.3). My mindset while entering the thesis process was to a large extent colored by my previous negative experiences from working on a BankID issuing bank. Moreover, Doolin (1998) argued for employing a higher degree of critical and reflective approach towards technology, within the scope of interpretivism. His examples were based on organizational research, although arguably electronic identification and people’s interpretations of it could be seen as existing in a larger organizational ecosystem, namely the Swedish society. This means that I, instead of researching a smaller organization’s use of a certain technology, reposition the focus to the Swedish society in general. Further, the focus is also on perusing state documents which are compared to people’s thoughts and use of the designated technology. Bloomfield (1995, p.497) described the relation between the social and the technical in a society as, “technology does not impact on organizations or society; a change in social relations, tasks, skills and knowledge is already prefigured in a way that the technology is conceived of and constructed”. Furthermore, my own position is that there needs to be viable alternatives to the digital society, even if there is a high degree of technology acceptance among the state’s population.

3.2 Data Collection

The environment where my interest for the issue grew was on a bank in a small municipality, in the south of Sweden. Reactions came from the young, the middle aged and the older people when they tried acquiring the Swedish banks’ e-ID. The ones struggling seemed to belong to different strata, thus the BankID was in general perceived as cumbersome. Hence, the targeted population in this study was the general public in Sweden. Since I am located in the municipalities of Växjö and Älmhult (both situated in the south part of Sweden), the data was collected in these two municipalities.

3.2.1 Sampling approach

As a sampling strategy I followed the purposive sampling approach, which is also known as judgement sampling (Gobo, 2011; Wildemuth, 2009). Through this “non-probabilistic” approach the researcher strives to maximize variation in the targeted population, through applying his or her own judgement. Additionally, it includes the aim of choosing information rich cases, i.e. interesting people to interview (Patton, 2015). Now, it is common in qualitative research to strive for variation in the sample (Trost, 2010). This means that the interviewed individuals should be heterogeneous within the defined homogeneity, which in this study is both Swedish citizens and non-Swedish citizens living in Sweden. Further, I made the conscious decision to interview people who have an understanding of what an e-ID is (no matter what this interpretation might be). There were some exceptions to this rule, for instance choosing to interview someone who claiming to be completely unfamiliar with electronic identification. The reason to why the concept of electronic identification had to be familiar to the interviewee,
was to create meaningful discussions and material for me to analyze and hence answer my research questions with. I strived to use Trost’s (2010) suggested ‘strategic sampling’ scheme in order to reach people from different strata, within the selected population. This means that I was purposefully reaching out to people belonging to different categories. By selecting different categories, the assumption was to increase the chances of finding different interpretations of e-IDs. Finally, to follow the strategic sampling scheme means the risk of not knowing who to approach and interview. This is where I relied on my own judgement as a researcher and thus followed the purposive sampling approach (Patton, 2015).

Now, it is important to note that the categorization is only a measure that I took to maximize the chance of receiving varying interpretations. In reality, I could get similar answers from people of different strata. Although, through targeting different groups in society, I hoped to reduce the risk of bias associated with choosing one convenient category of people to interview (e.g. interviewing only female friends).

Below, in Table 3, details about the ten study participants are shared. It goes without mentioning that within these age categories there are many different categories of people, with different interests, levels of knowledge etcetera. Moreover, the initially targeted categories of people were adolescents, young adults, middle aged and seniors. I decided from the beginning not to interview children or young teenagers under the age of 13, as these usually do not qualify to possess an e-ID token in Sweden (Bankid.com, 2018). Further, in these categories, adult immigrants, preferably those born and raised outside of the EU were targeted. Specifically, immigrants and seniors were coveted. Immigrants, because those who are new in Sweden and who have been facing the necessity of acquiring an e-ID token, could offer important insights into challenges encountered in Sweden, i.e. how is e-IDs understood when coming from a country which might not offer its’ population ways of identifying electronically? Elderly people, who have retired and therefore presumably are not as exposed to the digital (work-related) world were targeted in order to find out how the e-IDs were understood by them.

Although the elderly does not have experience work-related ICT interactions, it has been found that approximately 80 % of the senior population in Sweden own at least one ICT device. Seniors is a very wide and heterogeneous category and the levels of digital literacy vary within this population (Olsson, Samuelsson and Viscovi, 2017). According to Davidsson and Thoresson (2017), around 75 % of the Swedish population between the ages of 66 and 75, who own a smart phone use the mobile BankID. Among those who are over the age of 76 and who own a smart phone, the use of mobile BankID is over 50 %. In order to broaden the scope and understand the current e-ID scheme in Sweden better, Anders Henrikson, which is the co-founder of the IT security company Verisec was interviewed. Henrikson’s company owns (the e-ID) Freja eID which is a relatively new competitor to BankID.
Moreover, the documents used as primary data were all produced within the public sector. Below, in Table 4 some details about the chosen documents are presented. I will use the terms document and report interchangeably from now on. The chosen reports have similarities, as well as differences. The report written within the finance ministry was ordered by the civil minister in Sweden, who requested analyses and suggestions for effective governance of development, implementation and administration of national digital services (Regeringskansliet, 2018). eSam’s report is a legal guide primarily aimed at guiding organizations in the public sector in its implementations of e-identification and e-signatures. Further, this is a report written by legal practitioners for legal practitioners and other involved parts. (Esamverka.se, 2018). The e-ID Board’s report was produced on the Swedish government’s command to ensure continued provision (from 2018) of services for e-identification and signatures.

Table 4. Details about the documents included in the study.

<table>
<thead>
<tr>
<th>Titles</th>
<th>Agency</th>
<th>Published (year)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reboot-restart of the digital administration</td>
<td>The Finance ministry</td>
<td>2018</td>
</tr>
<tr>
<td>Legal guidance in implementation of e-identification and e-signatures</td>
<td>eSam</td>
<td>2017</td>
</tr>
<tr>
<td>Continued provision of services for e-identification and e-signature</td>
<td>The e-ID Board</td>
<td>2016</td>
</tr>
</tbody>
</table>

All three documents shared the main objective of enhancing the digital administration within public agencies in Sweden. Electronic identification is regarded as an important factor in achieving this. Further, these documents problematized the present state, in terms of issuance, but also security among other things. Further, they all argued for increased governmental responsibility, suggesting that the state should issue e-IDs, etcetera. However, they were relating slightly differently to e-IDs as there were different aims in the reports. The report written within the finance ministry was primarily written to ensure national digital services, which means painting e-IDs with a broader brush, on the impressive amount of 225 pages. The e-ID Board is in charge of coordinating and supporting secure e-identification and e-signing and based on this premise they were elaborating on the Swedish e-ID model more as such (Melin, Axelsson and Söderström, 2016). The e-Sam report had the mission of informing first and foremost legal practitioners of e-IDs and their legal status, how they are engineered and intended to be used. Despite the differences, all three reports shared the normative narrative in the way they were written, that is, offering suggestions on how e-IDs should be managed within the confines of digital public administration.

Table 3. Details about the ten participants in the study.

<table>
<thead>
<tr>
<th>Age</th>
<th>Nationality</th>
<th>Occupation</th>
</tr>
</thead>
<tbody>
<tr>
<td>21</td>
<td>Swedish</td>
<td>Student</td>
</tr>
<tr>
<td>30</td>
<td>Iranian</td>
<td>Teaching assistant</td>
</tr>
<tr>
<td>40</td>
<td>Iranian</td>
<td>Student</td>
</tr>
<tr>
<td>18</td>
<td>Swedish</td>
<td>Student</td>
</tr>
<tr>
<td>62</td>
<td>Swedish</td>
<td>Teacher</td>
</tr>
<tr>
<td>83</td>
<td>Swedish</td>
<td>Retired</td>
</tr>
<tr>
<td>65</td>
<td>Swedish</td>
<td>Retired</td>
</tr>
<tr>
<td>64</td>
<td>Swedish</td>
<td>Product executive</td>
</tr>
<tr>
<td>69</td>
<td>Swedish</td>
<td>Retired</td>
</tr>
<tr>
<td>46</td>
<td>Swedish</td>
<td>Founder of Verisec</td>
</tr>
</tbody>
</table>
3.2.2 Semi-structured interviews

The data was primarily gathered through the vehicle of semi-structured interviews. This choice of strategy was chosen in order to cater to the study’s aim of eliciting the selected population’s reflections, as well as knowing more about their use of electronic identification tokens. All interviews except from one was conducted face to face. The last interview was done via telephone.

The semi-structured interviewing technique lies in the middle of three different forms, the others being structured and unstructured interviewing. Wildemuth (2009) argues that the main differences between these three are their levels of formality and structure, as well as the requested profundity. The structured and unstructured interviews are two extremes, with the first implying a standardized set of questions, posed in a specific order. The unstructured interview is very flexible, and the conversation can go almost anywhere. This means that the researcher is faced with challenges in terms of analyzing the gathered data, since each interview is strongly individualized, and the talking points are highly dependent on the interviewee. The semi-structured interview lies somewhere in the middle of the two aforementioned approaches. It entails having a set of questions, that could be posed in different orders. The main reason for me choosing the semi-structured interview was the held belief that individuals think in a variety of different ways about the same designated phenomenon. The thinking and reasoning of people can be more easily elicited with the aid of a semi-structured interview guide, rather than what the structured interview offers, but more systematic than the unstructured interview (Wildemuth, 2009).

