Challenges of introducing a professional eID card within health care

Karin Hedström

*School of Business, Örebro University, Örebro, Sweden and
Department of Management and Engineering,
Linköping University, Linköping, Sweden*

Fredrik Karlsson

Business School, Örebro University, Örebro, Sweden, and

Fredrik Söderström

*Department of Management and Engineering,
Information Systems Division, Linköping University, Linköping, Sweden*

Abstract

Purpose – The purpose of this paper is to examine the challenges that arise when introducing an electronic identification (eID) card for professional use in a health-care setting.

Design/methodology/approach – This is a case study of an eID implementation project in healthcare. Data were collected through interviews with key actors in a project team and with eID end users. The authors viewed the eID card as a boundary object intersecting social worlds. For this analysis, the authors combined this with an electronic government initiative challenge framework.

Findings – The findings of this paper illustrate the interpretative flexibility of eID cards and how eID cards as boundary objects intersect social worlds. The main challenges of implementing and using eID cards in healthcare are usability, user behaviour and privacy. However, the way in which these challenges are interpreted varies between different social worlds.

Practical implications – One of the implications for future practice is to increase our understanding of the eID card as a socio-technical artefact, where the social and technical is intertwined, at the same time as the eID card affects the social as well as the technical. By using a socio-technical perspective, it is possible to minimise the potential problems related to the implementation and use of eID.

Originality/value – Previous research has highlighted the need for more empirical research on identity management. The authors contextualise and analyse the implementation and use of eID cards within healthcare. By viewing the eID card as a boundary object, the authors have unveiled its interpretative flexibility and how it is translated across different social worlds.

Keywords Healthcare, E-Government, eID, Identity management, Boundary object

Paper type Research paper

1. Introduction

Over the past decade, the idea of transforming the health-care sector through the use of information technology (IT) has grown to the extent that it has resulted in significant

This research has been made possible by the funding from the Swedish Civil Contingency Agency.

investments being made (Angst and Agarwal, 2009). One example is the introduction of electronic identification (eID) cards within healthcare. They are seen as an efficient tool for the identification and authentication of individuals when accessing sensitive information such as patient data (Stroetmann *et al.*, 2011). In general terms, an eID card offers three forms of functionality: identification, authentication and signature (Fiat and Shadir, 1988). The reasons for a government or an organisation choosing to introduce an eID system might vary. For example, it might be important to have the ability to recognise citizens or certain individuals or groups before letting them have access to specific rights. These rights can be related to citizenship, goods or services that come with restrictions such as age limits (Whitley and Hosein, 2009). The availability of eID is also considered a necessary "building block" for the delivery of "robust, streamlined and sustainable" public e-services by European governments to their citizens (European Commission, 2010). Furthermore, identity management is a profound socio-technical activity that is difficult to engineer and plan in detail. Any changes related to identity management are seen as socio-technical in nature, with the social and the technical intertwined and embedded in the identity management solution (Woolgar and Neyland, 2013).

The implementation and use of electronic health-care records instead of paper-based records has "pushed health care into the lead for identity management application areas" (Halperin and Backhouse, 2008). At the same time, health-care organisations are required to handle large quantities of sensitive information, which gives rise to the question of how to protect this information from unwanted disclosure. Previous research has illustrated how value conflicts can arise when health information systems (HISs) are introduced; such conflicts can lead to tensions between information availability and confidentiality (Mommens, 1999). Balancing the demands of health-care professionals and their need for timely access to accurate patient information with the demands of those in charge of safeguarding confidentiality and integrity of that information can create a great deal of tension. Such tension can affect information use in healthcare (Hedström *et al.*, 2011, Gaunt, 2000) and lead to the creation of specific challenges when introducing eID. In addition, Halperin and Backhouse (2008) have argued that we need more context-specific research into eID to "gain a better understanding of the identity domain". With improved understanding of the specific challenges of eID in healthcare, we can consciously address these core issues when introducing such a system, thus improving the quality of the developed and implemented identity management systems. In addition, a socio-technical perspective is advocated by several researchers as a way of coping with the diversity of HISs (Berg, 1999, Callen *et al.*, 2012).

The aim of this paper is therefore to examine the specific types of challenges that arise when introducing and using an eID card for professional use in a health-care setting. For this purpose, we used the theoretical lens of Gil-García's and Pardo's (2005) framework for classifying the challenges that arise from electronic government initiatives. We combined this approach with the boundary object theory (Star and Griesemer, 1989). Thus, we viewed eID as a boundary object, allowing us to study how the socio-technical challenges of eID are translated across different social worlds (Star and Griesemer, 1989). In turn, this gave us a better understanding of the different interpretations of eID and, subsequently, the role of eID within healthcare. We have used a case study from healthcare in a Swedish county council to show that although it is

possible to identify a set of main challenges for an organisation, the degree of coherence across different social worlds can vary. This research advances existing research on the professional use of eID in healthcare (Campos *et al.*, 2011) and how to use a multi-actor perspective when studying the challenges associated with implementing electronic government initiatives.

The remainder of the paper proceeds as follows. The next section introduces a description of eID in healthcare, together with its background and context. Following this, we describe the theoretical lens used in this study. Section 4 gives an account of the research setting, including a case description, data collection and data analysis. The results – the challenges associated with introducing eID into healthcare – are described in Section 5. This is followed with a discussion in Section 6. Finally, we present a short conclusion.

2. eID in healthcare – background and context

The ability to identify individuals is a key component of the eHealth infrastructure, for example, health-care professionals, providers and pharmacies (Stroetmann *et al.*, 2011). The increased multi-disciplinary approach to modern healthcare has created an increased need for the sharing of patient data between different health-care actors (Goundrey-Smith, 2013), which in turn has strengthened the requirements for the identification of the different actors involved. While the patient identifier or ID has been given a clear focus in the development of eHealth among European countries, the professional identifier seems to have attracted less attention (Stroetmann *et al.*, 2011).

