Managing the development of e-ID in a public e-service context: Challenges and path dependencies from a life-cycle perspective

Ulf Melin, Karin Axelsson and Fredrik Söderström

Original Publication:

Ulf Melin, Karin Axelsson and Fredrik Söderström, Managing the development of e-ID in a public e-service context: Challenges and path dependencies from a life-cycle perspective, 2016, Transforming Government, (10), 1, 72-98.
http://dx.doi.org/10.1108/TG-11-2013-0046

Managing the Development of e-ID in a Public e-service Context – Challenges and Path Dependencies from a Life-cycle Perspective[1]

Melin, Ulf; Axelsson, Karin; Söderström, Fredrik

Department of Management and Engineering, Information Systems, Linköping University, SE-581 83 Linköping, Sweden.

ulf.melin@liu.se; karin.axelsson@liu.se; fredrik.soderstrom@liu.se

Full reference and citation to published version of this journal article: Melin, U., Axelsson, K, Söderström, F. (2016): Managing the development of e-ID in a public e-service context - challenges and path dependencies from a life-cycle perspective, Transforming Government: People, Process and Policy, 10(1), pp. 72-98.

Abstract

Purpose – The purpose of this article is to analyse and understand the contemporary management of e-ID development to: a) identify and formulate challenges and b) reflect upon the use of a combination of perspectives. In order to generate knowledge on this issue we investigate e-ID development in Sweden from: an e-government systems development life-cycle perspective and a project challenge and critical success factor (CSF) perspective.

Design/Methodology/Approach – This is a qualitative case study covering an analysis of the three years in a larger project focusing e-ID in a public e-service setting. Empirical sources have been face-to-face interviews, official documents, and different kind of forums for presentations and discussions in for example hearings arranged by authorities, meetings with the coordinating agency, and practitioners' networks events.

Findings – This study concludes that there are significant challenges involved in managing e-ID development due to its contextual and integrated character. Challenges involve the organization and management of the program and can be traced back to e-government, general project management literature and theory on path dependency. Based on this study we can question, e.g., governance models, centralization, and a narrow focus on the technical artefact. Our study is also an illustration of a possible way to analyse e-ID within an e-government initiative.

Practical implications – The present research shows that an e-ID can be considered as a back office enabler for launching e-services, but also highlights the need for management of the artefact as an *integral part of e-service development* because it is intertwined with the *use of e-services* from a user perspective. This aspect, together with the insights related to challenges and success factors including path dependency provide implications for future practice of e-ID management and development in particular and IS artefact development in general.

[1] This manuscript builds on an idea developed and partially explored in Melin, U., Axelsson, K., Söderström, F. (2013): Managing the Development of Secure Identification – Investigating a National e-ID Initiative within a Public e-service Context, European Conference on Information Systems (ECIS), Utrecht, The Netherlands, In: Completed Research, Paper 63, http://aisel.aisnet.org/ecis2013_cr/63

Originality/value – This article addresses challenges related to the development of e-ID in a public e-service setting. Few studies have theoretically combined a life-cycle perspective on challenge and success factors related to e-ID development while also focusing different dimensions of path dependency as an example of a challenging area within a program frame. Studying e-ID as a contemporary phenomenon from a contextual perspective in line with sociomaterial thinking – with a focus on the interplay between technology and people – can also help us to understand and discuss artefact development in general.

Keywords – e-ID, electronic identification, implementation, public e-services, e-government, project management, path dependency.

Paper type – Research paper

1 Introduction

Electronic identification (e-ID) is an important prerequisite and key enabler for the secure identification, authentication and digital signing via the Internet and as a part of all aspects of secure e-service design (European Commission, 2010; 2015a; Halperin and Backhouse, 2008; Price, 2008; Rössler, 2008). As users, and digitized citizens, we become increasingly reliant on electronic solutions that give us a certain level of utility and trust, and use e-ID solutions to interact with local and central government (Collings, 2008) in an e-service context. Developing and implementing e-services and e-IDs continue to receive much attention in practice. In Europe, for example, individual EU states had issued e-ID solutions to more than 22.5 million citizens already in 2008 (Collings, 2008) and there is more to come in the area of development and distribution of e-IDs (Halperin and Backhouse, 2008). Significant investments are needed in development of e-government in general (Irani et al., 2005; 2007), trying to create new opportunities in the public sector's delivery of e-services which in turn requires identified citizens. Accordingly, an e-ID is of paramount importance for almost all e-government service applications (Rössler, 2008) and pointed out as one of the building blocks to provide secure electronic cross-border transactions and services (European Commission, 2015b) as a part of creating a Digital Single Market creating such online opportunities (European Commission, 2015a).

Developing, implementing and managing public e-services and secure e-ID solutions are challenging (Rissanen, 2010; Bühler et al., 2014; Liginlal et al., 2012) and require coordination and management. The European Commission recognises that common standards in issuing procedures are highly desirable in the field (Collings, 2008). Such procedures include people, processes and technology (ibid.), which stresses the complexities and interwoven character of an e-ID as an artefact in an e-service and in an institutional (or governmental) arrangement; not an isolated technical artefact. The fact that *path dependency* is present (Kubicek and Noack, 2010b) is also a challenging aspect for the development of e-IDs and formation of information systems (IS) strategy in general (Peters et al., 2002). Path dependency theory has its origin in economy, but is also applied in sociology, political science and organization theory. Industry evolution and technology adoption processes are areas of exploration. Path dependence originates from the idea that: "[…] a small initial advantage or a few minor random shocks along the way could alter the course of history" (David 1985) (Page, 2006, p. 87). In this article different types of path-dependency will be analysed and discussed in relation to the empirical case.

Managing e-ID development can on a general level be governed by an active role of the government, and/or managed by market driven solutions (cf. Grönlund, 2010; Kubicek, 2010). The reported fact that several e-government initiatives in general face a number of challenges of complexity and risk is another factor that calls for further studies (Irani et al., 2007; Gil-García and Pardo, 2005; Rosacker and Olson, 2008), using the development process of e-IDs as a contemporary example. The embedded complexity and risk in development and implementation projects can be considered as one explanation to why reports on project failures are common. An important issue for IS project management and e-government, in practice and research, is to understand how we organize initiatives like this and why some initiatives progress to success while others end in failure (e.g. Heeks and Stanforth, 2007; Melin and Axelsson, 2009; Christiansson et al., 2015).

Scholars have started to investigate e-ID development, but often from a technical oriented perspective focusing on the artefact as such as a part of e.g. an e-government initiative. However, this perspective represents much more than an information technology development perspective; "[…] the technology is only the customer facing front-end of a complex set of organizational structures, policies, and processes that are designed to provide particular services." (Grant and Rose, 2010, p. 29). On an overall level, there is a strong technical bias in the research and development of identity management-related concepts (Otjacques et al., 2007). Therefore, we argue that there is a need for more contextual studies focusing on implementation, processes and organizational settings and in accord we suggest a

program level analysis of the e-ID development to achieve a contextual perspective beyond the technology.

In this article the management of e-ID development in Sweden is studied as an example of a national e-ID program initiative. Learning from the past and from the experiences of different development initiatives is essential for the development of public e-service (Irani et al., 2007). There is also a call for empirical e-ID development studies moving away from the technical artefact (Halperin and Backhouse, 2008) to broaden the scope of the consequences of this specific kind of technical solutions (cf. Otjacques, 2007). The actions within the initiatives studied in this article are a response to what is perceived by the Swedish Government as poor centralized coordination of e-ID solutions. The poor coordination in this case have later been acknowledged by the Government forming of the e-identification (e-ID) Board that focuses solely on coordination and sustainable development of the e-ID solution.

Based on the reported fact (above) that e-government development initiatives, and especially inter-organizational projects, face a number of challenges, this article argue for a more thorough understanding of e-ID development within a public e-service context. The overall purpose of this article is to analyse and understand the contemporary management of e-ID development to: a) identify and formulate challenges, and b) reflect upon the use of a combination of perspectives. In order to generate knowledge on this issue we investigate e-ID development in Sweden from: a) an e-government systems development life-cycle perspective (Heeks, 2006) and b) a project challenge and critical success factor (CSF) perspective (Gil-García and Pardo, 2005). The e-ID development is regarded as a process and a special case of an IS development (ISD) initiative; performed under a certain set of laws and regulations, and therefore interesting to learn from. The research questions are: 1) What challenges and success factors are represented in a national e-ID development initiative?, 2) How can we judge the success/failure of an e-ID development initiative using a life-cycle framework?, and 3) What can we learn from the management of development of e-ID in a public e-service context on a program level, taking path dependencies into account?

After this introduction, the article is organized in the following way: in Section Two related research and theories on managing e-government and e-ID development are addressed; this section is followed by the research design in Section Three and a case study introduction in Section Four. The article continues with analysis and findings from a life-cycle perspective together with challenge and CSF's in Section Five; and finally, the article is concluded and discussed in Section Six, also with suggestions for further research.

2 Related Research

Within this section identity and identification are briefly defined and an outlook of previous e-ID studies is made, followed by a discussion about management of e-ID development from a program and a life-cycle perspective.