The semi-structured interview is permissive towards changing the order in which the questions are posed during the interview sessions (Wildemuth, 2009). This flexibility meant that the interviews had different durations, on average they lasted 41 minutes. As is shown in Table 5, there were a few interviews which stood out and were either short or long. Further, some of the interviews were a bit looser in structure but exhaustive data-wise, while others were more dependent on merely the questions, which were written in the interview guides (Appendix B-D). One ethical stance I took was to not force my questions onto the interviewees. Instead, they chose themselves if they wanted to pass on the questions which were posed. If they showed a genuine interest and demonstrated a will to add about a certain area (within the scope of the chosen research topic), they were free to express themselves extensively, as I made sure to book the interviews on times when I was available for several hours. Further, in my interviews (Appendix C) some questions had a higher degree of prioritization than others, for instance all interviewees were first asked to define the e-ID. Furthermore, the interview questions about e-ID definitions and e-ID use were ranked higher than the questions about digitalization. The most prioritized interview questions were memorized before conducting the interviews, as they related closely to the thesis’ purpose (Trost, 2010).
**Table 5.** shows details about the conducted interviews.

<table>
<thead>
<tr>
<th>Participants</th>
<th>Time (in minutes)</th>
<th>Date</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>21-year-old</td>
<td>15</td>
<td>March 5</td>
<td>University- open space, in Växjö</td>
</tr>
<tr>
<td>30-year-old</td>
<td>138</td>
<td>March 6</td>
<td>University- open space, in Växjö</td>
</tr>
<tr>
<td>40-year-old</td>
<td>33</td>
<td>March 12</td>
<td>University- open space, in Växjö</td>
</tr>
<tr>
<td>62-year-old</td>
<td>39</td>
<td>March 15</td>
<td>School- study room, in Älmhult</td>
</tr>
<tr>
<td>18-year-old</td>
<td>39</td>
<td>March 15</td>
<td>School- study room, in Älmhult</td>
</tr>
<tr>
<td>65-year-old</td>
<td>43</td>
<td>March 15</td>
<td>home environment, in Älmhult</td>
</tr>
<tr>
<td>83-year-old</td>
<td>43</td>
<td>March 15</td>
<td>home environment, in Älmhult</td>
</tr>
<tr>
<td>64-year-old</td>
<td>50</td>
<td>March 16</td>
<td>home environment, in Älmhult</td>
</tr>
<tr>
<td>69-year-old</td>
<td>23</td>
<td>March 17</td>
<td>home environment, in Älmhult</td>
</tr>
<tr>
<td>46-year-old</td>
<td>34</td>
<td>March 28</td>
<td>Distance, telephone call</td>
</tr>
</tbody>
</table>

Trost (2010) argues that the researcher should strive towards achieving a subject to subject relation during the interview. This means that the researcher tries to minimize the asymmetric power relation. The interviewee should be regarded as an expert on him- or herself and the researcher is an expert in the area being studied. The Swedish poet Erik Axel Karlfeldt had an expression, which was that (paraphrased) you should talk to the peasants their way and with the scholars on Latin. This expression implies that I as a researcher should try to adjust my language to the interviewee, but not attempt to mimic the interviewee. The targeted population in this study was very heterogeneous, meaning that I needed to be cautious, so that the interviewee did not get the impression of being mimicked or debriefed. This was a balancing act, since adapting too much and trying to adopt the jargon of, for instance, an older person could be perceived as clumsy or annoying.

**3.2.3 Documents**

Seale (2011) argues that interviews are normally seen as the “real” data in research projects. However, written documents of different sorts can be informative. Seale further develops this statement by informing that documents are active agents, serving as schemes in individuals’ interplay. Documents can be looked upon as artifacts to be used, manipulated, despised or shrouded, etcetera.

Further the chosen strategy of gathering data from multiple different sources can be referred to the concept of triangulation (Wildemuth, 2009). This is an approach where the researcher for instance conducts interviews simultaneously as perusing documents, in order to draw more valid conclusions. Often, one applies some kind of content analysis to the documents gathered in order to extract meanings from them.

Electronic identification is a matter which has been comprehensively described and referred to by governmental institutions, both nationally and internationally. There are records produced by the European Union, but also by public agencies in Sweden, such as the e-ID Board. The e-ID is a subcomponent (a “back-office enabler”) of a larger phenomenon, which is e-services, which ultimately cater to the concept of e-government (Melin, Axelsson, and Söderström,
2016). Public agencies in Sweden are co-operating in order to enhance e-government, for example through their cross-organizational association of eSam, which has 25 Swedish public agencies as members. Among these are the tax agency, the police agency, the pension agency and the employment agency, to name a few. Moreover, the explicit goal of eSam is to facilitate and accelerate the digitalization of public services in Sweden (Esamverka.se, 2018).

To find out more about electronic identification and its interpretations from the governmental point of view, perusing state published reports became a natural part of understanding the reasoning behind the e-ID governance in Sweden. Including state written documents enhances the analysis, as people’s e-ID interpretations and strategies of use could be compared to the “official” interpretation of how e-IDs are meant to be defined and used (Patel and Davidson, 2011). The criteria for choosing documents were in the beginning very few. Every document including detailed accounts on e-IDs were corralled. After reviewing the study’s purpose, the number of chosen and subsequently analyzed documents were three. These were produced within three different public agencies (finance ministry, eCooperate, or eSamverka, and the e-ID Board). The reports which had as a primary purpose to recommend various types of technical frameworks were deselected, as they would not significantly add to the study’s aim of understanding people’s reasoning about e-IDs. Furthermore, the remaining documents were mostly written about issues about issues which I initiated my research process pondering on, such as how to define e-identification and who (the government or the private sector) should issue e-IDs. The documents, which contained a higher degree of policy orientation (one of which was sent to me by a tax agency official via e-mail) were marked as more “active agents” in my data collection and were thus included as empirics in the process of data analysis.

3.3 Data Analysis

In order to identify and analyze patterns in the collected data, the method of thematic analysis was applied. This method consists of six phases (Braun and Clarke, 2006). They are:

1. Familiarization with the gathered data
2. Generation of codes
3. Searching for themes
4. Reviewing the themes
5. Defining and naming the themes and finally
6. Producing the report

This analytical method’s strengths are mainly its accessibility (with a “recipe” on how to do it) and theoretical freedom (Braun and Clarke, 2016; Nowell et al., 2017). Further, in this study, thematic analysis was employed mostly as an instrument for analyzing the collected data. Further, it coheres with the study’s aim of understanding how people understand and make use of e-IDs, through its flexibility, allowing the researcher to find latent themes within the data set (Braun and Clarke, 2006). Latent themes are of interest in this study, since the objective is to understand the interviewees reasoning (social constructions) from a constructionist point of view.

The primary data in the study were the conducted interviews, hence every interview was transcribed verbatim and pasted into a column, titled ‘transcript’. The analyzed documents were read thoroughly, but coded based on summaries which I had written about them. Further, after I had transcribed all interview data, I marked the sentences with notes in another column (title
‘codes’), placed next to the transcript column. Under every note I wrote a code, which went from the combination A1 (every letter had 20 numbers, i.e. from A1-A20 and so on) to K8, which generated a total of 208 codes. These were revisited and regrouped to fit with other similar expressions. This way, the most prevalent threads (i.e. codes occurring most frequently) within the whole data set eventually became more visible.

Table 6. Three examples of the initial coding.

<table>
<thead>
<tr>
<th>Transcript</th>
<th>Codes</th>
</tr>
</thead>
<tbody>
<tr>
<td>I do not know how secure it really is</td>
<td>I do not know how secure it really is A9</td>
</tr>
<tr>
<td>One trusts it, it is just this way and BankID in itself feels quite secure</td>
<td>BankID feels secure G8</td>
</tr>
<tr>
<td>They should see that we are doing it right from a security point of view</td>
<td>Do something right from a security perspective J6</td>
</tr>
</tbody>
</table>

As is shown in Table 6, the three statements (with examples taken from three separate interviews) were each given unique codes. Further, it should be noticed that these are taken out of context and only used to illustrate the initial coding. In the example above words such as ‘secure’ and ‘security’ are present. The prevalence of these were noticed after having gathered and created all codes. When all data had been coded (new codes were applied if things were left unnoticed), the codes were regrouped and placed in several categories, such as the ‘security category’. Furthermore, I was analyzing whether the essence of the sentence(s) concerned merely for instance the security thread. If not, perhaps the sentence in question fitted better into another category, for instance the ‘definitions of e-ID’ category. As is shown in Table 7, other examples of categories created were ‘e-ID use’ and ‘convenience of use’, since many codes contained words and expressions which engendered these categories. Moreover, coding is an iterative process, highly dependent on the researcher’s own judgement and ability to analyze the data set in a systematic fashion.

Table 7. Regrouping codes and creating categories.