Halperin and Backhouse (2008) pointed out that the tensions associated with digital identity are related to problems or key issues with "security and privacy", "interoperability" and "convenience and intrusiveness". According to them, "security and privacy" is the most debated issue; it is also one that requires much to be done. In particular, the complex relationship between security and privacy "gives rise to strong feelings, interesting questions and social implications". For instance, important questions to consider are the risk of identity fraud and the difficulties that citizens may experience when managing and controlling their own data (Backhouse and Halperin, 2007; Whitley and Hosein, 2009; Price, 2008; De Hert, 2008). Another key issue put forward by Halperin and Backhouse (2008) is "interoperability", that is, how to use identity information between identity management systems. It is of course practical to be able to re-use data registered at one point in another location; at the same time, however, this raises specific ethical concerns about who should access what and about whom. Questions about responsibilities related to personal data also arise. The third and final key issue put forward by Halperin and Backhouse (2008) is that of "convenience and intrusiveness". They have pointed out that data collected for one purpose might be used for something entirely different. Thus, previous research emphasizes questions and concerns about privacy and the individual's ability to control his or her personal data when introducing eID systems within healthcare.

There are also some challenges that are specifically related to eID within healthcare. For instance, Campos *et al.* (2011) argued that issues concerning identity management within healthcare tend to centre on interoperability, where it is important to consider a "functional understanding of the activity of eHealth" and its responsibilities and roles. Previous research has argued that there are special concerns when national eID cards are used within healthcare as part of a HIS (Santos *et al.*, 2008). Based on a literature

review, they identified concerns related to health-care professionals' use of eID cards include issues such as usability, resistance to use, inefficiency and the risk of leaving the card at home.

3. Theoretical lens – challenges of eID

3.1 eID as a boundary object

We searched for a theoretical concept that allowed us to "facilitate the interpretation of the interactions within a relevant social group" (Bijker, 1995). Therefore, we chose to view an eID card as a "boundary object" (Star and Griesemer, 1989) that connects different groups of actors. Boundary objects are artefacts such as patients' medical records (Berg and Bowker, 1997), engineering drawings (Henderson, 1991) and requirements engineering specifications (Karlsson and Hedström, 2013). Boundary objects are used by social worlds (groups of actors with shared knowledge, interests and tasks) as a common point of reference in their conversations. In our case, although all the actors agree that they are talking about eID (Star and Griesemer, 1989), the different social worlds are not actually talking about the same sort of thing. In other words, they attach different meanings to eID. For example, for a nurse, an eID card that provides access to classified patient data might be used as a key to medical records. To the information security manager, however, it might represent a step in fulfilling legal requirements. Thus, although boundary objects "adapt to local needs" (Star, 1990) within a social world through translation, they still maintain their identity across these worlds. The different views of the eID card can be described as an effect of "interpretative flexibility", where the eID is viewed differently depending on the social group (Bijker, 1995). There is thus more than one interpretation of the eID.

As different social worlds attach different meanings to eID, the set of translations that exists can differ in coherence. Star and Griesemer (1989) argued that the "coherence of sets of translations depends on the extent to which entrepreneurial efforts from multiple worlds can coexist" and that an infinite number of translations is possible. In other words, coherence is the degree of consistency between translations offered by the analysed social worlds. Consequently, in practice, coherence is an important aspect of successfully implementing and managing a boundary object, such as eID, across intersecting social worlds. This diversity is a starting point for exploring alternative approaches to working with eID, providing that "there is sufficient commonality to support dialogue between the 'voices'" (Suthers *et al.*, 2013). In this paper, we focus on the translation of challenges that arise from eID for different social worlds in a health-care organisation. Of course, this set of translations is a subset of translations that relate to eID. We have chosen this subset because the degree of coherence is an important starting point for the future coordination and the alignment of successful eID implementation.

3.2 Challenges of electronic government initiatives

The European Commission described eID as "a government-issued document for online identification, and authentication" (European Commission, 2010). Indeed, it has been suggested that eID is a foundation for realising seamless, interoperable and secure electronic government (European Commission, 2010). Thus, eID can be seen as an important part of the realisation of electronic government (Melin *et al.*, 2013, Rössler, 2008). We have therefore chosen to use the electronic government initiative

framework put forward by Gil-García and Pardo (2005) to analyse the challenges of eID within different social worlds; we have used the framework by Gil-García and Pardo (2005), which organises electronic government challenges into five main categories. We adapted the original framework for our focus on eID in healthcare (see Section 4.3). The adapted framework is presented in Table I below. The table is made up of three columns: the leftmost column contains the more general categories, the second column shows the specific challenges associated with each general category and the rightmost column shows our operational definitions when focusing on eID.

The framework put forward by Gil-García and Pardo (2005) is a general framework that does not distinguish between different types of public sector organisations or social worlds. Hence, it puts forward the organisation as a homogenous entity with a consensus on the identified challenges that is irrespective of the type of organisation, organisational level or actor(s). This is, of course, an over-simplification of how challenges are interpreted within a specific type of organisation. Accordingly, it is important to add social worlds to the framework to contextualize the challenges. We have therefore created a matrix through which we illustrate how separate social worlds interpret the challenges that arise from the eID card within the organisation (Appendix 1).

4. Research setting, data and methods
4.1 Case description
This paper is based on a study that was performed at one of Sweden's 20 county councils. We followed a project that was aimed at the organisation-wide introduction of an eID card in a professional health-care setting. The project was initiated in 2012 and driven by an urgent need to comply with the Patient Data Act (PDA) and the National Board of Health and Welfare's (NBHW) regulations.

In Sweden, the PDA has been created to assure patient security, high quality and cost efficiency in healthcare (SFS, 2008:355). It stipulates that a medical record must be kept for each patient and clarifies how patient data should be handled to ensure the privacy of patients. Further, in their operationalisation of the PDA, the NBHW issued regulations for the use of strong authentication, which includes at least two factors, when accessing patient data (SOSFS, 2008:14). The national eID card solution that complies with these requirements is called Secure ID for healthcare (SITHS) and consists of a centrally managed technical infrastructure that is locally implemented by county councils and regions (CeHis, 2006, 2010). By 2012, all Swedish county councils, regions and municipalities were connected to this solution, and the number of cards issued numbered in excess of 300,000 (eHealth, 2012).

The project we followed is an example of an implementation of a professional eID card in healthcare and was organised with a project team of four people who acted on behalf of the steering committee. The aim was to introduce the eID card to each of the 14,000 potential users working within healthcare in the county council. The initial deadline was set for February, 2013, although this was later postponed. Hence, this project offered us a unique opportunity to study the introduction of eID in real time.