2.1 e-ID in a Public e-Service Context

An e-ID builds on *identity* as a central element. On a general level, identity can be viewed as a "[…] dynamic collection of all attributes related to a specific entity, normally a citizen but the concept can be extended to include an enterprise, or object. […] an identity is what allows entities to be distinguishable." (Collings, 2008, p. 62). This makes identity a critical component in several transactions (social, economic and administrative). *Identification* can be defined as "the process of using claimed or observed attributes of an entity to deduce who the entity is." (Kubicek, 2010, p. 10). The field of identification and identity contains technical as well as social aspects of organizational and personal identity (Lyon, 2009; Söderström and Melin, 2012). There are studies focusing on identification (Seltsikas and O'Keefe, 2010; Whitley and Hosein, 2008), and on organizational and personal identity (e.g. Beynon-Davies, 2011; Kotlarsky and Oshri, 2005). Studies of identity in the IS

field focus e.g. on identity management (Barnard-Wills and Ashenden, 2010; Kubicek, 2010; Kubicek and Noack, 2010b; Otjacques et al., 2007) and policy engagement processes (Whitley and Hosein, 2007). Some studies have focused on the concept of national e-IDs and identity cards. In Denmark, for example, the development of the Danish e-ID has been described as a troublesome way of developing a national e-ID, despite a political attention and a high degree of e-readiness. The case of the Danish e-ID was also described as a paradox, and the main problems of implementation were related to privacy concerns, a lack of inter-governmental coordination, and a lack of private-public sector cooperation (Hoff and Hoff, 2010). Another Scandinavian e-ID initiative, the Finnish Electronic Identity (FINE-ID) card, failed to realize due to a poor uptake on a market with already existing commercial e-IDs (Rissanen, 2010) which in turn demonstrates the challenges at hand in reaching high diffusion and use for state issued e-IDs diverging from private sector use. While the e-ID artefact itself and different country based strategies or programs have continued to be focused in e-ID research, scholars also seem to have broadened the scope recently of potential aspects affecting its implementation and use as well as its societal benefits and challenges. For example, studies have focused on challenges regarding usability when delivering a national e-ID with a high level of security (Bühler et al., 2014) and also acknowledged different types of barriers towards adoption of digital identities (e-IDs) such as socio-technical and/or cultural (Liginlal et al., 2012). In addition, the development of multi-purpose smart cards such as card based national e-IDs has also raised privacy and security concerns (Shukri and Hafiz, 2015) as well as a need to safeguard the individual's rights in relation to digital identities (Sullivan and Stalla-Bourdillon, 2015). The very strong current development of the mobile platform has also raised concerns of new threats for identity management as a result of the convergence of the Internet and mobile platform (Jøsang, 2013). Further, initiatives trying to harmonize national e-IDs enabling interoperable cross-border services, e.g. the eIDAS regulation described below, have also gained considerable focus (e.g. Dumortier and Vandezande, 2012; Cuijpers and Schroers, 2014).

In digitizing Europe for example, the e-ID has been regarded as an important back office enabler for launching e-services and transforming government (European Commission, 2010) and sometimes mentioned as "other ICTs", together with database, networking, tracking and tracing (Jaeger, 2003; Zissis and Lekkas, 2011; Yildiz, 2007). Lately, the e-ID has received more attention since it has been identified as one of the key enablers of the Digital Single Market initiative with the aim of minimizing barriers and creating online opportunities (European Commission, 2015a). Thus, the e-ID is considered to be one of the building blocks to provide secure electronic cross-border transactions and services (European Commission, 2015b). To realize this cross-border European e-ID, the eIDAS regulation (EU No 910/2014) will provide the legislative framework and this development was motivated by the need of broadening the scope of the e-ID to include important aspects such as cross-border functionality. In turn this also addresses the too narrow focus of the previous e-Signature Directive (1999/93/EC) (European Commission, 2015c).

Turning back to the Swedish context, Grönlund (2010) focuses on the national e-ID emergence, where the market approach is further investigated and describes the Swedish e-ID, prior to the development focused in this article (e.g. the creation of the e-ID board and a more centralized approach), as a fairly complex solution based on a market approach with no central governance, but with a good service supply and use (ibid.). Given the focus of these studies of national e-IDs, we identify a need to investigate the Swedish e-ID further.

Launching e-IDs for citizens and businesses is very important for the governments in order to realize e-government policies and to provide better services to citizens, in an efficient, secure and trusted way on national as well as imminent transnational levels. Kubicek and Noack (2010a, p. 237) describe the rollout phases of e-ID projects and reflect upon the choices of different solutions for e-IDs and digital signatures. A high degree of path dependency is identified e.g. in Denmark and Sweden (ibid., p. 240) based on the fact that these countries are not following the European standards of hardware-based solutions for IDs and digital signatures. This is one aspect that describes the challenges related to the management of national e-ID development and the need to have a contextual perspective when investigating e-ID. A contextual focus taking the point of departure in the reasoning when IT artefacts

and organizations both arise at the intersection of social and material phenomena (Leonardi and Barley, 2008) and where the interplay between technology and people is in focus (i.e. an ensemble view; Orlikowski and Iacono, 2001). A combination of the interests of e-ID development, implementation and use from a sociomaterial perspective (further elaborated below) is to our knowledge not found in the literature and therefore interesting to explore in this research.

Within a European context there is good practice reported in INT-IS-IOP cases (Good Practice Case, 2006). If we take a look at Estonia, for example, their model is highly centralized and standardized with centrally provided unique identification number for each Estonian resident. This model is also combined with a central single point of access to public services (an e-citizen portal). The development model and governance structure used in Estonia is another example of path dependency addressed above. The national context and the overall governance traditions and models is determining the domain also of the development of e-ID, e.g. what is desirable and possible to accomplish in this area.

Path dependency, introduced above, is relevant to discuss in relation to development and implementation of e-ID. Kubicek and Noack (2010b) studied four national e-ID identity management systems (eIDMS) in Europe. They identified three types of paths; technological, organisational, and regulatory. One conclusion is that path-related decisions can concern the technical dimensions of an eIDMS, the organisational arrangements surrounding and supporting it, and the pattern of regulation. Kubicek and Noack (2010b) also reflect on how the creation of how new organisational or regulatory paths affects the establishment of new institutions and a change in contextual factors (e.g. legal structures and administrative structures on a national level). Using path dependency as a vehicle for understanding these issues is an important aspect for the present study, using a contextual perspective on the contemporary management of e-ID development in Sweden.

If we return to the more general definition of path dependency, Page (2006) interpret the concept of path dependence, based on David (1985), as almost metaphorical. Page (2006, p. 88) defines the meaning of path dependency as: […] current and future states, actions, or decisions depend on the path of previous states, actions, or decisions." In this work, and a literature review, Page (ibid.) also reveals four related causes in path dependency: (1) increasing returns, (2) self-reinforcement, (3) positive feedbacks, and (4) lock-in. In short, increasing returns means that greater benefits are expected when more choices or actions are taken, self-reinforcement means that a set of forces or complementary institutions encourage certain choices to be sustained and positive feedback means that the same choice is made by other actors and that the particular choice or action thereby receives positive externalities. Lock-in, finally, express that one action/choice becomes better than another because a sufficient number of people have already made that particular choice.

Studies of IS strategy and path dependency focusing on the evolutionary dimension of paths (e.g. Peters et al., 2002) also concludes that the paths of evolution cannot easily be reversed and that they shape the future path of the evolution of and organization (cf. Mintzberg, 1989). Using this perspective, we can conclude that past changes shape the current context of organizations (Ayres, 1994) or other collective, coordinated, efforts (Peters et al., 2002). Ayres (1994) link the existence of path dependency with the role of the IT champion and his/hers vision since the vision plays an important part in the evolution of an IS strategy and in change.

2.2 Managing e-ID Development

Rose and Grant (2010) report that the implications of e-government growth and evolution are not obvious. There are several unintended consequences and unfulfilled expectations. This calls for further studies of the management of such initiatives. The sections below describe theoretical points of departure for the management of e-ID development.

2.2.1 Managing e-ID Development – A Life-cycle Perspective

Viewing development of e-government in different life-cycle phases is common. Heeks (2006) describes that an e-government development project typically consists of five stages; (1) project assessment, (2) analysis of current reality, (3) design of the new system, (4) system construction, and (5) implementation and beyond. The development model for e-government suggested by Heeks (2006), and applied by e.g. Melin and Axelsson (2009), has several similarities with traditional systems development life-cycles or so called waterfall models (e.g. Avison and Fitzgerald, 2003; Tsai et al., 2009). The development of public e-services, including e-IDs, takes place in a certain context, but the tasks performed in each stage seem to be more or less the same. As mentioned above these phases will be used to structure the analysis (Section 5.1) in this article. Project assessment (1) in the development model, described by Heeks (2006), is the identification of possible e-government projects. In this phase, the outline of basic project parameters is completed, together with the assessment of whether or not to proceed with the project. E-government projects are typically oriented towards pragmatic problem solving or opportunity seeking (Heeks, 2006, p. 162). An opportunity can arise from different sources (internal or external). Analysis of current reality (2) includes the creation of descriptions of information, technology, processes, objectives and values, staffing and skills, management systems and structures, and other resources such as money and time. This stage consists of a mixture of hard and soft techniques such as an IS audit, an IS analysis, a problem analysis, a context analysis, etc., in order to build an overall map. A SWOT analysis can be conducted at this stage (ibid.). The design stage (3) consists of setting objectives related to dimensions (objectives) of the new system (including hardware and software). Organizational processes are also necessary to take into account from a design perspective. System construction (4) consists of the process and activities in acquiring new IT, undertaking detailed design of the new e-government system, building it, testing it, and documenting it (ibid.). The last stage, implementation and beyond, (5) is represented by the planning of implementation processes (training users, data conversion, systems maintenance activities, introducing the new system, monitoring and evaluating performance and context) (ibid.). In accord, diffusion and use of the system is not a part of the scope of this article.