<table>
<thead>
<tr>
<th>Definitions of e-ID</th>
<th>e-ID use</th>
<th>Convenience of use</th>
<th>Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>e-ID is a card, but on the mobile (B11)</td>
<td>Uses e-ID for Swish (A4)</td>
<td>Nice to avoid passwords (A5)</td>
<td>Unsure about the security in e-IDs (A9)</td>
</tr>
<tr>
<td>Identify electronically. (C18)</td>
<td>Needed an e-ID to pay the invoices (D5)</td>
<td>Avoids sitting in long telephone queues to public agencies (A6)</td>
<td>The bank recommends BankID, thus it is secure (A11)</td>
</tr>
<tr>
<td>BankID is related to money and identity (E8)</td>
<td>Good idea to use BankID everywhere. (D9)</td>
<td>BankID removes passwords (E14)</td>
<td>BankID does not feel secure. Like wearing a security token (F7)</td>
</tr>
</tbody>
</table>

The process of coding can be fragmenting, and it can decontextualize meanings in the data set. However, the method of thematic analysis is iterative, which means that the researcher should revisit the first phases (familiarizing with the data set and code generation) to help minimize
interpretations which are far from the what was originally encoded in the statements made during the interviews (Braun and Clarke, 2006). Another risk associated with coding is if the researcher is trying to straighten out inconsistencies detected in the transcripts. These inconsistencies have to stay and be included in the coding process. No data set is free from inconsistencies. To level them out is to simplify things which are potentially interesting to highlight and analyze. The aim of this study is not to fit the interviewees’ contributions within a prearranged theoretical framework, but rather letting their statements (in concert with the analyzed documents) guide my thesis writing process and as Creswell neatly describes, try to render the complexity of the problem (Creswell, 2014). This means that the coding was predominantly inductive in nature, where the content in the dataset was in itself important, as opposed to coding the gathered data from certain concepts or a specific theory. Further, thematic analysis is about finding proper themes, which Braun and Clarke (2006, p. 82) define as “A theme captures something important about the data in relation to the research question and represents some level of patterned response or meaning within the data set”.

Again, the judgement of the researcher decides what constitutes a theme and not. A theme might not be directly related to for instance prevalence as in the amount of times certain things repeated throughout the data set (Braun and Clarke, 2006). Rather, the qualitative researcher controls his or her data against the research questions and towards the data extracts as well as the whole data set. Nowell et al. (2017) contended that searching for themes can be a never-ending process, stating that” it is possible to go on modifying and refining definitions of themes forever, and one of the most difficult decisions to make is where to stop the process of development”. Further, Nowell et al. emphasized that the data should be coded at least two times, and the interviews should be transcribed and re-read. As these two aforementioned things were done, one example of a recurring thread, was the issue of security which the interviewees and documents were discussing extensively, often in terms of whether or not the e-ID tokens were sufficient in this regard. The prevalence was high, both in the data set as a total, but also in individual cases. Hence, this notion was solid enough to constitute a theme. After having a set of discovered themes, these have to be thoroughly defined and refined, meaning that each theme’s essence has to be clarified and assessed regarding what parts of the data the themes represent. Further, the found themes have to be filled with detailed analyses. Furthermore, the themes should correlate with the narrative brought forward in the thesis. Lastly, the thematic analysis entails the step of writing the analysis (chapter 4), in a way which persuades the reader of the validity in the analysis, which for instance can be done through using quotes, which enrich the analysis and narrative being presented (Nowell et al. 2017; Braun and Clarke, 2006). Moreover, in Table 8 below, the final themes are presented. These were created in line with the reasoning presented above.
Table 8. The final themes, categories and codes are compared, separated, merged and encompassed in three broad patterns.

<table>
<thead>
<tr>
<th>Theme 1: Definitions of the e-ID</th>
<th>Theme 2: The personal identity number as a precondition and obstruction</th>
<th>Theme 3: Banks as the main issuers of e-IDs</th>
<th>Theme 4: The security aspect, trust and skepticism</th>
</tr>
</thead>
<tbody>
<tr>
<td>Definitions of the e-ID category</td>
<td>Personal identity number category</td>
<td>Citizens-Banks-Agencies category</td>
<td>Security category</td>
</tr>
<tr>
<td>The e-ID as more than a plastic card</td>
<td>A key, opening many doors</td>
<td>e-ID should be possessed by individuals, not banks</td>
<td>Unsure about the security in e-IDs</td>
</tr>
<tr>
<td>Something more than identifying orally</td>
<td>Something taken for granted</td>
<td>Hindering for those without one</td>
<td>The bank recommends BankID, thus it is secure</td>
</tr>
<tr>
<td>The e-ID as a valuable document</td>
<td>The number is like an admission ticket</td>
<td>The number is like an admission ticket</td>
<td>BankID does not feel secure.</td>
</tr>
<tr>
<td>Difference between identity and authority</td>
<td></td>
<td>The government should have more responsibility</td>
<td>It is like wearing a security token</td>
</tr>
</tbody>
</table>

3.4 Establishing trustworthiness

My choice of using interviews as a way of gathering data raises questions about reliability and validity, and whether my research could be replicated, i.e. if it would generate the same results if it was repeated by another researcher.

Firstly, qualitative research does not call upon a higher purpose of replicability. Within constructivism one argues for multiple realities and therefore the strive towards replicability is merely an artificial consensus promotion, argued Seale (1999). Secondly, despite the position held by constructivists, there are many qualitative interpretations of the concepts of validity and reliability. Seale further argues that a “subtle realism” is appropriate for the constructivist to exert. Within this perspective, one distinguishes between internal and external reliability. Internal reliability has to do with other researchers extracting the same core concepts from the gathered data, which the study’s researcher extracted. External reliability is arduous, since it carries the classic argument of replication, where another researcher should be able to go out “there” and receive the same results.

Moreover, Seale (1999) proposes a typology wherein the four concepts of truth value, applicability, consistency and neutrality are desirable. Truth value problematize whether the strategy of inquiry generates the real truth, for instance when interviewing. Applicability concerns if the findings from interviews can be applied to other contexts or interviewees. Consistency raises the concern whether the same results would emerge, if the same interviewee was asked the same questions, in the same setting as before. Finally, neutrality has to do with whether the answers to the research questions clearly reflects the interview questions and the interviewee, or if the answers are colored by the researcher’s own biases and interests. Now, these four concepts are debatable. They could be related to the concepts of internal validity, external validity, reliability and objectivity. Whether one labels the aforementioned typology as these things or not is a matter of what paradigm or opinion the researcher stands for.

The qualitative researcher would presumably reject the notion of applicability, with the refutation that every situation is unique. The truth value could be criticized for over-simplifying
and bearing the assumption that only one reality exists, which could be unearthed and described. Moreover, there have been efforts from the qualitative approach to replace ill-fitting concepts through attaching new concepts to the aforementioned typology. Instead of adopting the positivist approach to validity, reliability and objectivity, one could pursue Lincoln and Guba’s reinterpretation of the aforementioned concepts (Wildemuth, 2009). Instead of aiming at truth value, one aims at *credibility*, which could be ensured through for instance peer debriefing and data collection triangulation (Nowell et al., 2017). Applicability, which is referring to external reliability (in the positivist paradigm) or demonstrating that the result is applicable to other contexts than merely the own study becomes *transferability*. Further, applicability is associated with quantitative research, so to parallel this, the qualitative researcher should offer thick descriptions and let other researchers decide on the transferability (Pandey and Patnaik, 2014; Nowell et al., 2017). The concept of consistency is in qualitative research commuted to *dependability*, which is mainly about demonstrating a clear and well documented research process, which is logical. If another researcher decides to research the same problem area, he or she should have comparable (and not contradictory) results. Finally, neutrality is converted to *confirmability*. This concept builds on the aforementioned concepts and thus this is achieved when they are accomplished. It refers to the researcher deriving his or her conclusion based on the collected data, not on unaddressed biases or agendas (Nowell et al., 2017). In table 9, Guba’s (1981) chart on trustworthiness are shown with the three columns of aspect, scientific term and naturalistic term. Further, Guba was contending, like Seale (1999), that the qualitative researcher should strive to use the concepts written in the “naturalistic term” column on the right side.

Table 9. Modified matrix of Guba’s (1981) view on trustworthiness

<table>
<thead>
<tr>
<th>Aspect</th>
<th>Scientific term</th>
<th>Naturalistic term</th>
</tr>
</thead>
<tbody>
<tr>
<td>Truth value</td>
<td>Internal validity</td>
<td>Credibility</td>
</tr>
<tr>
<td>Applicability</td>
<td>External validity, Generalizability</td>
<td>Transferability</td>
</tr>
<tr>
<td>Consistency</td>
<td>Reliability</td>
<td>Dependability</td>
</tr>
<tr>
<td>Neutrality</td>
<td>Objectivity</td>
<td>Confirmability</td>
</tr>
</tbody>
</table>

To sum this section up, there still is plenty of theorizing around validity and reliability within the domain of qualitative research, partly because (unlike the quantitative research) the qualitative accounts for these two core concepts have not reached a firm agreement (Seale, 1999). However, applying Lincoln and Guba’s concepts would make sure that the qualitative research has trustworthiness (Wildemuth, 2009).

3.5 Ethical Considerations

In this study, Vetenskapsrådet’s (2002) ethical requirements were followed extensively, in order to ensure a proper treatment of the interviewees. The requirements entail providing information about the study, obtaining consent (verbal or written), not exploiting or using information gathered about the interviewees for commercial purposes and finally, I followed parts of the confidentiality requirement. Below, I will describe the measures taken in order to be in line with Vetenskapsrådet’s requirements.

Wiles (2013) argued that “Informed consent is a central concept in ethical research practice and is one of the key principles underpinning professional guidelines for social scientists”. I provided the interviewees with information via an informed consent form (Appendix A and B), which was handed out and signed before the interviews were initiated. The informed consent
form covered the thesis’ purpose, main method and the interviewees rights. There were also
details about the interview as such and it was noticed that audio recording of the interview was
desirable, however the interviewees had to check off a box if they approved of being audio
recorded. Moreover, I ensured having verbal (for the telephone interview) or written consent
before conducting the interviews. Consent is an important cornerstone in ethical research. I
strived to make sure that my interviewees were properly informed about the study and if they
had any question, they had access to my telephone number and Email address, so that they could
easily get into contact with me (Vetenskapsrådet, 2002).