The chosen eID solution is a smart card solution that is based on a nationally governed technical infrastructure (SITHS). It has several functions, including acting as a physical ID card. It also has a magnetic stripe and RFID functionality. In addition to IT-related access, several functions and uses have been added to the card, such as access

Challenges	Operational definition
Information and data	
Information and data quality	Challenges related to "inaccuracies, inconsistencies and incompleteness of data" (Gil-García and Pardo, 2005) resulting from the use of eID
Dynamic information needs	Challenges related to not being able to satisfy changing needs of information resulting from the use of eID
Information technology	
Usability	Challenges related to the ease of use of eID
Security issues	Challenges related to security breaches when using eID
Technological incompatibility and complexity[a]	Challenges related to technologies in the eID implementation being incompatible and/or being complex which makes it difficult to understand the effects of changes made
Technical skills and experience	Challenges related to the eID implementation team's lack of necessary technical know-how and skills and/or being short of staff with the necessary technical know-how and skills
Technological newness	Challenges related to the newness of the eID technology, which constrains its implementation and use
Organisation and management	
Project size	Challenges related to the size of the eID implementation project
Managers' attitudes and behaviour	Challenges related to managers' support for the eID implementation project and the use of eID
User or organisational diversity	Challenges related to variations within the user groups and/or organisations involved in the use of eID
Lack of alignment of organisational goals and project	Challenges related to the differences between the organisational goals and the goals of the eID implementation project
Multiple or conflicting goals	Challenges related to "the existence of multiple, and sometimes conflicting, goals in the public sector" (Gil-García and Pardo, 2005) and the impact these goals have on the implementation and use of eID
Resistance to change	Challenges related to individual interests that lead to resistance to the changes proposed from implementing eID
Turf and conflicts	Challenges related to individual interests that lead to turf issues during the implementation and/or use of eID
Users' attitudes and behaviours[a]	Challenges related to individual interests that affect how eID is used
Administrative routines[b]	Challenges related to administrative routines not aligned with the use of eID
Legal and regulatory	
Restrictive laws and regulations	Challenges related to the organisation operating by "a specific rule or group of rules" (Gil-García and Pardo, 2005), rules that affect the implementation and use of eID
One-year budgets	Challenges related to how one-year budget cycles affect the long-term results of eID

(*continued*)

Challenges	Operational definition
Intergovernmental relationships	Challenges related to relationships between different levels of governments and how these relationships affect the implementation and use of eID
Institutional and environmental	
Privacy concerns	Challenges related to how privacy issues affect the implementation and use of eID
Autonomy of agencies	Challenges related to the government agency not taking into account what other public organisations are doing with regard to eID
Policy and political pressures	Challenges related to how policy agendas and politics affect the implementation and use of eID
Environmental context	Challenges related to the external context, not listed above, that affect the implementation and use of eID (e.g. users' experiences from previous implementations)

Notes: [a] In the original framework, technological incompatibility and complexity are two separate challenges; however, our empirical data show that these two challenges are highly interlinked; therefore, we decided to treat them as one challenge; [b] we have found it necessary to add these challenges to the framework based on our empirical findings
Source: Adapted from Gil-García's and Pardo (2005)

Table I.

to doors, secure printing and pneumatic tube systems. Further, the technical setup of the eID card also features a private eID as the primary certificate, which offers the possibility of using the card to access both public and private secure e-services.

4.2 Data collection
This is a qualitative case study (Yin, 1994) and, as such, is an established research method for information systems research (Benbasat *et al.*, 1987, Walsham, 1995, Lee, 1989). We have chosen a case study approach as our research method because it offers the possibility of developing generalisations based on specific empirical observations (Lee and Baskerville, 2003, Eisenhardt, 1989, Eisenhardt and Graebner, 2007). In addition, the case study method offered the possibility of studying our phenomenon in a natural setting, a necessity bearing in mind our desire to reveal the use of eID in daily practice.

The empirical material is mainly based on interviews that were carried out with 12 representatives of different social worlds in the organisation. They included nurses, nurse aids, IT support staff, health-care managers, one information security manager, IT consultant, IT department staff and a medical secretary (Table II). The interviews were carried out during the course of one year, from autumn 2012 until autumn 2013. We also reviewed strategic documents such as project plans and carried out one observation of the use of eID. The role of the interviews was to generate rich data on the implementation and use of eID within the organisation (Schultze and Avital, 2011). We interviewed high-level managers and project leaders in charge of the eID implementation project to get a better understanding of the drivers of the project, the staff who use eID within their health profession and the IT-support personnel. The latter have a great deal of experience of the problems that might arise when using eID cards.

The interviews were semi-structured and the answers were followed up with demands for examples and clarifications. Typically, we asked for concrete examples, motives and explanations in relation to the implementation and use of the eID card to generate data that are as rich as possible (see the interview guide in Appendix 2 for more details). We also came back to interview two of the respondents once again, as one of the authors was unable to participate in the original interviews of these two persons, and we wanted to add some specific questions concerning the use of the eID card and risk behaviour. The interviews, which typically lasted for one hour, were tape-recorded and transcribed. The respondents were initially selected according to their ability to discuss issues about the implementation and use of eID within the county council, which represents different social worlds. We complemented our initial interviews with a snowball or referral sampling strategy (Biernacki and Waldorf, 1981) to make sure that we would not miss important and interesting roles. To capture the diversity of issues related to the implementation and use of eID within the county council, we chose one hospital ward and one health centre under its authority for data collection to capture users' experience of the implementation project and the use of eID for health-care work. The two health-care settings differed most significantly in terms of the type of healthcare provided, that is, general versus specialist practice, and their requirements for operational flexibility, that is, a fixed versus flexible workplace.

Complementary to the interviews, we also observed how the medical secretaries used the eID cards in practice when they carried out their work at reception or in their office. The observation followed the interviews, which gave us an opportunity to clarify and follow-up any issues that arose during the interviews, as well as provide us with a better insight into the practical use of eID cards. The role of the strategic documents was to gather background data and get a better understanding of the eID project as well as the case study setting.