2.2.2 Managing e-ID Development – A Challenge and CSF Perspective

The challenges in managing e-government development, with e-IDs as one part, can be related to factors covering: information and data, organizational and managerial issues, legal and regulatory preconditions, and overall institutional and environmental aspects (Gil-García and Pardo, 2005). One critical barrier that needs to be overcome is the delaying factor of the lack of organizational cooperation (Kubicek and Hagen, 2000) in inter-organizational projects or programs. In general, agencies tend to act too independently – the initiatives tend to be poorly coordinated (Irani et al., 2007). This lack has also been the reality when it comes to the historical development of the national e-IDs (Grönlund, 2010; Söderström and Melin, 2012). There are several reported challenges when managing e-government initiatives. Reasons for failure are multifaceted (Sarantis et al., 2011), but some common reasons are: lack of internal ownership, a weak strategy and/or vision, poor project management (including management of technology), unsuitable technological infrastructure, and challenges related to data interchange. Interestingly, over-reliance on IT as a main driver for e-government development and inadequate administrative reform/process change are patterns also mentioned (ibid.). Kubicek and Hagen (2000) present six key areas of barriers to be overcome for fewer delays, failures and obstacles in e-government development. The first key area is the lack of organizational cooperation, the second key area is the deficiency of legal regulations, and the third key area is the necessary area of pre-conditions in regard to technology and, fourth, in regard to human factors. The last barriers are the lack of appropriate funding and political support. Signs of project failure in general are reported by e.g. Reel (1999) and seem to be relevant and present also in e-service development of today (Heeks and Stanforth, 2007; Melin and Axelsson, 2009). Those signs can be linked to the e-government patterns above. Examples are: project managers do not understand users' needs, the project scope is ill-defined, project changes are managed poorly, the chosen IT changes,

business needs change, deadlines are unrealistic, users are resistant, sponsorship is lost, the project lacks people with suitable skills, and managers ignore best practice and previous lessons learned (ibid.).

Going back to e-government in particular, Gil-García and Pardo (2005) propose five categories of *challenges* for e-government initiatives. These categories will be used to structure the analysis in Section 5.2. The categories are: (1) information and data, (2) IT, (3) organizational and managerial, (4) legal and regulatory, and (5) institutional and environmental. Adapted from Gil-García and Pardo (2005, p. 191-192), using Melin and Axelsson (2009) as a point of departure, and including a source covering software development risks to project effectiveness (Jiang and Klein, 2000), the categories can be summarized as follows: Information and data (1) covers the capture, management, use, dissemination, and sharing of information (ibid.). There are also aspects of data quality and data accuracy in this category, important in e-government initiatives. In the IT category (2) usability and security issues, technological incompatibility, technological complexity, technical skills and experience, and technological innovation are present. Organizational and managerial challenges (3) are considered to be the main challenges to ISD initiatives. The size (scope) of project, strategic alignment (IT and organization) and the diversity of users and organizations involved are important factors in this category. Dawes and Pardo (2002) also address the existence of multiple, partially conflicting goals in the public sector, which is critical for e-government initiatives. Legal and regulatory changes (4) represent the formal rules that government organizations operate upon. Restrictive laws and regulations must be taken into account when developing e-government in general and e-IDs in particular. The institutional and environmental challenges (5) are the institutional framework in which governments operate (ibid.) and include the policy environment. Norms and actions are also examples of the policy environment which is important for the success or failure of e-government development initiatives (Gil-García and Pardo, 2005). The authors (ibid., p. 193) discuss that "privacy and related security issues are challenges that must be adequately addressed in government IT initiatives" and that security issues are linked to (2), (4) and (5) above. Our research is one way of addressing e-IDs as a part of the supply of secure e-services.

Handling challenges and achieving success in e-government is not only a question of choosing the appropriate technology; it also includes managing capabilities in organizations, and regulatory and environmental conditions (ibid.). Looking at the other side of the coin (handling challenges above), the literature in the area of e-government and ISD projects reports on several sets of *success factors*. Gil-García and Pardo (2005) and Ho and Pardo (2004) have carried out literature reviews of key success e-government strategies. Examples of CSF's are top management commitment, project linkage to business, technical alignment, knowledgeable personnel, and user involvement.

Challenges and success in managing e-ID development can also be linked to how we frame the development initiatives. Rose and Grant (2010) propose a conceptual framework supporting the management (planning and implementation) of *e-government programs* (a collection of projects/initiatives). The framework, built around traditional marketing mix components, takes a point of departure in customer (citizen) focus and a relationship management perspective. Aspects like price, product, place, and promotion (4Ps) are addressed within a customer relationship management (CRM) approach (e.g. Schierholz et al., 2007). Each of the aspects in the conceptual framework includes critical issues derived from a literature review in the field of planning and implementation of e-government initiatives (ibid.). Rose and Grant (2010) emphasize that program management significantly can contribute to an overall success of a program. They list critical program management issues and relate them to e-government. A strong and active leadership is at the top of the list followed by several aspects linked to the broad spectrum of e-government programs being far more than technology implementation programs. Aspects like change management, policy, processes, structures, as well as laws and regulations are also identified as important (Gant and Gant, 2002). A rather centralized approach is proposed to ensure that a program is implemented in a consistent way throughout various agencies (Rose and Grant, 2010; Ke and Wei, 2004). Consistency should also be based on a robust strategy (ibid.), including political and bureaucratic support and funding. Due to the

numerous internal and external stakeholder groups with different agendas the issue of defining the program's goals, scope and outcome is cumbersome. Another CSF is the coordination of e-government programs on different levels (federal, provincial/state, and local level [Jaeger and Thompson, 2003; Rose and Grant, 2010]). To ensure privacy and security is also considered as a critical issue in the literature study (above).

3 Research Approach

This is a qualitative case study (Walsham, 1995). This article reports an analysis of the first three years in a larger longitudinal project focusing e-ID development in a public e-service setting between 2011 and 2014. The overall area of interest is to study policies, implementation and practice of e-ID in Sweden, including key actors, important decisions and events (cf. Langley, 1999), challenges and limitations related to the governance, as well as development and use of e-IDs. The overall project involves studies of the development on different levels; governmental actors, forums, descriptions (official documents published online or distributed in other ways), and case studies on organizational levels of implementation of e-IDs.

One way to investigate e-ID development and implementation is to divide the process in different phases; like any ISD project with generic phases such as analysis, design, construction, and implementation (e.g. Avison and Fitzgerald, 2003; Axelsson and Melin, 2009; Heeks, 2006). According to Tsai et al. (2009) government agencies often use traditional ISD life-cycles with generic phases. In the analysis below, inspired by Axelsson and Melin (2009), five generic stages are used to structure, assess and analyse the degree of success or failure in the e-ID development case. The analysis below is therefore structured based on the different stages in an e-government system life-cycle described by Heeks (2006), and on challenges to e-government identified by Gil-García and Pardo (2005), introduced above. In other words these theories have been used as guides and an analytical lens for structuring and analysing (Walsham, 1995) empirical data from the national e-ID program studied and the documents governing the initiative. The aim of explicitly using the concepts from Heeks (2006) and Gil-García and Pardo (2005) as lenses is also to contribute to that body of knowledge. At the same time the analysis tries to discover new concepts, areas and issues in the empirical material in an explorative matter as a part of a reflexive (Van de Ven, 2007) research approach. Adding a sociomaterial view (Orlikowski, 2007; Leonardi and Barley, 2008) together with an ensemble view on e-IDs is an example of the reflexive research approach, as this point of departure is fruitful in order to make the contextual aspect in this piece of research more explicit. The contextual perspective is distilled and applied in this study when we express the need to take future use and organizational characteristics of different settings (e.g. the organization of future work processes and different stakeholders use of e-IDs) *and* material dimensions of e-ID artefacts (e.g. the physical representation of e-ID carriers [cards] and card readers, unpacking the often unpacked black-boxed technology [Orlikowski and Iacono, 2001]) and taking them into account acknowledging path dependency when designing future e-ID solutions. The program perspective introduced above also helps us to broaden the scope. Another important aspect from a sociomaterial view is the bridging of the activities between development and future use (Leonardi and Barley, 2008) and the dynamic interplay between technology and people from an ensemble view of technology (Orlikowski and Iacono, 2001).