Vetenskapsrådet’s (2002) fourth requirement is about confidentiality. Wiles (2013, p. 42)
argued that:

“confidentiality is taken to mean that identifiable information about individuals collected during
the process of research will not be disclosed and that the identity of research participants will
be protected through various processes designed to anonymise them, unless they specifically
choose to be identified.”

I chose to keep my contacts with the interviewees as confidential as was possible, which meant
storing the interview related material on places protected from unauthorized access
(Vetenskapsrådet, 2002). Further, I pursued confidentiality in the sense that I removed names
and strong personal features (in the data analysis and presentation of findings) which could
reveal the interviewees’ identities. In this study, the answers from the interviewees were not
dependent on having their identities disclosed, therefore names and other distinctive
characteristics were removed in the data analysis and in the rendering of my findings. By
contrast, Anders Henrikson was interviewed as a representative for an enterprise challenging
the current dominant e-ID scheme in Sweden. Therefore, I asked if his name could remain,
which I received a verbal consent for. Henrikson was the only interviewed person who
consented to participate in the study without signing an informed consent form. However, I
made sure having his verbal approval before realizing the interview.

Moreover, while researching and conducting interviews, it is important to have ethical standards
and to act in accordance with them. One example of a practical issue (occurring during my
thesis writing) was having limited time for interviewing. Although there might be limited time
to realize the interview, it is vital to let the interviewee feel comfortable in order for the person
to be able to make a genuine contribution (Walsham, 2006). One technique proven to be
sufficient in this thesis was that I as the researcher would do the talking in the beginning of the
interview, or small talk for a little while as a way of warming up. Valuable time may have been
lost by doing it this way, but the interviewee may become more comfortable and thus able to
share interesting thoughts about the studied topic.
4 Empirical findings

Below the crystalized themes are presented. It should be noted that all gathered interview and documents data, except from two interviews held in English have been translated into English by me. Further, the process of thematic analysis generated four broad themes which related to the study’s aim and research questions. The aim of this study was to find out more about the general public’s reflections on- and use of electronic identification tokens. Furthermore, the research questions are:

1. How does the general public interpret electronic identification in terms of their use and reflections?

2. In what ways does electronic identification enable or obstruct when the general public use their e-ID tokens?

Theme 1: Definitions of the e-ID

There were varying interpretations of e-IDs among the interviewed individuals. The 30-year-old imagined the e-ID to be an ID-card, but on the mobile phone. Also, he argued that the e-ID was something connected to all different life aspects, such as work, education, the insurance, medical care and so on. During the interview with the 30-year-old, he was describing how his bank had given him a card and a belonging card reader, which could be plugged into his computer with a cable. This solution was in his mind merely related to making money transfers (online) transcending 20 thousand SEK, and thus the card was not seen as an identity related token. When I posed a question regarding whether this card could be a type of electronic identification token, he at first rejected the idea and then added an explanation of his definition of an e-ID, “well, it’s absolutely personal, cause if someone has it... The card is not enough of a personal ID. It’s something you could bring to the bar and get in. But it’s not like that. What can be extracted from the quote, is the idea that an e-ID should be the equivalent to a physical ID, something enabling access to societal institutions. It is something one could use to identify oneself with at a nightspot, not merely a device enabling money transactions on the internet. Moreover, several of the interviewees had BankIDs on card and one interviewee was showing me how he used it. However, the BankID on card was understood as less personal or valuable than for instance a driver’s license. It was regarded as a token more limited to performing bank related issues only.

The 40-year-old defined the e-ID as something which was more than verbally claiming to be someone. He said, “It is more than introducing oneself orally. To use some systems or toolkits, things like that, which will be able to identify you”. Several mentioned devices, such as the mobile phone and the computer when they were asked to define the e-ID. The 21-year-old defined the e-ID as “something with which you can identify, show that you are you on the internet, with the help of internet factors and well, the app, the phone”. The 62-year-old dodged a bit as he got the (e-ID definition) question and answered that, “there is both BankID on the computer and mobile BankID and that is what I use”. There was a degree of uncertainty in how to define the e-ID. The 83-year-old answered the question with, “that I do not know, I have my bank card and that is what I use for withdrawing money”. The 64-year-old had an inquisitive attitude towards electronic identification and gave a considerate answer to the question:

“Well, I partly know what it is. I know quite well the implications of it, but I have some issues with how it works in detail. There are variants of the whole thing, you could have it on the
computer, or in the phone and there are cards and files as well. Files are synonymous to the computer. Then it is this thing with the technology, the engagement and the criteria for it to be accepted. To have a BankID that you download is only a software, but there is probably a connection between the bank and my computer. Then there is my personal identity number and my code. I have actually asked people at work and it still isn’t crystal clear to me.”

The state documents attempted to define e-IDs in a variety of ways. The report written within the finance ministry had a different level of abstraction than the writings by the e-ID Board and eSam, who reasoned more practically, as they were anchored in today’s e-identification and e-signing in Sweden. As an example, the state public report suggested using a new terminology that would separate the concept of identity from legitimacies (Finansinspektionen, 2018). In the Swedish parlance, the e-ID is called ‘e-legitimation’, with ‘legitimation’ denoting a document through which something is rendered legal or authorized. According to the state report this term is misleading, as the implications of this kind of document (which is equal to a driver’s license, etcetera) are authorization structures. Identity on the other hand, is how an individual perceives him- or herself. Hence, it is suggested that the Swedish e-ID should be re-baptized to ‘identity document’ (in Swedish ‘identitetshandling’). Further, identity controls are made through an individual to his or her identity document. The report suggests that:

“Identity and authorization should be separated. Authorities emerge from the information about an individual on the identity document being combined with a legal framework, for instance if the individual is allowed to purchase alcoholic beverages or if someone is authorized for practicing a certain profession, with the doctor as one example.” (Finansinspektionen, 2018, p.171)

Further, the report’s argument of separating identity from authorities was portrayed as a necessity, since identity is permanent, but people’s authorities vary throughout life. Finally, it was suggested that the e-IDs in Sweden should be called electronic identity documents. The 65-year-old interviewee was commenting on the e-ID in concert with demonstrating one’s authority to drive. He concluded that:

“one would not really need driver’s licenses today, because if the police officers are stopping me, I would take up my phone and show them the BankID, or some other kind of e-ID that tells them I’m allowed to drive a vehicle”

Moreover, the report published by eSam had a different perspective on the e-ID and offered two definitions. First, the Swedish term of ‘e-legitimation’ was used both as a noun and as a verb (‘e-legitimering’). Second, the term of e-identification was described. E-identification was explained as a token used by the one who possesses it, through which one shows who one is. Third, eSam defined e-identification as a control of who has identified him- or herself. Further, the first definition was explained as applicable to three matters, which are: Access (1) - The purpose is to electronically have access to information which can be handed out to the person who has identified, and the person thereby gets protected from someone else claiming to be the person in question. Leaving information (2) - To leave information electronically and thereby get protection from someone else leaving information and claiming to be the person in question. Indirect signature (3) - To issue an electronic document which is protected against falsification and denial of signature analogous to the way a document would have been signed on paper (eSam, 2017). The legal reasoning was present in two reports (eSam and the state public report), both stating that e-IDs with higher trust levels should be considered as charters, defined by the second chapter in the Freedom of Press Act (in Swedish ‘Tryckfrihetsförordningen’). Further, the e-ID tokens which are classified as being on the trust levels of 3 and 4 (BankID is on level
Further, the three state reports covered different aspects of signing documents electronically, as this is one vital function integrated in the Swedish e-ID solutions. Despite this function being part of the BankID, signing electronically was merely mentioned one time in the total of eight conducted interviews. The 65-year-old interviewee briefly described how filling in forms was easier nowadays, because the forms would not have to be signed by hand. The e-IDs made it possible to sit in the home (located in the countryside) and sign documents electronically. The 65-year-old saw this as a major advantage, as the alternative was signing by hand and sending the papers away in envelopes or visiting the public agencies offices physically. Further, Anders Henrikson, the co-founder of the IT security company Verisec, contended that the population in Sweden may be the only one in the world understanding the advantages of using electronic identification, as it makes people’s lives easier. Furthermore, Henrikson compared the status of Sweden to other European countries. He stated:

“England, Spain and Germany have not at all come as far and they do not understand how useful it is. Instead, they are still working with 20 different solutions, where not a single one has become anything worth mentioning and it makes the situation much messier there.”

4.1 Theme 2: The personal identity number as a precondition and obstruction

One pattern which was recurring in the data analysis was the significance of the Swedish personal identity number. This number was for instance perceived as a key to accessing societal services, which are provided by the Swedish government. Further, this number was perceived as a requirement and a bar marking either the inclusion in- or the exclusion from the Swedish society. However, this number seemed to be internalized and undisputed in the interviewed swedes’ consciousness. Until I interviewed the first immigrant, the notion of giving people a key and registering them in the form of an identity number was never properly integrated in my own thinking. However, this theme was found and pursued after having iteratively analyzed the data set. The swedes who were interviewed never questioned the function or importance of a personal identity number in Sweden. They simply mentioned the number as they attempted to explain their ways of using the e-ID. This number was framed as a precondition, which together with a password (or fingerprint) constituted the mobile BankID. Hence, e-IDs were understood as something highly associated with one’s personal identity number.