4.3 Data analysis
The empirical data were analysed using the theoretical lens presented in Section 3. Our approach used a combination of boundary object theory (Star and Griesemer, 1989) and the electronic government initiative challenge framework put forward by Gil-García and Pardo (2005). From the boundary object theory, we chose to focus on the concepts of "social worlds" and "coherence" (Star and Griesemer 1989). The empirical data consisted of transcripts from interviews. The analysis was carried out using four steps (Table III, present a subset of our detailed analysis, which illustrates the way in which we categorized the quotes). First, we read the transcripts to elicit quotes that describe the challenges associated with the use of eID. Second, we organised the elicited quotes

Social world	Respondents	No. of interviews
IT support staff	3	3
Nurses and nurse aids	2	2
IT department staff	2	4
IT consultant (external)	1	1
Information security manager	1	1
Medical secretaries	1	1
Health-care managers	2	2

Table II. Data collection

Social world	Privacy concerns	Institutional and environmental Challenge		
		Inter-organisational relationships	Policy and political pressures	Environmental context
IT department	"We do not want people to lend their cards to other people"	"We do not know if the suppliers take us seriously. There are so many dependences. It gets unsecure and vulnerable. One feels powerless"	"Many problems are caused by the national services. Which are unable to influence"	None
IT support	"People do not lock the doors, and leave the cards in the computer when they leave for a break"	"We have lots of students. And they get their cards from their schools. It works with the students from the University, but the students who are going to become nurse aids do not get any cards from their schools. And that is a problem"	None	"Especially the physicians – about the eID card [. . .]. This is a bad system, and Cosmic (the medical record system) is a bad system. Many are unhappy with Cosmic, and they now blame the eID card system if things don't work"

Table III.
Illustration of the use of analytical framework

according to the challenges (i.e. translations) found in the electronic government initiative challenge framework and the social world to which the quote belonged. Third, we analysed those challenges that could be categorized as general, that is, those that were found across all social worlds. Fourth, these general challenges were further analysed to identify the degree of coherence across the social worlds. We identified three categories:

(1)   in support of coherence;
(2)   in partial support of coherence; and
(3)   lacking coherence.

If a specific challenge was found in several social worlds (e.g. having trouble accessing the systems when using eID), then this was categorised as being in support of coherence. The complete analysis can be found in Appendix 1.

During our iterative analysis, we also adapted the analytical framework based on the transcripts from the eID case. Although we started with the set of challenges identified by Gil-García and Pardo (2005), we continuously compared them against fresh data. This process made us go back further to elaborate on the abstracted challenges until the categories were stabilized and saturated (Urquhart and Fernández, 2013; Glaser, 1978).

Compared with the challenges put forward by Gil-García and Pardo (2005), our eID case is different in the way it focuses on the organisational and managerial aspects of electronic government. In particular, it revealed the need for greater emphasis on the user as well as on administrative routines. Thus, we decided to add two sub-categories to the organisation and management category: "users' attitudes and behaviour" and "administrative routines". We also found it difficult to separate technical complexity

from technical incompatibility, because these two challenges are closely interlinked in the case study material. Thus, we decided to treat them as one challenge. The complete list of challenges is shown in Table I (Section 3).

5. Challenges of eID cards within healthcare
Our analysis resulted in 16 challenges (Appendix 1) out of the complete list of 23. These are listed in the framework presented in Table I. Space limitations make it impossible to provide a detailed description of the complete analysis. Accordingly, we here present our analysis of the three challenges that have the most analytical power, that is, those challenges that frequently occurred across most social worlds. The identified common challenges are usability, users' attitudes and behaviours and privacy concerns. A summary of the complete analysis can be found in Appendix 1. The table illustrates the challenges that were discussed from the perspective of the different social worlds.

5.1 Usability
5.1.1 In support of coherence. The usability aspect revealed a high degree of coherence across all social worlds. Two types of problems were unanimously stated: difficulties in understanding how to log in and use the eID card and problems with delayed response time. In the empirical material, we see how important usability is for the successful use of eID.

From the accounts available to us in this case study, it is very clear that the users had problems using the eID to access information. In particular, they experienced technical problems that relate to the use of the eID card, problems logging in and difficulties in understanding how to handle the card. The workload of the IT-support team was higher than expected; indeed, they needed to hire an additional person on top of the extra staff already brought in to deal with the introduction of eID cards. The method of logging in to the systems is not intuitive; many users inserted their card at the wrong time when they logged in. A member of the IT-support team told us the following story:

> First, you must log in with your HSA-id (health services address directory id) and password, and then you have to wait a while until all the icons appear. And now you insert the card, which has been a huge problem for employees to learn. A lot of people insert the card at once, which doesn't work. This makes the computer start spinning, it doesn't understand a thing. Then you need to re-start and repeat what you just done. It takes some time, to learn how to do this. This has been the biggest problem.

One solution has been for some hospital clinics to start using a Single-Sign-On (SSO) solution, which has been developed to simplify the login process and, hence, act as a lever for increased adherence to the intended use of the eID. The SSO solution is expected to minimise the existing user behaviour of leaving the card in the reader, because it reduces the recovery time of the user session. However, this solution is not without problems for a unit such as the clinic, which requires a great deal of flexibility. Here, users might frequently change between professional roles and, hence, need to be able to quickly change between different user sessions associated with the same user. This is an example of how demand for a secure log-in conflicts with the need for an easy-to-use IT system.

The eID project has been a very large undertaking involving many users. Furthermore, it has been implemented at a high speed. This has resulted in major problems with regard to the speed and technical performance when accessing data.

Users have been spending too much time waiting for a connection. In this case, such usability problem has disrupted work. Users have also found it very irritating and time consuming when struggling to access the systems:

> And when you insert the card, the icon starts, and it scrolls and scrolls, and nothing happens. And you cannot get in, you have to take out the card and rub it on your trousers. And see if something happens. It does not take very long time, but it's still an annoyance that it does not work the first time (health care manager).

This is a heterogeneous work place, with differences in work tasks, differences in workplace setting (i.e. whether fixed or flexible) and differences in the sort of information that needs to be accessed. A variety of hardware and software is used, which also needs to be taken into account. Furthermore, there is a difference in requirements between workplace settings; for example, in operating theatres, hygiene requirements are more stringent. Such diversity can be highly demanding. As one IT consultant told us: "This is the difficulty with this technique, getting it perfect in all situations".

5.2 Users' attitudes and behaviours
The second challenge to the introduction of eID cards relates to the interpretation of challenges that arise when the eID card is used. This finding supports coherence across all social worlds and the interpretation of a limited number of social worlds, that is, partial support of coherence. One challenge, which is related to users' creation of work-around, lacks coherence across social worlds.

