

Different countries-different paths extended comparison of the introduction of eIDs in eight European countries

Herbert Kubicek · Torsten Noack

Received: 25 March 2010 / Accepted: 5 May 2010

© The Author(s) 2010. This article is published with open access at Springerlink.com

Abstract A first comparison of the innovation processes of introducing electronic identities on a national level in Austria, Belgium, Germany and Spain, based on extensive expert interviews with key actors, has been amended by four more country reports from Denmark, Finland, Estonia and Sweden in order to check the validity of generalisations derived from the first four cases. The extended comparison with the four additional countries increases the variance between the eID systems in Europe by showing differing technical and organisational features, such as purely software-based solutions, e.g. in Denmark, or complete outsourcing of the eIDMs, e.g. in Sweden. In the second part of the paper, the conceptual framework of the comparative study, a combination of path analysis, institutional actor theory and policy field analysis will be reflected. It has resulted in a fruitful approach allowing for the explanation of some, but by no means all, of the differences between the national eIDMs in Europe.

Keywords Comparative analysis · eID cards · Electronic identities · Identity management systems · Identity cards · Path analysis · Privacy · Staatsverständnis

Background and objectives

Four empirical case studies of the introduction of electronic identities (eIDs) at the national level in Austria, Belgium, Germany and Spain have been conducted according to a common research design and been compared following a common conceptual framework (Kubicek and Noack 2010). This framework combines the actor-oriented institutional theory and policy field analysis with path analysis

The paper is based on research funded by the independent Volkswagen Foundation, Germany.

H. Kubicek (✉) · T. Noack

Institut für Informationsmanagement Bremen GmbH (ifib), Am Fallturm 1, 28359 Bremen, Germany

e-mail: kubicek@ifib.de

URL: <http://www.ifib.de>

URL: <http://www.agim.informatik.uni-bremen.de>

(Kubicek 2010). The empirical research has been conducted by teams in each country by interviews of key actors according to a common interview guide. The countries for comparison have been selected on the principle of a most similar design (Kubicek 2010). They all have introduced a new eID for online authentication for e-government services based on a national ID card or a similar chip-card. The eID is defined as registered in national citizen registries based on particular legislation and produced and distributed within an eID Management System (eIDMS) operated by different agencies.

The findings for the studies in Austria (Aichholzer and Strauß 2010), Belgium (Mariën and van Audenhove 2010), Germany (Noack and Kubicek 2010) and Spain (Heichlinger and Gallego 2010) have been compared with regard to socio-technical system features, i.e. the eIDMS, their technical, organisational and regulatory path dependency, the main actors who have made these choices, the context in which these decisions have been taken, in particular privacy legislation and culture as well as “Staatsverständnis” and finally the use of the eID function for e-government services. There are big differences between the four countries and between their national eIDMS, which can be explained by differences between the earlier systems. In other words, there is a high degree of path continuation or incremental innovation. Path change or path creation could be observed in some countries where attempts were made to react on privacy concerns which occurred to a different degree in the four countries under comparison.

Despite the big differences between the four eIDMS, the rate of usage for online authentication in e-government services is quite low in each case. This raises the question whether the eIDMS, which has been introduced, was an appropriate and effective solution to the policy problem started with. The official policy problems to be solved were security and privacy concerns of citizens which keep them from performing online transactions in e-government and e-commerce and thereby not fully exploiting the potential of the Internet for economic growth and societal progress. Looking at the functionality of the eIDMS, it becomes obvious that they increase the security of service providers concerning the identity of their customers but except for the German case do not increase the safety of the citizens/customers with regard to the identity or the fulfilment of the providers of online services. As long as other methods of online authentication, in particular user name, password and/or one-time passwords are offered, there is no advantage for citizens to use the eID for online authentication regardless of whether it is considered by security experts as a stronger and more secure alternative compared to the existing methods (Kubicek and Noack 2010).

As this is an important finding with far-reaching economic and political implications, it is important to check its generalisability. Therefore another four country reports have been ordered selected according to the principle of a “most different design”, including countries such as Denmark, which has been planning to introduce an eID card for more than 20 years (Hoff and Hoff 2010), or Sweden, which has completely outsourced its eIDMS (Grönlund 2010). We also included Finland, the first country to introduce an eID (Rissanen 2010) and Estonia, said to be most successful with regard to usage rates of eID based online authentication for e-government services (Martens 2010). Indeed the four country reports written by experts well acquainted with the situation in their home country show relevant