The personal identity number was problematized as the 30-year-old interviewee (who lacked a personal identity number) compared Sweden’s identity systems with his homeland’s (Iran) systems. He expressed that his residence in Sweden was obstructive, with the statement “it doesn’t matter if I have a valid Visa or a passport, I cannot be identified as a normal person here”. Instead of being allocated one unique and valid number, which is stored in both private and commercial organizations’ databases, he claimed to have received five unique numbers. Further, these were to be used in different contexts, e.g. for visiting the doctor’s office or for opening a bank account, and so on. However, without the more valid personal identity number, the opening of a bank account and other bank related tasks were difficult. Despite the difficulties, he was hopeful after scrutinizing one of the Swedish bank’s paragraphs. He explained that, “I found one exception and I just persisted on that one. I tried to make it big in my life and based on that I convinced my bank... And I got the e-bank”. Still, this meant half of a victory for him. The e-ID in the form of a mobile BankID was not possible to acquire until
the personal identity number had been given to him. Until then he had to use a four digits code to login with on his internet bank.

The other interviewed immigrant, who was 10 years older and had also emigrated from Iran approximately at the same time period as the 30 year-old-man. He received his personal identity number two months after arriving to Sweden. However, the systems in Sweden and in particular the banking system was difficult for him to grasp. He remembered his process of acquiring the e-ID as cumbersome, something which he could not repeat on his own if he needed to. He stated that:

“Actually, it was very difficult for me, because the country which I come from is totally different, in terms of systems used. These days the systems over there are improving, but not like here. We do not use BankIDs, or things like that.”

The 30-year-old Iranian regarded himself as someone standing in the middle of two different cultures and was able to understand that the two countries had varying ways of identifying their populations. In his home country, the physical presence and family name was more significant than numbers. In Sweden, this number meant everything, i.e. having both rights (e.g. the right to vote or receive subsidies) as well as responsibilities (e.g. paying taxes). These cross-cultural experiences as well as the mistake of applying for a one-year Visa and thereby losing the opportunity of receiving a personal identity number quickly had informed his opinion about the personal identity numbers. He further explained that he socializes a lot with other newly arrived immigrants through attending so-called language cafés, where he meets people with different cultural backgrounds. He perceived the older immigrants as a major issue in terms of their cultural backgrounds and not being able to understand the administrative and digital elements embedded in the Swedish culture. While discussing the personal identity number, he stated the following about the older immigrants he had met:

“for them there’s no difference between that number and a telephone number. For them it is like you have to have it, otherwise you cannot get in and get services from society. So, they leave the analogue world and jump into the digital world. It is not at all easy.”

The views on personal identity numbers differed between the public agencies. The state public report argued that only those with a connection to the Swedish society would be entitled to have a state issued e-ID. Historically, those having a connection to Swedish society were those who were registered in the population register. Further, the function of the co-ordination number, which was implemented January 1st in the year of 2000 and issued by the tax agency, was explained. The reason for implementing an alternative to the personal identity number was that the latter was regarded as an admission ticket to the Swedish welfare state (Finansinspektionen, 2018, p.196). Apart from addressing state issued e-IDs, the state public report did not comment on private institutions’ e-ID issuance.

4.2 Theme 3: Banks as the main issuers of e-IDs

During the data gathering process it became clear that the current situation in Sweden was excluding several groups, which may need to have an electronic identification token, in order to access various public agencies’ web-based services. The excluded groups were said to be immigrants, children under the age of 13 and those without a bank account in one of the banks who are issuing BankIDs. Verisec’s Anders Henrikson was skeptical towards the present state in society of using merely the banks’ solution for electronic authentication and signing. Further,
Henrikson argued for shifting the power dynamics, moving the focus from banks to citizens and individuals, who for instance lack a personal identity number. Henrikson argued that it should be up to the people living in Sweden to decide how and where to use their e-ID tokens.

“An e-ID is the possession of the citizen or the individual and only this person decides what it can be used for... With BankID all kinds of services are connected, which have the right to access your BankID. They decide whether the social insurance agency or if a playing site could access the e-ID. We say that this is up to the individual” (Anders Henrikson, Verisec)

Henrikson’s perspective on e-IDs was contributing with a new angle in the gathered data, because no other interviewee or report was arguing for the e-ID as the possession of the individual, as opposed to being owned and governed by a bank oligopoly as identity providers (Söderström, 2016). Henrikson continued to explain the motives of the banks:

“They created a solution which primarily was for logging in to an internet bank and they have a lot of requirements on what they are supposed to do from the banking regulations... They regard it like this, we have become this big, that means people will have to comply and use our solution on our terms... There is no transparence in that solution, because there have never been any requirements.”

Moreover, Henrikson argued for an increased state responsibility, where the control over electronic identification is taken back. He argued that the national e-IDs has to be approved of by the Swedish state (i.e. the e-ID Board) and its e-ID framework. Moreover, objections to the current e-identification scheme, (where banks are the major identity providers) were also found in two of the analyzed state reports. Both in the state public report and in the report from the e-ID Board, there were suggestions stressing that there need to be state issued e-IDs. For instance, the e-ID Board argued for having the Swedish migration board issuing e-IDs for newly arrived immigrants. This way, all contacts with public agencies would occur digitally.

“Municipalities, public agencies and other social institutions have a great interest in the digital path to be the primary alternative also in contacts with newly arrived immigrants. The digital have a potential to simplify also for the newly arrived immigrants” (e-ID Board, 2017, p.31)

Additionally, it was contended that people should carry several e-ID tokens from different e-ID issuers, in order to have alternatives in case there would be system crashes. The state public report elaborated on the issue of having several electronic identification tokens and argued that, “The individual is forced to create strategies in order to minimize the risk of being without the possibility to identify electronically” (Finansinspektionen, 2018, p.67). Further one strategy could be to have e-IDs on several mobile devices. Also, the individual could acquire e-IDs from different providers. The report also stated that the banks should maintain and supply older techniques which are planned to be phased out. Further, it was claimed that individuals for convenience reasons want to possess only one electronic identity document, which could be used in all contexts. However, this idea was rejected, since the security is said to be higher when spreading out the risk and placing the individuals’ different authorities on several different solutions. Further it is argued that there needs to be a basic electronic identity document, which “everyone” could acquire, which could be utilized to re-create a lost electronic identity document.

Aside from the argument of a state issued e-ID, most interviewees regarded today’s situation with banks as the main e-ID providers as a bit strange, but not as a constraint. The most common reaction against today’s situation was that of the use aspect. All interviewees, except from the
man lacking a personal identity number, used their BankIDs in order to login on different public agencies’ websites. At the point where the actual usage of the BankID became manifest for the interviewees, they begun to reason about today’s situation. Some thought about the market-based e-ID as a matter of providing society’s citizens with a highly secure solution, good enough to use in sensitive matters such as filing taxes or applying for grants on the social insurance agency’s website. Apart from these thoughts, there were also more critical thoughts shared during the interviews. The 64-year-old said:

“I think they have tried out different trajectories throughout the years. Telia and BankID and someone else... This does not hang together, which I think is a pity. It would have been better if there was one which could have, well, like a public agency who would have issued these things”.

Moreover, it was common during the interviews for the interviewees to begin speaking about bank related artifacts, such as the bank card, while being asked questions about e-IDs. The e-ID was associated with their bank and its services, such as the Swedish payment system Swish. The e-ID was also summarized as something highly associated with economics. Even though it was used for logging into various public agencies’ websites, the main goal was to manage the personal economy, as the tasks managed after using the e-ID were related to the income or the pension, etcetera. Hence, it made sense for most of the interviewees to use the banks’ system to authenticate and sign documents with.

There was an element of haste in the state written documents. The underlying factor inciting this eagerness to address the e-ID, its constituent parts and function seems to be digitalization and the increased requesting for the public agencies to have a fully digital administration. The eSam report (eSam, 2017, p.15) stated that “e-identification and e-signatures are fundamental services in order to be able to achieve a real digitalization”. Further, the digital contacts between state and citizen are enabled via the populations use of the BankID. However, the e-ID Board contended that there needs to be a state provided solution as this would consolidate a societal robustness. Further, the e-ID Board claims that the state issued e-ID (emphasizing the fundamental identification) will proactively hinder frauds from occurring. Another argument is that Sweden would then have e-IDs which would be in compliance with the eIDAS regulation, where the European Union-approved national e-ID solutions will be valid to use in other EU member states.

4.3 Theme 4: The security aspect, trust and skepticism

Most interviewees mentioned security before being explicitly asked about it. This subject was nearly always portrayed as a distrust towards people, not the e-ID infrastructures. The interviewees feared having a conman behind their backs while using their mobile BankIDs. They also feared more advanced criminality, implying that people who are behind the systems could have malicious agendas. This fear was connected to public agencies and previous scandals, which have been published and amplified in various media outlets. The 69-year-old stated:

“The system I trust, but the crap behind it... You can never trust people. I guess it is supposed to be secure. But when one hears that the public agencies are sloppy with who is authorized to check their computers and so on, then things could occur that we know nothing about.”
The 62-year-old suggested that the e-ID could be used for was electronic voting. Further, he suggested that this had been done in the neighboring country of Denmark and therefore it would potentially be applicable to Sweden. However, the 18-year-old his pupil had objections to this idea. The pressure from peers or family, the 18-year-old thought posed a risk, implying that e-Voting is not cast iron. The e-ID token as such may be secure, but it may imply other challenges. The pupil said, “I’m thinking that voting from the home environment could be negative. Perhaps someone does not feel safe in the home. So, going down here makes it totally private who you choose to vote for. Moreover, the 62-year-old continued to reason about the risk of voting electronically. He concluded that voting in Sweden is something private, a sensitive domain which people never discuss in public. Further, he connected the reasoning about e-Voting to the threat of identity theft, adding that he does not know how often electronic identities are hijacked.