5.2.1 In support of coherence. Another key to successful implementation and use of eID is an awareness of working with users' attitudes and behaviours and an ability to do so. Even if the system works, the way that users operate within that system, and the dedicated routines that revolve around it, is important for maximising its potential. Many of the issues that surround user behaviour relate to the way in which users handle the eID card from the perspective of safeguarding patient data. It is clear from the interviews that at least some of the problems relating to user attitude and behaviour are a direct consequence of usability issues, such as problems logging in and out or delayed response time.

Our respondents describe how they forget or willingly leave their eID cards in the computers when they go for short breaks. According to one nurse:

> There are many who do not take out the card when they leave their computer. I know it is not. If, for instance, someone goes for a coffee break, the card is taken out, but these short errands, to go and get the papers in the printer, you only lock the computer and get the papers, and come back and continue. This I know, this is how it is […]. And in the end you do not think that this isn't how it should be. It becomes a norm.

The medical secretaries also described how their work involves getting up and fetching things all the time. This way of working makes them see the eID card as something that gets in the way of work. For example, one medical secretary stated:

> So I run up the whole time. Up and down and to the printer […] I have to take my damn card as soon as I shall be in another room or the next room. I always have to take the card. Even if I just jump up and down from the chair and then in and just to fetch something or so.

She also confessed that she "sometimes has left the card in the computer. It makes me feel a bit weary". The hospital staff finds it very cumbersome to log in and out all the time, which is why they sometimes leave the eID cards in the computer. As one member of the IT support team stated:

When you take out the card, then you need to log in again. First you need to get into the computer, then you need to enter the card, and you must log into the records again. You do not get anything automatically.

It is clear that many of the users lack a deep understanding about the reasons for implementing the eID card. The IT department even told us that: "We do not add any functionality – we only make this more difficult". When the eID cards were first introduced, there was some discussion about the reasons behind this solution. It is necessary for this dialogue to continue; otherwise, there is a risk of more problems relating to the use of the eID card.

It is also interesting to note how the physical environment has created a sense of security. From our observations, we can see how most of the medical secretaries work behind desks in the reception area. This makes them feel very secure. Consequently, they do not feel the same urgency to withdraw their eID cards from the computers. For example, one IT team member stated:

You have to take out the card every time you are away from your computer. When you leave the computer, you should always lock it. Most computers are in a room behind the reception, but it is almost never empty and there is the reception. So it is still quite protected. But not everybody locks. It is a pain to pull the card out and log back on.

5.2.2 In partial support of coherence. Several of the respondents expressed concerns about the risk of leaving their eID cards at home when they came to work. One IT support team member stated: "You need to keep the card on you" and "People forget their cards". To "teach" the staff to remember to bring their eID cards, it was seen as necessary to "go back home and get the card. Otherwise you never learn".

Another concern relates to the problem of unlocked doors. As one IT-support person said: "We don't pull the card, we don't lock the doors. Many leave their doors open, and the card in the computer". This behaviour illustrates a security breach with regard to privacy.

5.2.3 Lacking coherence. This challenge is related to users who construct work-arounds. This issue was only raised by the information security manager, which means that this interpretation lacks coherence across social worlds. The introduction of new technological solutions, such as the eID card, inevitably highlights routines and communication patterns. The information security manager reflected on the consequences of the implementation process and how, instead of using the eID card as intended, users have created unwanted solutions. Thus, the information security manager stated:

We have begun to discover that there have been some work-arounds that do not really work with the card. They have for instance created group log-ins. Things very much get into the open. One should perhaps change the work routines beforehand, but you do not do it because it's always tough. But with the card you must. You are forced to do it.

This way of acting can be seen as disclosed resistance to change.

5.3 Privacy concerns
The third and final challenge is related to the privacy concerns that arise from the use of eID cards. This was challenge was found in all social worlds. This is not surprising, because the reason for introducing this technical solution in a health-care setting was to safeguard the confidentiality of sensitive patient data. Respondents stated that they see safeguarding patient data as the main reason for implementing the eID card within the organisation. According to one medical secretary: "Well, the value of this card? That no one can get in, when I have pulled out the card".

5.3.1 In support of coherence. According to our findings, many of the problems relating to user compliance (see the section on users' behaviours and attitudes) are related to fears of privacy breaches. A member of IT support stated:

> This should be safe for the patient, if taken care of properly. The goal is patient safety. But it always takes a long time for people to learn, and we do not talk much about it. This is always how it is when you introduce something new. It is tedious to learn. People work 200 per cent, and everything is stressful, and they do not want to learn new things. But some people think it's good, of course. But not everybody. We are not doing this the right way, from the perspective of patient safety. We do not withdraw the card; we do not lock the doors. Many leave the doors open and the card in the computer. Anyone can of course get in. But this is anyway more secure than before.

The users are concerned about leaving the cards in the computers, because they are aware that this might risk the disclosure of sensitive patient data. However, we did not hear any reports about incidents where patient data actually had been disclosed. Several respondents did, however, describe reoccurring incidents where patient data were at risk of being exposed; for instance, when staffs leave the card in the computer or take out the card, but leave it on the desk beside the computer.

6. Discussion
The use of eID gives rise to issues that are both highly political and socio-technical in nature. Here, the social and the technical are intertwined and embedded in identity management systems. Problems arise when this socio-technicality is ignored, as illustrated by the tension that builds up between security and usability. The implemented eID solution is based on highly standardised parts that are linked together in a rather complex process, affecting usability and user behaviours. The eID solution is non-flexible, even though the studied organisation is heterogeneous, both in terms of technology, user groups, work situations and user movability. This case describes the implementation of an eID card with a strong technical focus, where organisational and user issues are given less attention. They have, in other words, treated the social and the technical as different aspects of the eID, rather than as integrated parts. Based on these findings, some notable lessons can be learned with regard to practice and research.