Important empirical sources have been the 11, on site, face to face, semi-structured qualitative interviews lasting approximately 1 hour each, with different actors deeply involved in the e-ID process e.g. an office manager of the e-ID Board, a government security expert, an e-ID concept manager and several agency e-ID development representatives, different kind of forums for presentations and discussions such as hearings and annual seminars arranged by authorities (e.g. the e-ID Board), meetings with the e-ID Board, practitioners' networks events and documents (e.g. the Swedish e-ID practitioner network hosted by the Swedish Computer Society and government level policy documents and reports). The respondents (described above) were identified by snowball sampling (Patton, 1980)

and represent e-service providers such as central government agencies, local authorities and health care regions as well as the provider of the technical e-ID solution itself.

4 Case Study Introduction

The emergence of the present national public e-ID policy in Sweden can be traced back to the end of the 1990s, when the government started to investigate the future use of public e-services. The need for secure and coordinated solutions for identification was pinpointed in this work. Internet banking (e-banking) was already well established by then as a channel for delivering banking services and had an installed base of solutions for identification. In 2000/2001, The Swedish Tax Agency got the commission to investigate a national e-ID solution for the public sector, resulting in the first set of frame agreements with e-ID providers. Frame agreements that agencies need to follow during a certain period of time. Accordingly, this government initiative, called the SAMSET project (RSV, 2003) (overview in Figure 1) was the starting point of the public e-ID of today (Grönlund, 2010; Söderström and Melin, 2012). The market driven e-ID delivery model was chosen for several reasons; 1) to support competition among providers, 2) to promote e-IDs as an important driver for further e-service development, and 3) to avoid investments in e-ID (Grönlund, 2010). Grönlund (ibid., p. 196) describes the market driven model as advanced: "Not only the e-IDs themselves but also the control structure, the certification system, was left to the providers." Other major incentives behind this approach were the public sectors' potential access to the significant stock of e-banking customers already established (Söderström and Melin, 2012) and potential efficiency gains by an increased level of service automatization.

In mid-2015 the banking sector had approximately 6.5 million identified customers/users with an estimated yearly transaction volume of over 1 billion. Approximately 90 % of the e-ID use in Sweden is currently related to e-banking services (provided by the BankID consortium) and 10 % is related to public e-services (BankID, 2015).

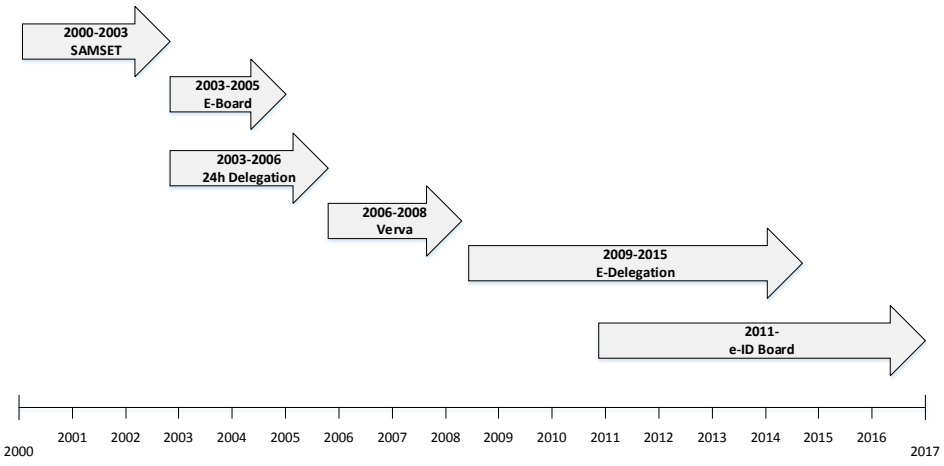

Figure 1. Overview of Swedish governmental e-ID actors

Apart from the initial SAMSET project, several governmental actors have historically been active in developing the Swedish e-ID as illustrated in Figure 1 above. After the SAMSET-project, the E-Board focused on further defining the e-ID as well as developing guidelines for the e-ID (E-Nämnden, 2004) as well as its use in public e-services (E-Nämnden 2005). Acting in parallel from an added benefits perspective, the 24h Delegation focused on how to stimulate the development of public sector e-services including the use of the e-ID (24-timmarsdelegationen, 2005). As the result of a more general

focus on public sector development, the Agency for Administrative Development (Verva) managed the development of the secure electronic exchange of information and safe handling of electronic documents between 2006 and 2008. In its final report (VERVA R 2008:12a, b), the agency pinpointed the need for: 1) a distinct definition of the Swedish e-ID and 2) a central coordinating body. As a result of this and other actions the e-Government Delegation (e-Gov Delegation) was created in 2009. Their role was to strengthen national inter-organizational development of e-government including e-IDs. This can be considered as a new wave in the Swedish management of e-ID development on a national level. As a part of the coordination, a technical infrastructure based on a solution where the government should act as a central node towards the issuers (e.g. the banks) was suggested. According to the e-Gov Delegation, this solution should serve as a basis for the technical interoperability for electronic identification and facilitate further diffusion and development in the area (SOU 2009:86; 2010:62). Later on the delegation was appointed to investigate the next generation of inter-organizational e-ID solution (SOU 2010:104). This initiative was driven by the fact that the current procurement model was outdated, without any reported option of renewal. The investigation resulted in a report, dominated by a technical oriented blueprint. In January 2011 the previously suggested coordinating authority (see above) named The Swedish e-ID Board was created, with a mandate to centrally coordinate, manage and develop sustainable e-ID solutions based on the investigation's report.

The main purpose of the e-ID Board, a subordinate agency to the Ministry of Enterprise and Innovation, is to coordinate and support the need for secure solutions for electronic identification and digital signing as a part of the provision of e-government services within the public sector (i.e. agencies, municipalities and regional health care). The e-ID board itself is headed by an appointed chairman and consists of six members with leading positions in the Swedish public sector. Together they represent the Swedish Companies Registration Office, the Swedish Post and Telecom Authority, the Swedish Association of Local Authorities and Regions, a legal perspective and the Swedish Pensions Agency. In addition to the Board members, there is also an office which holds a manager, two strategists, a legal expert and an administrator. Over the years, the e-ID board has also been forced to enlist the help of third party contractors such as technical security consultants.

So far, the main task of the e-ID Board has been to develop and implement the new version of the Swedish national e-ID (Svensk e-legitimation) as described in their mandate. This work has been done under an extreme tight timeframe and the launch date has been pushed forward on several occasions. This mainly due to the fact that the development of the new e-IDs is a huge undertaking including aspects such as technical, commercial and legal and it even demanded a legislative amendment.

Grönlund (2010) compares the historical Swedish e-ID development with other EU countries, and characterizes the Swedish approach, until 2010, as a fairly complex, and market driven, solution, with multiple contracted private e-ID providers, no centralized e-ID identity management system, and several e-ID card solutions in parallel. One has also to keep in mind that Sweden has a governance model with strong, rather independent, public agencies and relatively weak Ministries; at least historically, and policies are more negotiated than implemented top down (ibid). The National Audit Office in Sweden regards the political leadership as weak in this sense. As reported above, the Cabinet are more in control, however, since 2009 (Grönlund, 2010; SNAO, 2009). The proposal, above, by the e-Gov Delegation is a step towards a centralized e-ID infrastructure focused in this article. This includes aspects such as standardization, usability, privacy, and costs focus (ibid.).

The e-ID solution developed by the Swedish e-ID board is characterized as being a federated e-ID solution where the e-ID board acts as a central node for the entire public sector. Hence, the providers of e-ID solutions must meet the requirements (the trust framework) as formulated by the e-ID board to become approved providers of the new Swedish e-ID. Further, the e-ID board becomes the sole contracting party towards the providers since it signs the agreements with the approved providers with the power of attorney of public sector actors. Hence the e-ID board also have to sign agreements regarding regulations and technical infrastructure with the e-service providers (i.e. the agencies, municipalities and health care regions). This federated structure has been put forth as a simplification

and a more flexible solution than the previous bilateral procurement model where the agreement was signed between one public sector actor and one e-ID supplier for a fixed period of time. From a user's perspective this e-ID model also means that a central e-ID switch will be hosted by the e-ID board where the user selects his or hers preferred way of electronic identification among all approved and signed e-ID providers when using the public sector's e-services (i.e. a central e-ID forwarding service).

5 Analysis and Findings

The analysis in the two first sections below is structured according to the life-cycle perspective on development followed by a challenge and CSF perspective on program management introduced above. When we discuss the findings from using the life-cycle and the CSF perspective we also add the dimension of path dependency introduced above.

5.1 Managing e-ID Development – A Life-cycle Perspective

A life-cycle perspective is introduced in section 2.2.1 above, and the different stages suggested by Heeks (2006) are utilized below to structure the analysis of the e-ID development initiative.

Project assessment – E-government projects are typically oriented towards pragmatic problem solving (Heeks, 2006); the studied e-ID initiative is no exception. The current procurement model (and the frame agreement) in Sweden was outdated, so an explicit need for a new e-ID solution was present. Opportunity seeking (ibid.) is another orientation identified in the literature and in the empirical case. From a political perspective the e-ID initiative was a way of trying to stimulate competition among e-ID providers and to have several actors on the future market. However, even if the external pressure from the outdated frame agreement were present, the initiative had scarce resources available. Therefore decisions were taken in order to postpone the deadline on several occasions which in turn influenced the next step below.