One strategy in minimizing the risk of identity theft and web-based attacks is to live simpler and use the mobile phone less than what other people usually do (as this device do not have the proper firewall as the computer do). Moreover, the 64-year-old interviewee was firm in his belief that the current supply in terms of technology has exceeded every reasonable boundary. He contended that there that there are too many web-based platforms and technological innovations for us to discover and adopt. There is pressure created from the web-based platforms, as they for security reasons usually recommend or demand the use of ingenious passwords, which (also for security reasons) should not be written down and kept in a drawer or an excel file. The password issue was regarded as a real dilemma, as there presently is a large number of websites requiring unique passwords, which because of cognitive reasons need to be set down on paper.

The 64-year-old man also mentioned the attacks made by slick deceivers who use people’s benevolence against them and empty their accounts, through merely two telephone calls. The man explained he had heard about frauds while listening to the radio. To him the security threat was most imminent to those who were customers in Nordea bank (who uses mobile BankIDs), not in the bank where he was a customer. His explaining about the fraudulent activities was complex and he went back and forth and was repeatedly asking if he was correct in his observation. His interpretation of the frauds was:

“Apparently they are going in on login mode with your personal identity number. They call you and say that there is a security risk, so they ask if you would be kind and login to your internet bank for a control and blocking of the hijacked account. Well, they become nervous, as one would be, and they will type in their code to their BankID and then the person who first accessed will go in through your BankID.”

The eSam report partly had its point of departure in the wave of e-ID frauds in Sweden and the mistrust it could create among for instance BankID users (eSam, 2017). Consequently, the report addressed fraudulent crime, through providing examples and explaining the implications of each example in a chapter about abuse and culpability. One example was topical as it relates to the contemporary wave of identity crimes (i.e. spoofing). The deceiver is abbreviated with the letter B:
“Sometimes B also tricks the e-ID user to grant access for B or B’s robot through the user authenticating unknowingly of that B or B’s robot has been typing in the user’s personal identity number on a certain website. – The user’s consent to or power of attorney for the person who erroneously is granted access is not discharged of responsibility because culpability is prescribed to the one who is untruthfully invoking identity documents” (eSam, 2017, p. 46)

Important to note from the quote above, is that neither the e-ID user nor the deceiver (“B”) are considered as discharged from responsibility in a situation like the exemplified. If the e-ID user “lets” another person login on for instance his or her internet bank, this means that he or she has to take the consequences of allowing this to happen. Further, the state public report suggested a change of terminology in order to differentiate between logging in and identifying (Finansinspektionen, 2018). The current interfaces used on most Swedish public agencies websites suggests that users are employing their e-ID as one method of logging in, in order to access information protected from the public. The report discouraged this wording as it suggests that electronic identification is synonymous with logging in on a website. Moreover, it was argued that the e-ID user was employing a valuable document through which he or she authenticated him or herself. Further, the interface of BankID was addressed as something confusing, because it does not differ sufficiently between identifying or signing in the mobile device application. It was argued that people do not fully understand that they are signing a charter of their identity. Rather, the report claim that the interface is designed as one is merely authenticating oneself (eSam 2017).

Security issues were manifest in the analyzed reports. There was an emphasis on increasing the state involvement in electronic identification, in order for the e-ID scheme to become more secure. The analyzed documents contained multiple paragraphs on the e-ID issuing as such and highlighted the importance of being sufficiently identified before being able to acquire an e-ID. The Swedish word “grundIdentifiering” was used frequently to refer to the primary identification of a person. This occurs through a physical meeting when a person is traced back to the population registration, to know whether he or she is qualified to possess an electronic identity token. This procedure was framed as a central component in building trust for electronic identification. Henrikson referred to the procedure, which must occur through a physical meeting as it is regulated by Swedish law. Further, he prophesied that this process will occur digitally in the future, as the data included in the future physical ID cards will be stored in a database, which allows for a totally digital identity control procedure.

Further, the e-ID Board envisioned a future where we people are using more secure e-ID tokens, by presenting consisting of three comprehensive cornerstones (see Figure 2). The e-ID Board was arguing for a holistic view on the issue, emphasizing that each and every cornerstone’s descriptions must be achieved, in order to create a robust infrastructure. Moreover, this representation of an envisioned e-ID, is one subset to a larger issue. The e-ID Board was essentially commenting on digitalization and thus electronic identification as an enabler for digitalization (The e-ID Board, 2016).
The state involvement in an e-ID solution was not entirely seen as a necessity by some interviewees. The 30-year-old man from Iran was skeptical towards eventually having to adopt an e-ID, essentially because of his low level of trust towards the government. He ended the interview session by concluding that:

“I do not want the state to know everything about me. It is everything here, the e-ID... I do not want to have it sometimes. I will have to adopt it, but still I will remain a skeptic. As soon as you give them (the state) your identity, you give them everything”
5 Discussion

Electronic identification has been analyzed and criticized from several perspectives. Academic literature about e-IDs have touched on topics such as biometrics, security, privacy, usability, pseudonymisation, infrastructures, state surveillance, legal barriers, pan-European schemes, forms of e-IDs, adoption, sociotechnical issues, governing of e-IDs, and so on. These concepts will be used in the discussion in concert with Söderström’s four sub-concepts of identity, identification, authentication and authorization as a theoretical foundation. Now it should be emphasized that this study is inductive in nature, with the results of the data analysis guiding the discussion. Below, in Figure 2 the three categories created from the body of literature are shown and the relation to the e-ID individual user. The three categories carry technical, legal and social premises which informs the individual’s use of electronic identification.

![Figure 3. The three aspects e-ID and their relation to the e-ID user](image)

5.1 Interpretations of the e-ID

The interviewees shared many thoughts about what constitutes an electronic ID. One interviewee was defining it as a tool which was more than verbally claiming to be a certain person. This reasoning lies in between the concepts of identification and authentication, where the interviewee was alluding to authentication, while describing identification (i.e. to merely claim and not prove to be someone). When answering the question of what an e-ID is, they often mentioned the kinds of mobile devices they employed while authenticating, such as the smart phone or the tablet. This implies that electronic identification is something highly associated to the hardware of choice in authenticating. Moreover, all interviewees (except from one) used e-IDs which are soft solutions, i.e. apps in mobile devices or on file in the computer. There were several interviewees who owned e-ID cards. However, these seemed to have a marginal role in the everyday electronic authentication and was put in drawers collecting dust.

Several interviewees associated their e-ID tokens with the banks, where they had their accounts, and services offered to them besides this. In this regard, the e-ID was related to identity,
implying a unique combination of attributes. The e-ID was also associated as being something more than merely enabling money transfers on the internet. The fourth concept (authorization) in Söderström’s (2016) conceptualization became apparent when the 65-year-old interviewee, commented that an e-ID should be the equivalent a driver’s license which signals a certain kind of authority. Moreover, the terminology used in Sweden to denote e-IDs was also questioned. The state public report proposed a change of terminology so as not to confuse e-IDs with authority structures, which are instantiated in a driver’s license. The driver’s license is signaling that the car driver has undergone an adequate education in order to become certified to drive a car. Instead, the state public report argued that the e-ID merely should be seen as (electronic) identity, defined as related to how an individual regard him or herself.

The public agencies wording of accessing their web-based services were also criticized as something being misleading. Using the terminology of “logging in” could mislead people into thinking that they are merely logging in somewhere with a made-up username and password, as opposed to authenticating themselves with a valuable document, which through the constitution could be considered as charter. Further, the state public report encouraged the public agencies to change their interfaces’. The state public report’s reasoning corresponded with how most of the interviewees were perceiving the e-ID. Essentially the interviewees regarded it as an instrument used to conveniently logging in on different digital platforms, minimizing the stress of remembering a myriad of passwords (which has to be written down on paper). The perceived purpose with the e-ID could further have implications on use aspects. Henrikson’s comment that the population in Sweden may be the only one in the world to have recognized the utility of e-IDs may not necessarily mean that they have understood the real function of the e-ID as it is currently (legally) operating, i.e. both for authentication and signing electronically. Other than people seeing the advantage of avoiding passwords on plenty of digital platforms, I observed during my bank employment during 2017 that the e-ID was shared with family members or friends, which indicated that the electronic identification document did not have the same significance as for instance the driver’s license. This experience could be linked with the 30-year old interviewees’ testimonies from attending language cafés and socializing with several elderly immigrants, who according to him did not thoroughly comprehend the differences between a telephone number and the personal identity number.

Moreover, there was an element of frustration when on interviewee was unable to define the e-ID and grasp the infrastructure of it. His guesswork further created an ambiguity towards whether the solution really was waterproof, especially since the wave of BankID frauds had been going on in Sweden for several years. The reviewed scientific articles, which developed the technical discourses on e-IDs, embarked on issues such as security in authentication. However, the intricacies of different e-ID infrastructures create questions about for instance security and pseudonymisation, and whether those things can be assured when most e-IDs are based on numbers which different countries use to identify their citizens with. This discussion was however rather distant in the collected interview data, which as a whole suggested that people use e-IDs for convenience and also because the bank or the public agencies have recommended them to use it.