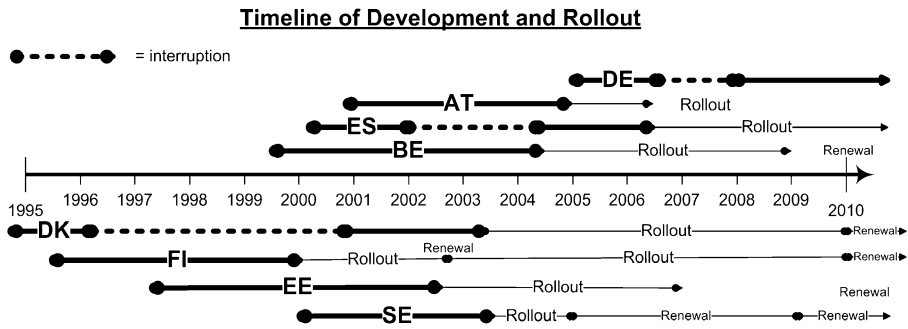


Fig. 1 Timeline of development and rollout of eIDs in eight countries

additional variations of the eIDMS with regard to technology, organisation and regulation. However, it has to be noted that all eight countries have one thing in common: The eID is based on an official identity registered in an obligatory national citizen registry and these cases therefore are completely different from e.g. the United Kingdom.

In three of the four countries the innovation process started much earlier, i.e. in 1994 in Denmark, in 1995 in Finland, in 1997 in Estonia (see Fig. 1)

Broadening the range of eIDMS

The only common feature of the national eIDs in the eight countries is their origination from the national citizen registries, based on an obligation to register for every citizen by birth (Table 1).

Differences between the eIDMS

While in the first sample in three out of four cases the new national ID chip-card was chosen as the only token for the eID, in the second sample only Finland and Estonia started with this option. However, Finland, where the ID card is not mandatory, has opened an alternative path of accepting the bank eID for e-government as well. In Denmark, there is no national ID card at all, and Sweden, comparable to Austria, offers an optional ID card, which by law can be used as token for the eID, but which is so far not being offered with this functionality.

The government-issued eIDs in Denmark and Sweden are software certificates for digital signatures, which according to the European signature legislation are considered to be less secure than those on chip-cards. In Sweden, they may be placed on chip-cards, but this option accounts for less than 10% (Grönlund 2010). The eID in the four countries in the second sample includes a unique identifier, which is the national register number in Estonia and Sweden or a number derived from this number in Denmark or from the social security number in Finland. Where chip-cards are used, they employ contact chips, and these do not contain biometric data.

Table 1 Main attributes of the eID-solutions

	BE	ES	AT	GE	DK	FI	SE	EE
	BelPIC	DNIe	Bürgerkarte	ePA	OCES	FINEID	BankID et.al	ID-card
Carrier card	1	1	> 1	1	SW certifi.	1	> 1 ^a	1
Identical with national ID card/mandatory	Yes/Yes	Yes/Yes	No	Yes/Yes	No	Yes/No	No ^b	Yes/Yes
Chip	Contact	Contact	Contact	RFID	No card	Contact	Software/contact	Contact
Card function	Authentication (online)	Yes	Yes	Opt in	No card	Yes	Depending on card	Opt out
	Yes	Yes	No	Yes	No card	Yes	Depending on card	Yes
e-signature	Opt out	Yes	Yes	Opt in	No card	Yes	Depending on card	Opt out
Source of ID data	Central register	Central register	Central register	Local register	Central register	Central register	Central register	Central register
eID attributes	eID data on chip				Certificate:		Certificate:	
· Name	Yes	Yes	No	Yes	Optional	Yes	Yes	Yes
· Address	Yes	Yes	No	Yes	Optional	No	No	No

· Date of birth	Yes	Yes	No	Yes	No	Yes	Yes	Yes
· National register number	Yes	Yes	Derived Number (SSPN)	No	Derived Number (PID)	No	Derived Number (FINUID)	Yes
Visual data:								
· Address	No	Yes	Depending on card	Yes	No card	No	Depending on card	No
· Owner's photograph	Yes	Yes	No	Yes	No card	Yes	Depending on card	Yes
Biometrics:								
· Face	No	Yes	No	Yes	No card	No	Depending on card	No
· Fingerprints	No	Yes	No	Opt in	No card	No	Depending on card	Yes
· Unprotected readable data file	Yes	No	No	No	No card	No	Depending on card	Yes
· Access certification of service provider required	No	No	Yes	Yes	No	No	No	No

^a Including one time passwords and software certificates

^b eID on eIDC technically possible, but not provided

Most remarkable are differences with regard to the organisations which issue the eIDs accepted for online authentication in e-government services: In the four countries, banks and the eIDs accepted by banks for online banking play a dominant role, but in different ways:

- In Denmark, the government-issued OCES eID will be merged with the dominant bank eID and the new Nem ID, still software-based, will be issued and administered by a bank consortium (Hoff and Hoff 2010).
- In Estonia, from the beginning, issuing of eID certificates on the national ID card has been outsourced to a consortium of the largest bank and the largest telecom enterprise (Martens 2010).
- In Finland the eID on an eID card did not receive any acceptance while the bank eID in the form of One Time Passwords (OTP) boomed. The Finnish Government therefore in 2003 opened up this path and accepts the bank eID for online authentication for e-government services (Rissanen 2010)
- In Sweden, until recently there was no government-issued eID at all, instead bank-issued eIDs based on a government contract are accepted for e-government services (Grönlund 2010).