Analysis of current reality – The analysis of the current reality in the e-ID initiative was initially extremely forced in time and temporarily staffed. The initial intention was to anchor the plan in different stakeholders' (government agencies, providers, citizens etc.) views, but the report describing the current reality and the design has, instead, been developed in a more isolated and forced way. The report as such contained a principal blueprint of the next generation technical solution of the e-ID, based on a market driven approach. The contextual analysis (e.g. to include different governmental levels), is an important part of this stage according to the literature (Heeks, 2006), were put in the background in the project and the technology in the foreground. A SWOT analysis that can, for example, be completed at this stage (ibid.), was first operationalized in the referral process (below), increasing the risk of developing and managing and national e-ID solution that is not optimal.

Design of the new system – important activities in this stage (Heeks, 2006) is the setting of objectives related to dimensions of the new system (including hardware and software). Organizational processes are also necessary to take into account from a design perspective. No IT artefact design (hardware and software) took place at this stage in the studied project; instead a more conceptual design of the system was made. The model proposed in the report was based in multiple contracted private e-ID providers and a federated e-ID solution with the e-ID Board acting as a central coordinating contractor between the e-ID providers and the e-service providers. According to the plan, the Board should deliver and maintain a central technical base structure (an Identity Federation) for the public sector. Important design issues (e.g. digital signing) were not solved in detail at this stage. In order to open up the design process and to collect feedback on the future e-ID report, the managing ministry initiated a referral process in the spring of 2011. Critique from actors in the public and the private sector was frequent, and several actors mentioned that the conceptual and principal development was not enough, it was interpreted as "too theoretical".

System construction – this stage consists of the process and activities in acquiring any new IT, undertaking detailed design of the new e-government system, building it, testing it, and documenting it (ibid.; Melin and Axelsson, 2009). In the present case, still no IT artefact (application) is constructed; beyond the conceptual infrastructure is instead in focus also at this stage. This was still interpreted as a challenge, and compared to the existing, tested, and wide-spread market driven solution. The main purpose with the construction of the infrastructure for the national e-ID is to conceptually design secure e-ID solutions, to provide an agreement model, an infrastructure and regulatory framework for electronic identification and signing, and to procure additional technical services needed. Time consuming building of trust and acceptance was made in this phase trying to establish a dialogue.

Implementation and beyond – the last stage, implementation and beyond, includes the planning of implementation processes introducing the new e-government system; monitoring and evaluating performance and context (Heeks, 2006). In the focused plan there are a number of activities such as changes in the constitution, preparation of agreements, technological development, and the establishment of frameworks for security and trust related to this stage. All these dimensions are challenges for the future implementation. A transition plan can also be seen as a critical part of the work to ensure a smooth transition from the current to the future model as a part of the implementation process. The latter aspect is an important issue for implementation and beyond (future use; i.e. how the suggested federated national e-ID solution will affect the current one) together with the intention that the model for e-IDs should be sustainable and flexible (SOU 2010:104); which is a challenge in itself.

5.2 Managing e-ID Development – A Challenge and CSF Perspective

This part of the analysis is based on challenges to e-government identified by Gil-García and Pardo (2005), introduced above (Section 2.2.2). The findings regarding these challenges and in some sense inverted success factors are used to assess the e-ID initiative and summarised below. Some of the empirical examples have also been used when discussing the life-cycle perspective above. Below, input from the theoretical section looking at the e-ID initiative from a program perspective (Section 2.2.2) is integrated. The reasons for failure in this area are multifaceted (Kubicek and Hagen, 2000; Sarantis et al., 2011). Several challenges are present also in the e-ID development program. Related to the e-ID initiative ownership is a key issue within the Swedish model for governance (Section 2.2.2). The untested, conceptual, infrastructure for e-IDs is also a challenge from a program management perspective.

Information and data – this category covers the capture, management, use, dissemination, and sharing of information. There are also aspects of data quality and data accuracy in this category (Gil-García and Pardo, 2005). The federated e-ID solution in the suggested new Swedish e-ID infrastructure demands data interchange between different actors (e.g. e-ID providers, e-service providers, attribute issuers, registrar). Data interchange is complex and a multi actor arrangement is also complex (cf. Jaeger and Thompson, 2003; Rose and Grant, 2010) from an information and data management perspective.

IT – the technological conditions for the program are based on different existing e-ID artefacts on the market (installed base; the widespread BankID solution from e.g. Swedish banks with many users) as well as a technological base structure provided by the e-ID Board. In the studied case there is also a situation where the infrastructure and applications (e-ID solutions) are conceptually designed in parallel – resulting in an untested, conceptual and therefore abstract, e-ID infrastructure. One must also consider that there is no detailed IT artefact designed at this stage – this is also a possible risk (e.g. unprecedented technological constraints) and multiple standards and regulations coexist. Several issues, considered as challenges by Gil-García and Pardo (2005), are thus present in the implementation that we study; technological incompatibility and complexity and, to some extent, innovation.

Organizational and managerial – the role of the e-Gov Delegation, and the e-ID Board, is perceived as unclear by actors from the different government agencies and commercial actors on the market. This is

a major challenge based on the need for strong and active program leadership that is placed at the top of the list of CSF's by Rose and Grant (2010). The size and scope of the e-ID development program is also perceived as unclear, so is the ownership of the program (Sarantis et al., 2011). Taking into account the limited resources and the time pressure described above, this can definitely be perceived as a high risk program. This interpretation is also in line with e.g. Kubicek and Hagen's (2000) reasoning. Due to the numerous internal and external stakeholder groups, with different agendas, the issue of defining the national e-ID program goals, scope and outcome is cumbersome. Dawes and Pardo (2002) also address the existence of multiple, and partially conflicting goals in the public sector, which is critical for e-government initiatives. Based on the analysis and findings in the present case above, e-ID development is no exception. Adding a complex infrastructure with relationships between technology, law and business model makes it even harder to communicate with different stakeholder groups. The latter aspect is highlighted in literature reviews as a major issue to succeed in (Rose and Grant, 2010; Schierholz, et al., 2007). If we look at the total scope of the program and the embedded projects, technical, legal and regulatory issues are placed in the foreground while contextual aspects such as organizational and user/using issues are put in the background.

Rose and Grant (2010) as well as Ke and Wei (2004) propose a rather centralized approach to ensure that a program is implemented in a consistent way throughout various agencies. Consistency should also be based on a robust strategy according to Rose and Grant (2010), consisting of political and bureaucratic support and sufficient funding. As mentioned earlier the national context and history for the e-IDs has to be considered here. Sweden has a governance model with strong, rather independent, public agencies and relatively weak Ministries (Grönlund, 2010; SNAO, 2009). However, as reported above, the Cabinet is more in control, since 2009 and the creation of the e-Gov Delegation is a step towards a more centralized development of a national e-ID infrastructure. This includes standardization, usability, privacy, and costs focus. When the Swedish e-ID Board was created in 2011, with a mandate to centrally manage and develop sustainable e-ID solutions, this was a step towards a more centralized approach, in line with consistency proposed by Rose and Grant (2010) and Ke and Wei (2004).

Legal and regulatory – this category represents the formal rules that government organizations operate upon. Restrictive laws and regulations must be taken into account when developing e-government in general (Gil-García and Pardo, 2005) and secure e-IDs in particular. If we take a look at the studied e-ID initiative changes in law and regulation are needed to implement and use the suggested e-ID infrastructure in practice. A public sector procurement model needs to be more flexible and allow parallel agreements with several providers (multiple sourcing); described as a system of choice.

Institutional and environmental – challenges in the institutional framework in which governments operate (Gil-García and Pardo, 2005) and the policy environment are included here. Norms and actions are also examples of the policy environment which is important for the success or failure of e-government development initiatives. As reported above, the Cabinet are more in control now. This is obviously a step towards a more centralized and consistent e-ID infrastructure (Rose and Grant; 2010; Ke and Wei, 2004) and a changed set of norms compared with the previous more decentralized national approach. This is in that sense challenging the existing norms and power structures (i.e. the independent authorities). Another aspect taking the environmental issues into account is the business model of the Swedish e-ID's intention to create an e-ID federation structure that works effectively with benefits and incentives for different operators. It is also highlighted that the structure for the future e-ID provision should be evolutionary and adaptable to new conditions (SOU 2010:104). However, a balance between robustness and flexibility is hard to achieve in practice implementing e-ID solutions since the solution itself adds complexity to several levels such as the technical and regulative ones.

If we analyse the e-ID initiative from a program perspective (Rose and Grant, 2010) we can see that several aspects highlighted by Gil-García and Pardo (2005) above are overlapping. The contribution of management to the overall success of a program is one aspect; a strong and active leadership, change management, a contextual view of technology, laws and regulations are other important aspects.

5.3 Findings

As reported above several challenges are present. The development and implementation initiative is oriented towards pragmatic problem solving (an outdated procurement model that needs to be replaced) and an explicit demand from public agencies (secure e-ID solutions for e-services). However, the problem solving and implementation process is forced in time and has scarce available resources as illustrated by the fact that the e-ID Board has postponed the launch date for the new e-ID solution on several occasions. The fact that the program scope is unclear, and even too broad (i.e. public sector wide coordination and development in parallel), and that the relation to the existing and dominating e-ID solution in Sweden (BankID) is unclear and hard to coordinate (i.e. bilateral business driven agreements) from a governmental perspective puts further pressure on the national e-ID program.