5.2 Peoples trust in societal institutions

What was clear after reviewing the data set was that the interviewed individuals, in particular the interviewees born in Sweden, had a high level of trust towards societal institutions, such as the Swedish banking system. The comparatively high figures in the use of BankIDs indicates
in accordance with McGraths (2016) ideas on trust, that there is more of an ambivalence (if any at all) in Sweden than suspicion, which characterizes failed e-ID implementations.

However, there were those who did not think that the current electronic identification scheme in Sweden was reasonable. The 64-year-old interviewee was questioning why e-IDs were not issued by one designated public agency, instead of the banks dominating the market. The analyzed documents shared this objection and referred to societal robustness in their argumentation of why there should be e-IDs issued by the Swedish public agencies. Further, the exclusion of immigrants was problematized, and it was suggested that the Swedish migration board should provide newly arrived immigrants with e-IDs.

There were new insights deriving from the interview with Anders Henrikson. The company he represented (Verisec) wanted to challenge the current dominant e-ID scheme, through discussing the current state where the used e-IDs essentially are the possession of banks. The banks are surrounded by legislation and interests which impact on how the users can use their e-ID tokens. For instance, people cannot review when their BankID was used the last time or the transactions made with it. Henrikson argued in line with Eaton, Hedman and Medaglia (2017) that there had been a laissez faire approach from the Swedish state’s side, and that there needed to be increased state supervision in this regard. The banks had according to Henrikson refused being properly audited by the e-ID Board. Further he claimed about BankID that “There is no transparence in that solution, because there have never been any requirements.”. Instead, this solution was so well established that the responsible for this system could do as they pleased. Since there is a perceived lack of transparence in the BankID infrastructure both from Henrikson and a couple of other interviewees, and because it is as dominant as it is, there is little room for evaluation. This applies to both users as well as the public agencies, which through the trade-off of financialization have had a less active role (i.e. a laissez fair approach) in the national e-ID scheme. It is the banks and their company Finansiell ID teknik AB, who are owning the e-ID in Sweden.

Henrikson contended that this ownership should be relocated to the individual, i.e. not be in the hands of banks (or other market actors), who currently controls the e-ID. The existing power dynamic could be associated to factors such as politics, economics, technology, culture and social life, through which distinct national e-ID schemes are shaped (Eaton, Hedman, and Medaglia, 2017). Further, it is through the process of financialization that national e-IDs emerge. Eaton, Hedman, and Medaglia compared Sweden to Denmark and Norway and concluded that every country has its own ways of skinning the cat, however there were three general components included in the process towards achieving national e-ID solutions. These were: common e-ID solutions not considered, common e-ID solution desired and finally common e-ID achieved. The researchers mentioned that what was striking in Sweden was the large adoption of BankIDs as the Swedish real time payment system Swish was launched. Further, this corresponds to the gathered interview data, which suggested that many used BankID partly because of wanting to use Swish.

From the interviewees point of view, having the banks or private sector issuing e-IDs was not a major dilemma. All interviewees had bank accounts in BankID issuing banks. Further, all interviewees, except from one person used BankID. All using BankID, used the mobile BankID on their mobile phones or tablets with the exception of the 64-year-old interviewee, who had made the conscious decision to only use BankID on file, for security reasons, as the computer was assumed to be more secure than the mobile devices. Further, he was critical towards the
current model of letting the market be identity providers. It should be one, in his opinion, in order to have a more cohesive or logical national e-ID scheme.

5.3 The personal identification number as an enabler and obstruction

There is a long tradition in Sweden of registering people and controlling them towards the population register. Moreover, people have historically been accepting towards having their personal data stored in databases, both in the public and in the private sector.

The interview with the man lacking a personal identity number was highlighting the issue of being included or excluded from the Swedish society. Those who are born in Sweden are automatically recorded in the population register and given a unique number frequently used in different situations, both in the public and in the private sector. Without this number, a resident in Sweden who lacks one may become excluded, and this for instance marked through not being allowed to acquire and use an e-ID. Eaton, Hedman and Medaglia (2017) emphasized that even though the registration of people implies responsibilities, most immigrants aspire to be perceived as legal, and claim a legal identity. The public administration in Sweden is comprehensive, but it differentiates between those having a “connection” to the Swedish society, i.e. those who are in the population register and those who do not have a connection (even if they are employed and working). Further, the cooperation number is a threshold, because the personal identity number is seen as an admission ticket, something coveted by all outside of the system. However, with an increasingly digital administration, the situation for those who are not in the population register presumably becomes increasingly difficult. Further, if the e-ID is perceived as something used in almost all Swedish people’s different life aspects, then not having one will become a bar marking if one is in or outside of the system. In the case of the 30-year-old man, there were comparisons made and thus deeper philosophical thinking about this number which nearly every Swede has and do not question the function of. In the home country, the physical being was said to be a much stronger way of identifying than any physical identity document.

Further, the present technological schemes were not as advanced as the technology of BankIDs etcetera. The use and non-use of electronic identification methods could be related to a country’s current use of ID documents (Lentner and Parycek, 2016). A country where the population identify through verbally claiming to be someone or referring to the family name, etcetera, could have problems in adopting e-IDs as these are dependent on the available physical ID documents. For instance, in countries where ID-cards are common or mandatory, the e-ID scheme can be in the form of physical cards with a chip on them.

5.4 Security and skepticism

The interviewees and perused documents clearly indicated an established thought pattern in relation to technology, as the e-ID. Most interviewees began to speak about security before any questions had been posed about it. It often came as a subordinate clause, the 21-year-old interviewee said during the interview that “the e-ID is so convenient for me to use, but I do not know how secure it really is”. Whether or not the security thread was an authentic concern, or a thing stated for the sake of it, was not clear from these kinds of statements. Arguably, individuals could choose not to use things which were authentically experienced as threats.

Furthermore, the lack of knowledge in how the identification systems were designed, seemed to be one explanation to the ambiguity related to the use of the BankID. Most interviewees
generally had a high level of trust towards the banks and other institutions. Hence, they motivated their use of BankID from this point of view. However, there was an element of distrust towards public agencies, with the 69-year-old interviewees’ referral to clumsy handling of sensitive data by some public agencies. Indirectly this distrust was also directed towards the banks (or Finanssiell ID-Teknik Bid AB) as this also was an example of the distrust targeted towards people who are behind the technical systems, as these were perceived as not being trustworthy with assumed hidden agendas. With a certain amount of distrust, the ambiguity could be converted to suspicion, which is characterized mainly by negative sentiments, argued McGrath (2016).

The most prevalent fear was being deceived in some way. Because of not knowing in detail how the slick deceivers go about the ID hijacking, this increased the ambiguity. The 18-year-old interviewee thought it was more unsafe to carry the mobile phone with him, which has the mobile BankID installed on it, than carrying his security token, which he received from his bank. The reason for this was that the security token was perceived as being more advanced and secure than the mobile BankID.

The most imminent fear was having someone standing behind one’s back and memorizing the passwords when using the mobile device and BankID. Another fear was slick deceivers calling on the telephone and manipulating people into committing erroneous actions. The rise of discussions about biometrics in academia may have risen partly as a consequence of the fraudulent crimes, which many people for instance in Sweden have been victims of. The systems may be more secure than merely using for instance a username and a password (such as single factor authentication, e.g. using an email address and a password). Moreover, the discussions about biometrics were not totally free from problematisation, as the data always needs to be stored somewhere. As was dealt with in for instance Turkey, the state issued e-ID’s card access device was initially supposed to store people’s personal data in the databases of private companies (Bostan, Şengül, and Karakaya, 2017). This solution was questioned, and it was suggested to create a solution where the data would be stored by the state instead. However, one threat being explored in some academic articles about e-IDs was that the state could begin to govern based on identity (Whitley, Gal and Kjaergaard, 2014). Furthermore, the horror of mass surveillance and was present both in literature on e-IDs as big amounts of data are being stored in the different states’ databases. This fear of being monitored by the state was also present in the interview data, best described by the 30-year-old man who was standing in somewhere in between the two nations of Sweden and Iran and who longed for receiving a legal identity. His message was that “As soon as you give them [the state] your identity, you give them everything”.
6 Conclusion

6.1 Conclusions

As was crystallized in chapter 4, the interviewees and documents had different ways of defining the e-ID. However, the e-ID token was mainly perceived as something more than simply verbally claiming to be someone. It means that the e-identification is more than asserting for instance that I (Annie) is someone. Rather, Annie is somehow proving to be the Annie writing this particular thesis (i.e. authenticating) instead of merely identifying (i.e. simply claiming to be someone). Further, one of the interviewees mentioned signing electronically, however this was a marginal interpretation of what the e-ID is and was not given a significant amount of attention during the interviews, as in contrast to the three documents which expanded on electronic signatures. The signature aspect was criticized by the eSam report, which contended that there are deficiencies in mobile BankID in terms of separating authenticating from signing, which are not sufficiently separated (both sharing nearly the same interface). Moreover, most interviewees regarded the e-ID as the first-alternative to use while logging in to public agencies web-based services, paying the invoices (in the internet bank), or making various payments, etcetera. The mobile BankID was regarded as a convenient tool. Several interviewees also mentioned the advantage of BankID reducing the hassle of remembering passwords. Further, the BankID was perceived as something used to login with, rather than authenticating. This perception was picked up and criticized by the state public report which encouraged the public agencies to change their interfaces, so that the users would not think that BankID was merely a login method.