Path continuation

Similar to the other four countries, these organisational arrangements continue previous paths and are in the regulatory tradition of the respective country—except for Estonia which has completely cut with all the traditions dating from the Soviet occupation and has created a new path with regard to citizens' registration and ID documents including eIDs (Martens 2010).

It is remarkable that neither Denmark nor Sweden changed over to the European standards of hardware-based solutions for IDs and digital signatures, but rather continued their software-based solutions. This shows a high degree of path persistence.

Sweden has a long tradition of government relying on identities provided by other organisations such as the post office. Following this tradition Sweden contracted out the administration of the eIDs to a bank consortium (Grönlund 2010). Finland and Denmark conducted a kind of path shift for pragmatic reasons when they failed with their government-issued eID and saw the strong uptake of the bank eIDs. Estonia, in creating new paths followed its Scandinavian neighbours, went for a private consortium of the largest bank and the largest telecom enterprise. As the authors of the Swedish and the Estonian case study emphasize, in their countries there is a tradition of reducing government activities to the bare minimum and to contract out many tasks that in other European countries are retained by government (Grönlund 2010, Martens 2010). At the same time there is a high trust in banks regarding data protection (see Table 2).

Policy fields and actors constellation

One core finding from the first four cases was that eIDs are a multi-field innovation, i.e. becoming subject of different policy fields, in particular public administration/e-

government, public safety, industry/e-commerce and others. While in Germany and Spain, safety and security were the most powerful policy fields leading to digital fingerprints on the eID chip, the policy fields of public safety or security played no role with regard to the eIDMS in the four northern European countries. This may be one reason why the national ID cards, if there are any, do not play an important role as the eID token and why even bank IDs are accepted for e-government services. In the Swedish case study the greatest influence is assigned to the finance/tax policy field, as the eID as well as the national registry are under the authority of the Ministry of Finance (Grönlund 2010).

With regard to the actors constellation, the most significant difference between the countries in the first and the second sample concerns the role of the banking sector and the strategy that governmental actors developed in this respect.

In Belgium, Germany and Spain governmental actors considered banks as one of many service providers who might accept the eID-based authentication for their online services in addition to their propriety and less secure methods. When the banks showed little interest this did not lead to any changes of the governmental system. In Austria government could win the banks to provide their chip cards as one of several tokens for the national eID (“Bürgerkarte”) but had not included them in the development process nor reacted to the recent fading out of this option by some banks which no longer are promoting the eID (Aichholzer and Strauß 2010). In contrast, the four countries in the second sample cooperated in different ways and relied on the banking sector: Sweden contracted the whole eIDMS out to a bank consortium, Estonia to a consortium of a bank and a telco enterprise, Denmark merged its governmental issued eID with the bank ID and hands this over to a bank consortium and Finland, besides its government-issued eID, accepted the bank eID for online authentication in e-government services. This is most remarkable as all bank issued eIDs are either employing One-Time-Passwords or software certificates, both considered to be less secure than chip card based solutions in a PKI environment.

“Staatsverständnis” and privacy

The above-mentioned strong tendency for contracting out the eIDMS and only running the central citizen registry is the result of a particular “Staatsverständnis”, which looks after cost reduction wherever possible and reduces the government’s tasks to the minimum. In Austria, Belgium, Germany or Spain, neither political parties nor the public would accept national eIDs being issued by banks or other private businesses. There is a north-south difference, calling for further explanation which, however is beyond the scope of this study.

With regard to privacy, at first glance, we expected a similar legislation and culture in Denmark and Sweden, but we found big differences with regards to the eIDMS. In Denmark, early attempts to introduce a digital citizen card failed because of privacy concerns (see Hoff and Hoff 2010) while in Sweden the government contracted the eIDMS to the private sector and did not demand any privacy enhancing provisions (see Grönlund 2010).