Based on the three types of path dependencies identified by Kubicek and Noack (2010a), technological, organisational, and regulatory, we identify that the federated e-ID solution proposed by the e-ID Board challenge the dominating installed used base of BankIDs in Sweden (the technical dimension of the path). It is therefore hard to shape the new situation and context (Ayres, 1994) of the implementation of another e-ID solution in the national setting from an organizational path point of view. Pressure is also present from influential actors on the market questioning the initiative. This is an example of what Page (2006) labels as a dimension (among three other related causes) in path dependency. The self-reinforcement in this case is the set of forces or complementary institutions that the influential actors (the major government agencies in Sweden) are entirely dependent on the choice of BankID for their secure e-services to be sustained.

Above, the national e-ID initiative is also analysed as a program and from a challenge and CSF perspective. Important findings based on this analysis is that there is a significant challenge in the designing of the infrastructure for e-ID (conceptually and applying it in parallel) and at the same time taking existing e-ID solutions into account. Even if there is a more robust strategy (cf. Rose and Grant, 2010) as a baseline now, there are significant challenges related to organization and management of the program (scope, ownership, time, resources, governance structure, and design issues on a conceptual level). The involved actors are also heterogeneous and with different sets of needs and expectations ranging from leading agencies to less IT and e-ID experienced municipalities; and even agencies that propose that the historical and established solution is the most appropriate one (BankID) as a part of a self-reinforcement cause in path dependency (Page, 2006). This is a major challenge based on this dimension, but also the fact that this can be considered as a lock-in cause in path dependency (Page, 2006). The use of a certain e-ID solution (BankID) can therefore be interpreted as a choice that becomes “better” than an alternative solution (the new e-ID) because a sufficient number of people (in governmental organization providing public e-services using BankID; and end-users [citizens and bank customers] using the BankID solution) already have made that particular choice. The critique against the program putting the technological preconditions i.e. the new infrastructure, in foreground, and the user setting (e.g. citizens and professional users) together with the link to e-services provided in the background, are other major challenges for the program. When the e-services are put in the background we argue that the contextual dimension of the program is downplayed. The need to integrate the context in order to successfully implement IS and IT is well known and reported in literature from a socio-technical point of and later on in terms of contextual IS development, implementation and use and the focus on sociomaterial practices (Orlikowski, 2007; Leonardi and Barley, 2008). Acknowledging a contextual perspective is also a part of the path dependencies illustrated above. Applying a contextual perspective from the general IS domain on e-ID development can help us identify and to handle shortcomings and challenges that are present and a result from a more limited view of e-ID development and management. Our study is therefore also an example of how to apply a set of socio-material aspects when analyzing e-ID development and implementation, acknowledging a contextual perspective *and* material dimensions of e-IDs.

The e-ID development program in Sweden is facing some of the challenges reported in Denmark and Finland (Hoff and Hoff, 2010; Rissanen, 2010) concerning e.g. privacy concerns, a lack of inter-governmental and public-private coordination. This is important to learn from for both practice and research. Despite the more centralized approach, within the Swedish model of governance nowadays and the creation of the e-Gov Delegation and the e-ID Board, inter-governmental coordination is still a major challenge (challenging the decentralized governance structure in Sweden). This is another example of path dependency (Kubicek and Noack, 2010a; Page, 2006; Peters et al., 2002), and the organizational and regulatory dimension of it. Therefore an important finding is that the centralized approach suggested by Rose and Grant (2010) can be questioned; at least it is no silver bullet in managing successful e-ID development. Peters et al. (2002) claim that an IT-champion in the organization is very powerful. A critical question that we ask us based on this study: is the e-ID Board the (new) champion of the national e-ID development in Sweden? That is an open question, but so far they have not gained that status and trust in the development of a national e-ID. Looking at the market position and the installed base the Bank-ID solution and the joint business behind that e-ID solution is the champion shaping the market and an important actor in the paths outlined above. Therefore it is important to critically examine success stories of e-ID implementation (such as the one in Estonia, reported above). The relation to the widespread existing solution for e-banking (issued by the banks), the installed base, is also a challenge. Coordinating an area that is partially market driven, a sort of public-private partnership, is highlighted by the eID Board as a major challenge. However, this partnership is depending of both parties still supporting the e-ID program. 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 due to development costs and a potentially less profitable business model. This is an issue challenging the CSF literature within e-government (Rose and Grant, 2010; Ke and Wei, 2004). We have also identified that the management of e-ID development shares the challenges and possibilities in relation to e-government management in general (cf. Irani et al, 2007).

Further, another specific challenge that must be taken into account is the relationship formed between (a) the end user (citizen), (b) the market actor (the bank as e-ID provider) and (c) the public sector (the public agency as e-service provider). If something happens to the relationship between (a) and (b), it will most definitely affect the relationship between (a) and (c). Hence, the market actor has the ability to enable, control and possibly restrict the citizen's access to public e-services. Further, in the current e-ID solution, agreements are made between the e-service provider and the bank, but in the future e-ID solution, the e-ID board will act as the central contracting party for the entire and diverse public sector (cf. the scope discussed above). Though, the aim has been to simplify and centralize this process, we raise the concern that this possible single point of success can turn out to be a single point of failure. From a historical and more longitudinal point of view, the relations between the banks and the leading agencies have been constructive, fruitful and built on mutual trust, but what will happen when the e-ID Board will have the explicit role of trying to negotiate with the actors on the market? From what we have learned, there has not been any open dialogue between these parties yet, and the eID-Board has more or less taken the continued participation of the banking sector for granted. Hence, this is a central agreement and contextual aspects that we argue needs to be taken seriously in order to successfully manage e-ID development in a program.

To sum up, the findings identified in the analysis of the development, implementation and management of the national program for e-IDs in Sweden reveal several challenges related to the:

- Scope of the program and its path dependencies
- Management of the program
- Abstract system design
- Resources, legitimacy and trust in the program and the coordinating body

- Relation to the existing and dominating e-ID solution
- A multi-actor government and private setting

6 Conclusions, Discussion and Further Research

Below a concluding discussion will follow, together with theoretical and practical implications, limitations and suggested further research.

6.1 Concluding Discussion

The overall purpose of this article was to analyse and understand the contemporary management of e-ID development to: a) identify and formulate challenges, and b) reflect upon the use of a combination of perspectives in to generate this knowledge. In order to generate knowledge on this issue we have investigated e-ID development in Sweden from: a) an e-government systems development life-cycle perspective (Heeks, 2006) and b) a project challenge and critical success factor (CSF) perspective (Gil-García and Pardo, 2005) including a program perspective.

The challenges presented and analysed above has been related to different phases in a life-cycle (Section 5) and illustrates several of the challenges (and also contains several inverted CSFs) identified in the literature (Section 2 and 5). Challenges are also related to different dimensions of path dependency (technological, organisational, and regulatory) and illustrated empirically by e.g. the new e-ID solution challenging the established and wide-spread market solution (BankID) on a technical level and the problems involved in shaping a new situation and context challenged by influential actors in the market. Path dependency has informed the analysis of challenges in a novel way which, strengthen the originality of this research.

Based on this we can conclude that it is important to acknowledge and include path dependency when developing complex solutions like the one studied in this article. Our study is an illustration of how to analyse different *dimensions* of path dependency, in line with (Kubicek and Noack, 2010a), and to anchor this analysis also in general definitions and review of path dependency (in Section 2). This also opens up for a discussion on the role of an e-ID from a contextual perspective discussed below.

On a perspective and methodological level we can conclude that is a challenge to analyse initiatives on a principal and a more abstract level, compared to more mature and concrete IT artefacts. On the other hand this is also one of the challenges with the particular project above; to have a too principal and abstract design of the future e-IDs. Our study has shown that a combination of theoretical elements along a development life-cycle (including path dependency), and challenge perspective can be informative to view understand and analyse like the management of e-ID.

6.2 Implications

The conclusions above can be discussed in terms of the uniqueness of e-ID as an artefact in e-government of ISD. What is so special with e-ID – is this not like any implementation of e-government or even IS in general? As an implication for both research and practice, we claim – based on this research – that some characteristics of e-IDs need to be taken into account: 1) The e-ID as an artefact seems to be underestimated in terms of its contextual and organizational complexity. This can be claimed to be the case in general IS implementation and research (in e.g. normative IS development process models, elaborated on and criticized by e.g. Lyytinen and Newman, 2008), but the role of the e-ID as a pre-supposed delimited back office standardized technical artefact provided by external providers can support this underestimation. 2) The role of the e-ID as a prerequisite for the use of secure e-services, and 3) the national program dimension and range of the artefact and the search for standardization. These three aspects are not unique respectively, but we claim that the combination of these is characteristic for this field and important to learn from in further research and practice.

As an important implication of this research we would like to broaden the scope based on the analysis above; in digitizing Europe for example, an e-ID is regarded as an important back office enabler for launching e-services and transforming government (European Commission, 2010). Yes, e-IDs can be considered as a back office enabler for launching e-services, but it also needs to be viewed and managed as an *integral part of e-service development* because it is intertwined with the *use of e-services* from a user perspective. Thus, an e-ID is more than a back office enabler – it is an integrated part of successful e-service development, management and use. This is illustrated in Figure 2.