Further, most interviewees got the impulse of mentioning security in relation to the e-ID. Mostly this notion was referred to after praising the mobile BankID, as if the mobile BankID was almost too good to be true. Some interviewees were arguing that people behind the system could have malicious agendas. Also, what was feared was the wave of BankID frauds which has been going on in Sweden for several years. With these notions being left unnoticed or neglected it could lead to a suspicion spreading throughout society, as was argued by McGrath (2016).

Moreover, the personal identity number was regarded as a fundamental enabler (in the current e-IDs) by people born and raised in Sweden but also as an obstruction. The 30-year-old man from Iran who lacked a personal identity number was critical towards having a number as the primary way of identifying oneself. In his home country, his character or family name was the common way of identifying oneself. Despite this critical position, he had the objective of attaining a legal identity as soon as possible, since this would make him enrolled in the system and have a connection to it.

6.2. Contribution

From the beginning of my thesis process it was obvious to me that I would attempt to contribute to the social dimension of Information System (IS) research, emphasizing user perceptions in relation to the designated technological artifact. More specifically, I was interested in knowing more about the general public’s reflections on e-IDs, as this angle has been understudied. The experiences I made while working on a BankID issuing bank, in concert with many read news articles about the BankID frauds in Sweden, was vindicating this thesis’ raison d’être. Further, I decided to regard e-IDs as a socio-technical matter, i.e. that e-IDs are highly dependent on the meanings people ascribe to them. Practically, it meant that instead of entering the thesis process
with a one-sided notion of the e-ID as an isolated or fixed object, I focused on how the general public, Anders Henrikson from Verisec and public documents made sense of e-IDs. In order to have a concept to compare people’s reflections of the Swedish e-ID solutions with, I decided to use Söderström’s (2016) conceptual framework of electronic identification. Further, the e-ID has different definitions depending on the researcher’s motivations, hence Söderström’s definition of electronic identification as the four generic sub-concepts of identity, identification, authentication and authorization offered a template, together with topical e-ID issues for discussing people’s notions of electronic identification.

6.3 Future Research

In Sweden, the BankID (specifically the mobile BankID) has become the dominant e-ID system, since it is adopted and used by many people. People seem to think it is a convenient tool, with its implication of reducing passwords etcetera. However, the notion of BankID as the only alternative for electronic identification should be challenged and further investigated. For the sake of finding more varied and accurate interpretations of electronic identification, one should actively target a larger population in order to have a fuller understanding of how the “general public” reason and use e-IDs. Further, those who consciously choose not to use the technology in question could be targeted and preferably interviewed in-depth. It should be further researched how the present analogue alternatives to using the BankID are changing, since the governmental agencies rapidly are altering their services to fulfill their agenda of ‘digital first’.

Moreover, on a higher dimension, the Swedish public agencies’ agenda of ‘digital first’ could be researched through studying the general public’s reflections about this shifting landscape of analogue services becoming increasingly digital. For instance, one could follow Söderström’s encouragement of studying how people increasingly are adopting digital identities, in contrast to merely using e-IDs in a tangible way, that is in the form of cards or mobile applications related to specific mobile devices and as a convenient way of logging in on different websites.
7 References


Cato, C., (2018). Bankernas ansvar vid bedrägerier ska utredas [The banks’ responsibilities in frauds is to be audited]. SMP, p.16.


Skatteverket.se, (2018). *Samordningsnummer [Coordination number]*. [online] Available at: https://www.skatteverket.se/privat/skatter/internationellt/bosattutomlands/samordningsnummer.4.53a97fe91163dfce2da8001279.html


Wiles, R., (2013). What are qualitative research ethics?. London [u.a.]: Bloomsbury Academic, pp.9-54.

Inbjudan till medverkan i en studie om e-legitimationer

Studiens författare: Annie Göransson 073-810 65 24 ag222mi@student.lnu.se

Mitt namn är Annie Göransson och jag studerar informatik på masternivå, vid Linneuniversitetet i Växjö. Under vårterminen 2018 kommer jag att skriva min master-uppsats i ämnet e-legitimation samt hur allmänheten i Sverige uppfattar och använder den.

Information om studien
Ämnet e-legitimationer är aktuellt, då människor i allt större utsträckning använder sig av sådana gentemot sin bank och myndigheter, m.fl. Myndigheter digitaliserar sina verksamheter och e-legitimationen blir en viktigare komponent (en ”möjliggörare”) för att nå deras internetbaserade tjänster. I dagsläget använder sig många människor i Sverige av ett så kallat BankID, vilket hämtas genom banken som man är kund hos. Jag är bland annat nyfiken på hur allmänheten i Sverige ställer sig inför att behöva gå genom sin bank för att skaffa en e-legitimation. Mitt övergripande syfte med studien är att bättre förstå den breda allmänhetens användning och åsikter om e-legitimationer i Sverige. Studien kommer att publiceras i databasen DIVA.

Din medverkan

Några allmänna upplysningar:
- Du kommer att anonymiseras i studien, dvs ditt namn inte syns i rapporten.
- Intervjun spelas in, om samtycke till det har getts. Inspelningen lyssnas enbart igenom av undertecknad.

Om ovanstående information godkänns av dig, vänligen kryssa för ett av alternativen och signera nedanför.

☐ Ja – ljudinspelning är okej.
☐ Nej – ljudinspelning är inte okej.

53
Invitation to participate in a study about electronic identification
Researcher: Annie Göransson 073-810 65 24 ag222mi@student.lnu.se

My name is Annie Göransson and I study informatics on master level, at Linnaeus University in Växjö. During the spring semester of 2018, I will write my master thesis on the topic of electronic identification and its interpretations and use by the general public in Sweden.

Information about the study
The subject of electronic identification (eID) is topical, as people increasingly are using their eID tokens towards their bank and public agencies, etcetera. Public agencies are digitalizing their operations and the eID token becomes a crucial component (an “enabler”) in accessing their e-services. Today, many people use a so-called BankID, which is acquired through the bank where one is a customer. I am interested in, for instance, what the general public in Sweden think about having to engage with their bank to acquire an eID token. My overall purpose with this study is to better understand the general publics’ use and opinions about electronic identification tokens. The study will be published in the database DIVA.

Your participation
I have chosen the interview method to better understand what people think about electronic identification tokens. Interviews provide me with useful material to analyze this social issue, i.e. people’s interpretations of electronic identification. The duration for the interview will be around 30 minutes. I you don’t want to answer questions or withdraw, that is okay. You also have the right to have your contributed material erased before the study has been published.

Some general instructions:
– You will be anonymized in the report, meaning that your real name will not appear in the report.
– I will audio record the interview, if you give your consent. The recording will only be used by me when transcribing the interview.

If the information above is approved by you, please put a cross in one of the boxes and sign below.
☐ Yes - audio recording is okay.
☐ No - audio recording is not okay.
Appendix B - Interview guide non-e-ID users (in Swedish and English)

Definition
Vad är en e-legitimation?
What is an e-ID token?

Anledningar till att inte använda e-legitimation- Reasons for not using an e-ID
Varför använder du inte en e-legitimation?
Why do you not use an e-ID?

Utföra saker utan e-legitimation - Manage things without e-ID
Hur gör man om man inte har någon e-legitimation?
How do you go about things without any e-ID?

Finns det saker du inte kan göra, blir utestängd från?
Are there things you cannot do, that you are excluded from?

Allmänt- General
Hur ser du på framtiden för e-legitimering?
How do you view the future in terms of identifying electronically?
Appendix C - Interview guide e-ID users (in Swedish and English)

Definition
Vad är en e-legitimation?
What is an e-ID token?

Anskaffning - acquisition
Vilken e-legitimation har du?
What e-ID token do you have?

Hur skaffade du din e-legitimation?
How did you acquire your e-ID?

Användning av e-legitimationen- Use of the e-ID
Vad uträttar du för ärenden med hjälp av e-legitimationen? /när använder du dig av den?
For what things do you use your e-ID? When do you use it?

Finns det mer saker du skulle vilja att e-legitimation kunde användas till?
Are there more things would you want the e-ID token to be used for?

Har du upplevt några problem med din e-legitimation, Om ja- vad?
Have you experienced any problems with your e-ID token, if yes-what?

Vad är fördelarna med att använda e-legitimation?
What advantages are there with using an e-ID?

Hur länge har du använt e-legitimation?
For how long have you been using an e-ID token?

Finns det tillfällen då du undvikt att använda ditt e-leg?
Have there been occasions when you have avoided using your e-ID token?

Hur ser du på framtiden för e-legitimationer?
How do you view the future in terms electronical identification?

Hur ser du på säkerhet och e-legitimering?
What is your view on identifying electronically in terms of security?

Hur ser du på relationen individ – bank – stat/myndigheter?
What do you think about the relation of individual-bank-public agencies

Hur gör de som inte har någon e-legitimation?
How are those without an e-ID token doing things?

Digitalisering - Digitalization
Ser du dig som en digital person?
Do you regard yourself as a digital person?

Hur ser du på digitaliseringen av svenska myndigheter? /
How do you regard the digitalization of public agencies in Sweden?
Appendix D - Interview guide Anders Henriksson (in Swedish and English)

Vad är en e-legitimation?
*What is an e-ID?*

Vilka är de största utmaningarna med e-legitimationer, i en svensk kontext primärt?
*Which are the main challenges with e-IDs, in a Swedish context primarily?*

Hur kommer vi att legitimera oss i framtiden?
*How are we identifying in the future?*

Vilka lagar förhåller ni er till när det kommer till e-legitimationer – och hur?
*Which laws are you affected by regarding e-IDs- and how?*