6.1 Contribution to practice
Resistance to change is not surprisingly related to user behaviours and attitudes. We have found that experiences from previous implementation projects have a strong effect on how users perceive the introduction of new IT systems. Many at the studied organisation felt that they had been affected by an earlier implementation of an electronic medical records system, making them view this new technology with a great deal of scepticism. This case also showed us that the physicians formed a group of users

who, in some stages of the implementation, showed a high level of aversion towards the eID based on its possible negative impact of their work. For some users, the previous attempt to implement electronic medical records was fresh in their memories. They used the problems that arose when introducing this new technology as a way of fuelling their dislike of IT implementations in general. We therefore believe that when introducing new technology, it is important that previous experiences of similar implementations are taken into consideration. Existing research has shown that the benefits of using eID cards must be tangible to the users if they are to adopt this new technology. The relative advantage for the professionals involved must also be clear (Aubert and Hamel, 2001). In this case, we found that the IT department struggled to create added functionality to increase use, for example, by enabling private use of the eID card. Furthermore, from a professional's point of view, the relative advantage was questionable; for them, it was just one more thing to keep track of.

In our case, we found that although the health staff were fully aware of the eID card's function to govern and protect the privacy of the patients' records, in the interviews, they focused more on the poor usability of the eID card system and ways in which it obstructed their daily work. This illustrates how important it is to work with and take into consideration the social as well as the technical organisational aspects when introducing eID within healthcare. Users need to be aware of the rationality behind the technical solution. At the same time, the people working with the implementation project need to adapt the technical solution to the specifics of the organisation.

It is also evident from our case that a technology such as an eID card has far-reaching socio-technical consequences. Just as the eID card embeds social as well as technological features, it effects the organisation in a similar way. We believe that a successful implementation of eID needs to take this socio-technicality seriously; otherwise, only a part of the problems or possibilities is taken into account.

6.2 Contribution to research
Our results corroborate and add to the findings in the literature review carried out by Santos *et al*. (2008). As noted in Section 2, Santos *et al*. (2008) found that health-care professionals' use of eID cards raises such challenges as usability, resistance to use, inefficiency and the risk of leaving the card at home. As illustrated in this paper, we found the very same issues in our empirical material. Based on our case study material, we were able to reveal in more detail the nature of the different challenges and how they vary across social worlds.

This research contributes by using an elaboration of the challenge framework put forward by Gil-García and Pardo (2005) as our theoretical lens. The original framework treats an organisation as having a homogenous view on challenges. Our analysis uses concepts from the boundary object theory (Star and Griesemer, 1989) to show that this is not the case and that, with regard to challenges, different degrees of coherence exist between social worlds. This means that actors interpret the challenges of eID differently, depending on the social world to which they belong. The use of degree of coherence has allowed each challenge to be seen in greater detail, thus making it possible to identify the different interpretations of each specific challenge. Consequently, the concepts of social world, translation and degree of coherence are important contributions to the challenge framework for electronic government initiatives. They would be particularly useful not

just in the introduction of eID but also when analysing other types of initiatives in the electronic government context.

7. Conclusions

The purpose of this paper was to analyse the specific types of challenges that arise when using and introducing an eID card for professional use in a health-care setting. We wanted to give guidance to those who wish to gain a better understanding of implementation and the use of eID within healthcare. The specifics of eID mean that it is important to view it as a socio-technical artefact with unique attributes, where the social and technical are highly intertwined and embedded. This also means that any implementation and use of an eID has socio-technical effects. Previous research has called for more empirical research on identity management. This paper responds to this call by contextualising and analysing the implementation and use of eID within healthcare as a boundary object (Star and Griesemer, 1989) using a socio-technical perspective.

Our research thus offers some insight in how to view artefacts such as eID as boundary objects. Indeed, our analysis of the social groups' different interpretations of the challenges can be used as a starting point to align and co-ordinate implementation and the use of eID. These different interpretations also illustrate the interpretative flexibility of the eID card. The framework put forward by Gil-García and Pardo (2005) has guided us towards an analytical framework that allows us to better understand the challenges of eID in health-care practice. Our results illustrate how usability, users' attitudes and behaviours and privacy concerns are challenges that occur across all social worlds. However, as our analysis of degree of coherence shows, the interpretation of these challenges varies between these social worlds. However, the framework put forward by Gil-García and Pardo (2005) does not differentiate between actors in an organisation and view the organisation as a homogenous world where there exists consensus on the identified challenges. This is of course an over-simplification. We believe that there is a need for a more nuanced and rich description of the challenges of electronic government initiatives. Therefore, we introduced the concepts of social worlds and degree of coherence to provide a more detailed and multi-faceted analysis of the challenges of eID.

References

Angst, C.M. and Agarwal, R. (2009), "Adoption of electronic health records in the presence of privacy concerns: the elaboration likelihood model and individual persuasion", *MIS Quarterly*, Vol. 33 No. 2, pp. 339-370.

Aubert, B.A. and Hamel, G. (2001), "Adoption of smart cards in the medical sector: the Canadian experience", *Social Science and Medicine*, Vol. 53 No. 7, pp. 879-894.

Backhouse, J. and Halperin, R. (2007), "A survey on EU citizen's trust in ID systems and authorities", London School of Economics and Political Science, London.

Benbasat, I., Goldstein, D.K. and Mead, M. (1987), "The case research strategy in studies of information systems", *MIS Quarterly*, September.

Berg, M. (1999), "Patient care information systems and health care work: a socio technical approach", *International Journal of Medical Informatics*, Vol. 55 No. 2, pp. 87-101.

Berg, M. and Bowker, G. (1997), "The multiple bodies of the medical record: towards a sociology of an artefact", *The Sociological Quarterly*, Vol. 38 No. 3, pp. 513-527.

Biernacki, P. and Waldorf, D. (1981), "Snowball sampling problems and techniques of chain referral sampling", *Sociological Methods Research*, Vol. 10 No. 2, pp. 141-163.

Bijker, W. (1995), *Of Bicycles, Bakelites, and Bulbs, Cambridge*, The MIT Press, MA.

Callen, J., Georgiou, A., Li, J. and Westbrook, J. (2012), "The value of sociotechnical theories for implementation of clinical information systems", in Vaidya, K. (Ed.), *Inter-Organizational Information Systems and Business Management: Theories for Researchers*, IGI Global, Hershey, PA.

Campos, M.J., Correia, M.E. and Antunes, L. (2011), "Leveraging identity management interoperability in eHealth", *IEEE International Carnahan Conference On Security Technology (ICCST 2011)*, IEEE, Barcelona.