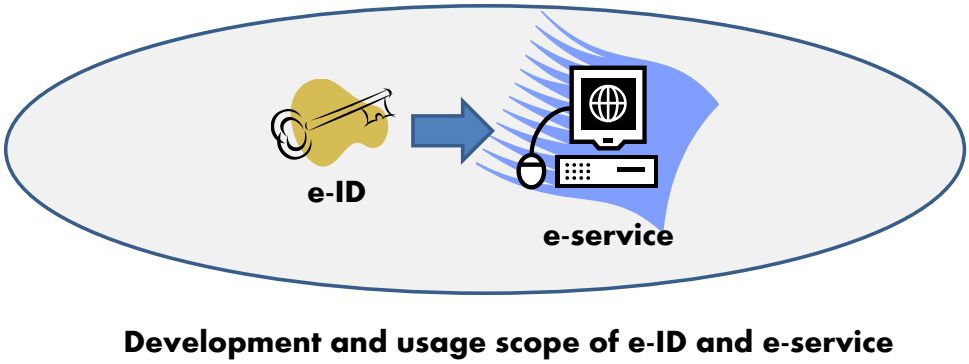

Figure 2 An e-ID as an integrated part of e-service use and development

This perspective is an attempt to avoid optimization of e.g. the e-ID as a solution as such, at the expense of the e-service focus in a usage situation or vice versa (the optimization of the e-service at the expense of the e-ID). A narrow focus on one of the objects (the e-ID artefact or the e-service) can lead to non-use or usage levels that are not satisfactory in realizing benefits of e-government projects or programs, e.g. internal efficiency and/or citizens' use of e-services for availability and transparency; cf. Collings (2008). This aspect, together with the insights related to challenges and success factors provide implications for future practice of e-ID in particular and artefact development in general. The conclusion above and illustrated in Figure 2 calls for future studies moving away from only focusing the e-ID as a technical artefact (Halperin and Backhouse, 2008; Otjacques, 2007), and instead opening up the setting and context for the e-ID artefact in order to deal with implementation issues, governance structures, multifaceted user and organizational settings and challenges, and life-cycle related issues described above. Further, we argue that this expanded contextual view of the e-ID will most likely become even more important as a prerequisite for understanding the upcoming challenges related to cross-border e-ID interoperability as described by the eIDAS regulatory environment which is currently in force (European Commission, 2015b, 2015c).

Even if we elaborate on the need to have an integrated perspective on e-ID and e-service development and use, there are situations when there is a need to focus the two artefacts respectively. When support is needed (e.g. problems with certificates etc.) it is a need to focus the e-ID, or when an e-service provides wrong data or representation of functions it is a need to focus that as an isolated object. This line of reasoning is synonymous with the general agreement that IT artefacts and organizations both arise at the intersection of social and material phenomena (Leonardi and Barley, 2008). In our study of e-IDs we therefore acknowledge the materiality's relevance (ibid.), and in parallel acknowledge and explore the interplay between materiality and agency across development (on a program and project level), implementation and use in contexts. This represents an example of an ensemble view of technology (cf. Orlikowski and Iacono, 2001) taking the dynamic interplay between people and technology into account. Previous studies analysing and discussing e-IDs from this perspective have not been identified; so this is another contribution and implication for further research from this article.

6.3 Limitations and Further Research

The present study is also an attempt to learn from e-ID development initiatives. We regard that this is essential also for future e-government development (cf. Irani et al., 2007) in general. One limitation is that we focus our study of the management of e-ID development in one national context; Sweden. Management of e-government and e-ID development have national specificities, but also general characteristics. We would also like to address the need for future contextual studies of e-ID in order to generate more knowledge on the issue of e.g. national differences, governance structures, IT and e-ID user maturity and diffusion. Further research can also address the paradoxical situation that e-IDs can contribute to security and at the same time may become a threat to privacy (Kubicek, 2010; Halperin and Backhouse 2008); this issue is not addressed in this article, but an important aspect in future research. A way of taking a contextual perspective one step further, than the limited frameworks explored in this article, is to explicitly use a framework taking process, structure and actors (e.g. viewing e-ID as a technological actor) into account. This can be achieved by using Actor-Network Theory (Callon, 1986; Latour, 1992) or Structuration Theory (Giddens, 1984).

Acknowledgement

The study is part of a larger project (Future safe electronic identification) focusing e-ID in a public e-service setting (2011-2014), financed by the Swedish Civil Contingencies in Sweden. Agency

References

24-timmarsdelegationen (2005). E-legitimation för säkra e-tjänster - Lägesrapport från 24-timmarsdelegationen. 24-timmarsdelegationen. Stockholm. [In Swedish]

Avison, D.E., Fitzgerald, G. (2003). Information Systems Development: Methodologies, Techniques and Tools, 3rd Edition, McGraw-Hill, London.

Ayres, R. U. (1994). Information, entropy and progress, American Institute of Physics, New York.

BankID (2015). Statistik BankID - användning och innehav. Retrieved Aug 10, 2015, from https://www.bankid.com/assets/bankid/stats/2015/statistik-2015-07.pdf. [In Swedish]

Barnard-Wills, D., Ashenden, D. (2010). Public sector engagement with online identity management, Identity in the Information Society, 3(3), 657-674.

Beynon-Davies, P. (2011). The Enactment of Personal Identity, In: Tuunainen, V., Nandhakumar, J., Rossi, M., Soliman, W. (Eds.). Proceedings of the 19th European Conference on Information Systems, Helsinki, Finland.

Bühler, G., et al. (2014). Security Versus Usability–User-Friendly Qualified Signatures Based on German ID Cards. ISSE 2014 Securing Electronic Business Processes, Springer, 94-105.

Callon, M. (1986). Some elements of a sociology of translation: Domestication of the scallops and the fishermen of St Brieuc Bay, In: Law, J. (Ed.), Power, action, and belief, 196-233, Routledge & Keegan Paul, London.

Christiansson, M-T, Axelsson, K., Melin, U. (2015). Inter-organizational Public E-service Development: Emerging Lessons from an Inside-Out Perspective, In: Tambouris, E. et al. (Eds.), 14th IFIP Electronic Government, EGOV 2015, LNCS 9248, 183-196.

Collings, T. (2008). Some thoughts on the underlying logic and process underpinning Electronic Identity (e-ID), Information Security Technical Report, 13, 61-70.

Cuijpers, C. and Schroers, J. (2014). eIDAS as guideline for the development of a pan European eID framework in FutureID, Open Identity Summit 2014, 237, 23-38.

Dawes, S.S., Pardo, T.A. (2002). Advances in digital government, Springer U.S., New York, 259-273.

David, P. (1985). Clio and the Economics of QWERTY, American Economic Review, 75(2), Papers and Proceedings of the 97th Annual Meeting of the American Economic Association, 332-337.

Dumortier, J. and Vandezande, N. (2012). Critical Observations on the Proposed Regulation for Electronic Identification and Trust Services for Electronic Transactions in the Internal Market, ICRI Research Paper 9, Leuven, Belgium.
E-Nämnden (2004). Grundläggande vägledning för myndigheternas användning av e-legitimationer och elektroniska underskrifter, E-Nämnden. [In Swedish]
E-Nämnden (2005). Vägledning för myndighetsföreskrifter vid införande av e-tjänster, E-Nämnden. Stockholm. [In Swedish]
European Commission (2010). Digitizing Public Services in Europe: Putting ambition into action, 9th Benchmark Measurement, Dec 2010, Directorate General for Information Society and Media.
European Commission (2015a). COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS - A Digital Single Market Strategy for Europe. European Commission. Brussels.
European Commission (2015b). Trust Services and eID, Retrieved Aug 10, 2015, from http://ec.europa.eu/digital-agenda/en/trust-services-and-eid.
European Commission (2015c). Electronic identification and trust services (eIDAS): regulatory environment and beyond, Retrieved Aug 10, 2015, from https://ec.europa.eu/dgs/connect/en/content/electronic-identification-and-trust-services-eidas-regulatory-environment-and-beyond.
Gant, J. P., Gant, D. B. (2002). Web portal functionality and state government eservice, Proceedings of the 35th Annual Hawaii International Conference on System Sciences, IEEE, 1627-1636.
Giddens, A. (1984). The constitution of society: outline of the theory of structuration, Polity Press., Cambridge, MA.
Gil-García, J.R., Pardo, T.A. (2005). E-government success factors: Mapping practical tools to theoretical foundations, Government Information Quarterly, 22(2), 187-216.
Good Practice Case (2006). eID in Estonia, eGovernment Unit DG Information Society and Media, European Commission.
http://www.ifib.de/publikationsdateien/Interoperability_in_eID_in_Estonia.pdf
Grönlund, Å. (2010). Electronic identity management in Sweden: governance of a market approach, Identity in the Information Society, 3(1), 195-211.
Halperin, R., Backhouse, J. (2008). A roadmap for research on identity in the information society, Identity in the Information Society, 1(1), 71-87.
Heeks, R. (2006). Implementing and Managing eGovernment – An international text, SAGE, London.
Heeks, R., Stanforth, C. (2007). Understanding e-Government project trajectories from an actor-network perspective, European Journal of Information Systems, 16(2), 165-177.
Ho, J., Pardo, T.A. (2004). Toward the Success of eGovernment Initiatives: Mapping Known Success Factors to the Design of Practical Tools, In: Proceedings of the 37th Hawaii International Conference on Systems Sciences, IEEE, 1-6.
Hoff, J.V., Hoff, F.V. (2010): The Danish e-ID case: twenty years of delay, Identity in the Information Society, 3(1), 155-174.
Irani, Z., Love, P.E.D., Jones, S., Themistocleous, M. (2005). Evaluating e-Government: learning from the experiences of two UK local authorities, Information Systems Journal, 15(1), 61-82.
Irani, Z., Love, P.E.D., Montazemi, A.R. (2007). e-Government: past, present and future, European Journal of Information Systems, 16(2), 103-105.
Jaeger, P.T. (2003). The endless wire: E-Government as a global phenomenon, Government Information Quarterly, 20(4), 323-331.
Jaeger, P.T., Thompson, K.M. (2003). E-Government around the world: Lessons, challenges, and future directions, Government Information Quarterly, 20(4), 389-394.
Jiang, J., Klein, G. (2000). Software development risks to project effectiveness, Journal of Systems and Software, 52(1), 3-10.
Jøsang, A. (2013). "dentity management and trusted interaction in Internet and mobile computing, IET Information Security 8(2), 67-79.

Ke, W. Wei, K.K. (2004). Successful E-Government in Singapore, Communications of the ACM, 47(6), 95-99.
Kotlarsky, J., Oshri, I. (2005). Social ties, knowledge sharing and successful collaboration in globally distributed system development projects, European Journal of Information Systems, 14(1), 37-48.
Kubicek, H., Hagen, M. (2000). One Stop Government in Europe: An Overview. In: Hagen, M., Kubicek, H. (Eds. 2000). One Stop Government in Europe, University of Bremen, 1- 36.
Kubicek, H. (2010). Introduction: conceptual framework and research design for a comparative analysis of national e-ID Management Systems in selected European countries", Identity in the Information Society, 3(1), 5-26.
Kubicek, H., Noack, T. (2010a). Different countries-different paths extended comparison of the introduction of e-IDs in 11 European countries, Identity in the Information Society, 3(1), 235-245.
Kubicek, H., Noack, T. (2010b). The path dependency of national electronic identities - A comparison of innovation processes in four European countries, Identity in the Information Society, 3(1), 111-153.
Langley, A. (1999). Strategies for Theorizing from Process Data, Academy of Management Review, 24(4), 691-710.
Latour, B. (1992). Where are the missing masses? The sociology of a few mundane artifacts, In: Bijker, W., Law, J. (Eds.), Shaping technology/Building society: Studies in socio-technical change, 225-258, MIT Press, Cambridge, MA.
Leonardi, P., Barley, S.R. (2008). Materiality and change: Challenges to building better theory about theory and organizing. Information and Organization, 18, 159-176.
Liginlal, D., et al. (2012). Tracking the Sociotechnical Barriers to Digital Identity Adoption in Arab Countries–A Case Study of Qatar, 9th International Conference on E-Governance (ICEG-2012), Cochin, Kerala, India
Lyon, D. (2009). Identifying citizens: ID cards as surveillance, Polity Press, Cambridge, UK.
Lyytinen, K., Newman, M. (2008). Explaining information systems change: a punctuated socio-technical change model, European Journal of Information Systems, 17(6), 589-613.
Melin, U., Axelsson, K. (2009). Managing e-service Development – Comparing two e-Government Case Studies, Transforming Government - People, Process and Policy, 3(3), 248-270.
Mintzberg, H. (1989). Mintzberg on management, The Free Press, New York.
Modinis Study (2005) On Identity Management in eGovernment. Common terminological framework for interoperable electronic identity management, E.C./University of Leuven.
Orlikowski, W.J. (2007), Sociomaterial Practices: Exploring Technology at Work, Organizational Studies, 28(9), 1435-1448.
Orlikowski, W.J. Iacono, S. (2001). Research Commentary: Desperately Seeking the "IT" in IT Research - A Call to Theorizing the IT Artifact. Information Systems Research, 12(2), 121-134.
Otjacques, B., Hitzelberger, P., Feltz, F. (2007). Interoperability of E-Government Information Systems: Issues of Identification and Data Sharing, Journal of Management Information Systems, 23(4), 29-51.
Page, S. E. (2006). Essay: Path Dependence, Quarterly Journal of Political Science, 1(1), 87-115.
Patton, M.Q. (1980). Qualitative evaluation methods, Sage Publications, Beverly Hills.
Peters, S.C.A, Heng, M.S.H, Vet, R. (2002). Formation of the information systems strategy: in a global financial services company, Information and Organization, 12(1), 19-38.
Price, G. (2008). The benefits and drawbacks of using electronic identities, Information Security Technical Report, 13, 95-103.
Rissanen, T. (2010). Electronic identity in Finland: ID cards vs. bank IDs", Identity in the Information Society, 3(1), 175-194.
Rosacker, K.M., Olson, D.L. (2008). Public sector information system critical success factors, Transforming Government: People, Process and Policy, 2(1), 60-70.
Rose, W.R., Grant, G.G. (2010). Critical issues pertaining to the planning and implementation of E-Government initiatives, Government Information Quarterly, 27(1), 26-33.
RSV (2003). SAMSET - dagsläget sommaren 2003. Stockholm, Riksskatteverket.

Rössler, T. (2008). Giving an interoperable e-ID solution: Using foreign e-IDs in Austrian e-Government - Interoperability in electronic identity management, Computer Law & Security Report, 24(5), 447-453.
SNAO (2009). E-legitimation – en underutnyttjad resurs, Riksrevisionen (The Swedish National Audit Office) Rapport RiR 2009:19, November 23, 2009 [In Swedish].
Sarantis, D., Charalabidis, Y., Askounis, D. (2011). A goal-driven management framework for electronic government transformation projects implementation, Government Information Quarterly, 28(1), 117-128.
Schierholz, R., Kolbe, L. M., Brenner, W. (2007). Mobilizing customer relationship management: A journey from strategy to system design, Business Process Management Journal, 13(6), 830-852.
Seltsikas, P., O'Keefe, R.M. (2010). Expectations and outcomes in electronic identity management: The role of trust and public value, European Journal of Information Systems, 19(1), 93-103.
Shukri, M. and M. Hafiz (2015). The Privacy and Security of An Identification Card: Malaysian Perspective, MPRA Paper No. 65855, posted 30. July 2015
SOU 2009:86 (2009). Strategi för myndigheternas arbete med e-förvaltning, Betänkande, E-delegationen, Stockholm [In Swedish].
SOU 2010:62 (2010). Så enkelt som möjligt för så många som möjligt - Under konstruktion - framtidens e-förvaltning, Betänkande, SOU 2010:62, E-delegationen, Stockholm. [In Swedish]
SOU 2010:104 (2010). E-legitimationsnämnden och Svensk e-legitimation, Betänkande av Utredningen om bildandet av en e-legitimationsnämnd, Stockholm. [In Swedish]
Sullivan, C. and S. Stalla-Bourdillon (2015). Digital identity and French personality rights–A way forward in recognising and protecting an individual's rights in his/her digital identity, Computer Law & Security Review, 31(2), 268-279.
Söderström, F., Melin, U. (2012). The Emergence of a National e-ID Solution – an Actor-Network Perspective, Presented at the 35th Information Systems Research Seminar in Scandinavia, Sigtuna.
Reel, J.S. (1999). Factors in Software Projects, IEEE Software May/June, 18-23.
Tsai, N., Choi, B., Perry, M. (2009). Improving the process of E-Government initiative: An in-depth case study of web-based GIS implementation, Government Information Quarterly, 26(2), 368-376.
Van de Ven, A.H. (2007). Engaged scholarship – A guide for organizational and social research, Oxford University Press.
VERVAR 2008:12a (2008). Slutrapport om säkert elektroniskt informationsutbyte och säker hantering av elektroniska handlingar, Verket för förvaltningsutveckling, Stockholm. [In Swedish]
VERVAR 2008:12b (2008). Elektronisk identifiering och underskrift i Sverige, Särtryck ur 2008:12, Verket för förvaltningsutveckling, Stockholm. [In Swedish]
Walsham, G. (1995). Interpretative case in IS research: nature and method, European Journal of Information Systems, 4(2), 74-81.
Whitley, E.A., Hosein, I. R. (2007). Policy Engagement as Rigourous and Relevant Information Systems Research: The Case of the LSE Identity Project, In Proceedings of the 15th European Conference on Information Systems (Österle, H., Schelp, J., Winter, R. Eds.), 1301-1312.
Yildiz, M. (2007). E-government research: Reviewing the literature, limitations and ways forward. Government Information Quarterly, 24(3), 646-665.
Zissis, D., Lekkas, D. (2011). Securing e-Government and e-Voting with an open cloud computing architecture, Government Information Quarterly, 28(2), 239-251.