CeHis (2006), "Nationell IT-strategi för vård och omsorg", available at: www.cehis.se/images/uploads/dokumentarkiv/Nationell_ITstrategi_fr_vard_och_omsorg_100520.pdf

CeHis (2010), "Nationell eHälsa – strategin för tillgänglig och säker information inom vård och omsorg", available at: www.cehis.se/images/uploads/dokumentarkiv/Lagesrapport_Strategi_2010_Rapport_100629.pdf

De Hert, P. (2008), "Identity management of e-ID, privacy and security in Europe. A human rights view", *Information Security Technical Report*, Vol. 13 No. 2, pp. 71-75.

eHealth (2012), "Nationell eHälsa – landstings, regioners och kommuners handlingsplan för eHälsa 2013-2018", available at: www.nationellehalsa.se/Content/Cms/img/temp/Utmaningaroch m%C3%B6jligheter med de eH%C3%A4lsosattsningar som g%C3%B6rs inom landsting och regioner,%C3%85ke Rosandher.pdf

Eisenhardt, K. (1989), "Building theories from case study research", *Academy of Management Review*, Vol. 14 No. 4, pp. 532-550.

Eisenhardt, K.M. and Graebner, M.E. (2007), "Theory building from cases: opportunities and challenges", *The Academy of Management Journal*, Vol. 50 No. 1, pp. 25-32.

European Commission (2010), "Digitizing public services in Europe: putting ambition into action", *9th Benchmark Measurement*, Directorate General for Information Society and Media, Unit C.4 Economic and Statistical Analysis, Bruxelles.

Fiat, A. and Shadir, A. (1988), "How to prove yourself: practical solutions to identification and signature problems", in Odlyzko, A.M. (Ed.) *Advances in Cryptology – CRYPTO '86*, Springer-Verlag, Berlin Heidelberg.

Gaunt, N. (2000), "Practical approaches to creating a security culture", *International Journal of Medical Informatics*, Vol. 60 No. 2, pp. 151-157.

Gil-García, R. and Pardo, T.A. (2005), "E-government success factors: mapping practical tools to theoretical foundations", *Government Information Quarterly*, Vol. 22 No. 2, pp. 187-216.

Glaser, B.G. (1978), *Theoretical Sensitivity*, The Sociology Press, Mill Vaelly, CA.

Goundrey-Smith, S. (2013), *Information Technology in Pharmacy – An Integrated Approach*, Springer-Verlag, London.

Halperin, R. and Backhouse, J. (2008), "A roadmap for research on identity in the information society", *Identity of the Information Society Journal*, Vol. 1 No. 1, pp. 1-16.

Hedström, K., Kolkowska, E. and Karlsson, F. (2011), "Value conflicts for information security management", *International journal of Strategic Information Systems*, Vol. 20 No. 4, pp. 373-384.

Henderson, K. (1991), "Flexible sketches and inflexible data bases: visual communication, conscription devices, and boundary objects in design engineering", *Science Technology Human Values*, Vol. 16 No. 4, pp. 448-473.

Karlsson, F. and Hedström, K. (2013), "Evaluating end user development as a requirements engineering technique for communicating across social worlds during systems development", *Scandinavian Journal of Information Systems*, Vol. 25 No. 2, pp. 1-26.

Lee, A.S. (1989), "A scientific methodology for MIS case studies", *MIS Quarterly*, Vol. 13 No. 1, pp. 33-50.

Lee, A.S. and Baskerville, R.L. (2003), "Generalizing generalizability in information systems research", *Information Systems Research*, Vol. 14 No. 3, pp. 221-243.

Melin, U., Axelsson, K. and Söderström, F. (2013), "Managing the development of secure identification – investigating a national e-ID initative with a public service context", *European Conference on Information Systems Utrecht*, *The Netherlands*.

Mommens, P. (1999), "Ethical issues of health care in the information society", *Health Informatics Journal*, Vol. 5 No. 4, pp. 223-239.

Price, G. (2008), "The benefits and drawbacks of using electronic identities", *Information Security Technical Report*, Vol. 13 No. 2, pp. 95-103.

Rössler, T. (2008), "Giving an interoperable e-ID solution: using foreign e-IDs in Austrian e-Government", *Computer Law & Security Report*, Vol. 24 No. 5, pp. 447-453.

Santos, R., Correia, M.E. and Antunes, L. (2008), "Securing a health information system with a government issued digital identification card", *ICCST 2008 42nd Annual IEEE International Carnahan Conference Security Technology*.

Schultze, U. and Avital, M. (2011), "Designing interviews to generate rich data for information systems research", *Information and Organization*, Vol. 21, pp. 1-16.

SFS 2008:355, "Patientdatalag [Patient Data Act]", Socialdepartementet, Stockholm.

SOSFS 2008:14 (2008), "Socialstyrelsens föreskrifter om informationshantering och journalföring i hälso- och sjukvården [National board of health regulations on information management and record keeping in health care]", Socialstyrelsen, Stockholm.

Star, S.L. (1990), "The structure of ill-structured solutions: boundary objects and heterogeneous distributed problem solving", in Gasser, L. and Huhns, M.N. (Eds), *Distributed Artificial Intelligence*, Morgan Kaufmann, San Mateo, CA.

Star, S.L. and Griesemer, J.R. (1989), "Institutional ecology, 'tranlsations' and boundary objects: amateurs and professionals in Berkeley's museum of vertebrate zoology, 1907-39", *Social Studies of Science*, Vol. 19 No. 3, pp. 387-420.

Stroetmann, K.A., Artmann, J., Stroetmann, V.N. and Whitehousee, D. (2011), "European countries on their journey towards national eHealth infrastructures", European Commission DG Information Society and Media ICT for Health Unit.

Suthers, D.D., Lund, K., Rosé, C.P. and Teplovs, C. (2013), "Achieving productive multivocality in the analysis of group interactions", in Suthers, D.D., Lund, K., Rosé, C.P., Teplovs, C. and Law, N. (Eds), *Productive Multivocality in the Analysis of Group Interactions*, Springer, New York, NY.

Urquhart, C. and Fernández, W. (2013), "Using grounded theory method in information systems: the researcher as blank slate and other myths", *Journal of Information Technology*, Vol. 28 No. 3, pp. 224-236.

Walsham, G. (1995), "Interpreative case studies in IS research: nature and method", *European Journal of Information Systems*, Vol. 4 No. 1, pp. 4-81.

Whitley, E.A. and Hosein, I. (2009), "Global challenges for identity policies", *Identity in the Information Society*, Vol. 2 No. 3, pp. 359-361.

Woolgar, S. and Neyland, D. (2013), *Mundane Governance. Ontology & Accountability*, Oxford University Press, Oxford.

Yin, R.K. (1994), *Case Study Research: Design and Methods*, SAGE, Thousand Oaks, CA.

Further reading

Pinch, T. and Bijker, W. (1987), "The social construction of facts and artefacts: or how the sociology of science and the sociology of technology might benefit each other", *Social Studies of Science*, Vol. 14 No. 3, pp. 3990-4441.

Söderström, F. and Melin, U. (2012), "The emergence of a national eID solution – an actor-network perspective", *The 35th Information Systems Research Seminar in Scandinavia (IRIS) Sigtuna*.

Star, S.L. (2010), "This is not a boundary object: reflections on the origin of a concept", *Science, Technology & Human Values*, Vol. 35 No. 5, pp. 601-617.

Appendix 1

Challenge	IT support staff	Nurses and nurse aids	IT department staff	IT consultant	Information secondary manager	Medical secretaries	Health-care managers
Information and data							
Information and data quality							
Information needs	X	X	X	X	X		X
IT							
Security issues			X	X			
Usability	X	X	X	X	X	X	X
Technological incompatibility and complexity		X	X	X	X		
Technical skills and experience							
Technological newness							
Organisational and managerial							
Project size			X	X	X		
Managers' attitudes and behaviours	X		X		X		X
User or organisational diversity	X	X			X		X
Lack of alignment of organisational goals and project							
Multiple or conflicting goals	X			X	X		
Resistance to change	X	X	X		X	X	X
Turf and conflicts					X		X
Users' attitudes and behaviours	X	X	X	X	X	X	X
Administrative routines	X		X		X		X
Legal and regulatory							
Restrictive laws and regulations		X		X			
One-year budgets							
Inter-governmental relationships							
Institutional and environmental							
Privacy concerns	X	X	X	X	X	X	X
Inter-organisational relationships			X	X			X
Policy and political pressures			X	X			
Environmental context							

Table A1.
Analysis of challenges of eID within healthcare

Appendix 2

No.	Question
1.	Can you please tell us about your organisation and your role? What is your role in relation to the eID card? What is your role regarding information security?
2.	What is your view on the eID card? How would you describe it?
3.	For what is it used?
4.	In which contexts?
5.	Who is using the eID card?
6.	For what are they using it?
7.	Are there any differences in usages?
8.	In what ways are patients affected by the use of the eID card?
9.	In what way are you engaged in working with the eID card within the county council? What are your experiences from implementing the eID card? Positive and negative
10.	Which actors (people, organisations, companies) have participated in this process and what is your relation to these? Have the results of the participation met your expectations and intentions?
11.	How have communication, understanding and collaboration between different parties worked? Can you give us good and bad examples?
12.	Which plans, strategies, decisions and rules (internal/external) are important for the development and implementation of eID cards, and what are the possibilities/challenges with these?
13.	How are users' usages of eID cards regulated? Examples of policies, guidelines, rules
14.	How is the use of eID card regulated in your information security policy? What are the bases for the policy? Standards? Laws? Can you give us an example?
15.	What are the risks of using the eID card?
16.	What are the risks according the staff? Is there any discrepancy between different categories? What are the risks from a patient perspective?
17.	Have you heard about and security breaches that have occurred due to the use of eID card?
18.	Are the users following, according to you, policies and regulations about the use of eID card? If they do, why? If the do not, why?
19.	What are your expectations and intentions of the eID card? Have these be met? Are there any aspects that have failed to be realised? If so, can you describe why?
20.	What is the future development of the eID card? What possibilities and challenges can you see and how are these valued?
21.	How has the spread and use of eID card been in the past, and how is it today?
22.	What differences in need and use of eID cards are there between different parts of your organisation and how is this dealt with?
23.	Are there any other key aspects, for instance, regulatory, organisational or security issues that make implementation and use of the eID card easy or difficult?
24.	How is the work on the eID card carried out on a regional and national level? Are you a member of any national or regional networks regarding eID, and if so, what actors are you working with?
25.	How are your eID solution and the future national solution for electronic identification and signature related? What are your thoughts about this, and how can it affect your organisation?
26.	Is there anything else we should have asked about? Do you want to add anything?

Table AII.
Interview guide
(information security
manager, IT
department staff, IT
consultant, health-
care managers)

No.	Questions
1.	Can you please tell us about your organisation and your role? What is it that you work with?
	What is your role in relation to the eID card?
	What is your role regarding information security?
2.	What is your view on the eID card? How would you describe it?
3.	How do others view the eID card?
4.	For what is it used?
5.	When is it used?
6.	Where is it used?
7.	For how long have you used the eID card?
8.	Why has it been implemented? What is the goal? Why?
9.	In which contexts?
10.	Who is using the eID card?
11.	Are there any differences in usages?
12.	In what ways are patients affected by the use of the eID card?
13.	Are there any risks related to using the eID card?
14.	What are the problems related to the usage?
15.	What are the advantages of using the eID card?
16.	What are your experiences from the implementation process?
17.	Is there anything one could learn?
18.	Have you experienced any security breaches when using the eID card?
19.	What would an ideal solution look like?
20.	Is there anything else we should have asked about? Do you want to add anything?

Table AIII.
Interview guide (IT support, nurses, nurse aids, medical secretaries)

About the authors

Karin Hedström is Professor of Informatics at Örebro University. She holds a PhD in Information Systems Development from Linköping University. Her research interests concern the ethics of information systems, e-government and information security. Dr. Hedström has published in numerous international journals and conference proceedings. Karin Hedström is the corresponding and can be contacted at: karin.hedstrom@oru.se

Fredrik Karlsson is Professor in Informatics at Örebro University, Sweden. His research on information security, tailoring of systems development methods, system development methods as reusable assets, CAME-tools, method rationale and electronic government has appeared in a variety of information systems journals and conferences. He is currently research leader of the research environment Centre for Empirical Research on Information Systems (CERIS) at Örebro University.

Fredrik Söderström is a PhD Candidate in Information Systems at Linköping University and his dissertation is focused on electronic identification (e-ID) in the public sector. Fredrik has a particular interest in how various organisational and social aspects affect the development, implementation and use of e-ID solutions across different organisational levels. He has a long experience working as a software developer in the private sector and has actively followed the development of the Swedish e-ID since 2011.