Most notable are differences regarding the use of the unique personal identity number which all four countries have. As this number in Denmark, and likewise the

Table 2 Privacy trust and concerns in surveys in eight countries, Eurobarometer 225 (Gallup 2008)

Country	(1) Trust in tax authorities concerning data privacy (% who trust)	(2) Average trust in governmental institutions (social, tax, local) (% who trust)	(3) Trust in banks and financial institutions concerning data privacy (% who trust)	(4) Concerns about personal data privacy by private and public organizations (% very concerned)	(5) Concerns about personal data protection on the internet (% very concerned)	(6) Level of personal data protection in the home country—properly protected (% agree)
DE	66	69	68	65	67	46
BE	76	80	74	22	72	63
AT	69	71	72	70	67	62
ES	76	80	63	35	69	48
FI	92	88	92	5	68	84
SE	91	85	84	46	73	63
DK	94	84	90	45	65	85
EE	74	65	81	20	54	48

Social Security Number in Finland, includes the date of birth and a code for the sex of the holder, its use for authentication purposes by non-governmental agencies is considered a privacy risk. Therefore both countries do not allow the direct use of the original number in the software certificate in Denmark and on the eID card in Finland, but rather produced a derived, non-speaking ID number for the eID (see Hoff and Hoff 2010 and Rissanen 2010). In Sweden and Estonia, the use of the original national number did not raise any concerns and no provisions were taken.

These differences between the eIDMS do not perfectly match with available data on general privacy governance or survey data on trust in different institutions (Table 2). Eurobarometer statistics of 2008 show that citizens in Finland, Denmark and Sweden much more frequently said that they trust their tax authorities regarding data privacy of their personal data than the Austrian, Belgian, German and Spanish citizens. The data on the average trust in different governmental institutions, including local authorities and social security (column 3), however do not show similar differences between the countries. Trust in data privacy provided by banks, again in the northern countries, is much higher. This may be one reason why the stronger involvement of banks in the northern countries did not raise any concerns.

However we cannot explain the different regulation regarding the use of the National register or Social Security Number between Denmark and Finland on the one hand and Sweden and Estonia on the other, as a reaction to stronger privacy concerns, as we did with regard to the differences between Austria and Germany *vis a vis* Belgium and Spain (see Kubicek and Noack 2010). Rather, it could be the reverse: Finnish citizens perceive a high level of personal data protection and therefore have few general concerns regarding data privacy. Danish data show a high level of data protection but also much more concerns of citizens. Estonian citizens report a lower level of protection and are more frequently concerned. In all four

countries the respective eIDMS, even where employed for several years, leave a similar degree of concerns regarding data privacy in the internet in general.

Take-up and usage

Finland shows a similarly low usage rate of the government-issued eID as Austria, Belgium and Spain (Table 3). The government-issued eID had to compete with a less secure but much more popular bank eID, which has finally been accepted for e-government services as well. Only Estonia can record a relatively high usage rate of the national chip card based eID, which is issued by a private consortium, does not have any privacy provisions but can be used for many e-government services, including electronic voting in national elections (see Martens 2010). As the usage rate in the view of the consortium is still low, and as banks are part of this consortium, only recently have they started to make the parallel existing OTP authentication for online banking less attractive.

Remarkable are the usage rates in Denmark and Sweden of the software based eIDMS, reaching 18,8% in Denmark and 24,4% in Sweden with increasing trends. This calls for reflection on the general policy approach taken and already questioned in the comparative analysis of the four countries in the first sample. Are chip card based stronger authentication methods an effective solution to safety and privacy concerns of citizens, which make them refrain from using the Internet for online transactions in e-government and e-commerce? In our first comparative analysis (Kubicek and Noack 2010) we argued that the dominant one-sided authentication methods in Austria, Belgium and Spain — Germany being the exception — may enhance the security for the service provider but not for the citizen/customer and thereby do not offer any advantage for the additional investment. Now we may add, that even where citizens accept the need for stronger authentication against their service providers they do not accept the more complex and expensive methods, which provide for the most security. Software-based authentication methods are

Table 3 Roll-out and usage of eIDs in eight countries

2009	BE BelPIC	ES DNIe	AT Bürger- karte	DK OCES	FI FINEID	SE BankID et.al.	EE ID-card
State of rollout	9,3 mill 100%	8 mill 25%	8,4 mill 100%	no card	265.000 5%	Several tokens	1,1 mill 100%
eID function activated	7,5 mill 80%	Not necessary	Approx. 74.000 0,9%	1,2 mill 21%	220300	2,5 mill 33% (92% software, 8% cards)	approx. 550.000 50%
Use rate for electronic income tax, (% of declaration)	56%	21%	25,7%	87%	No data	53%	87%
eID use rate for electronic income tax, (% of declaration)	14,2% (half by service of tax office)	0,2%	1,0%	18,8%	1% of all online authentications use eIDC	24,4%	19%

considered to be stronger than username/password based methods but less secure than chip card based methods (possession and knowledge). But this seems not to be the most important criterion for citizens. They appreciate that software certificates can be downloaded at no extra cost, do not require a card reader or driver software, and are not bound to other tokens with a different validity period and additional functions.

Reflecting the conceptual approach

For the comparative analysis of European eIDMS, a conceptual framework has been developed which combines the institutional actor theory for policy field analysis with path analysis from technology-related social science research, expecting a mutual fruitful gain of insight (Kubicek 2010). Traditional path analysis most of all claims the strong influence of history and does not look in detail at the actors taking decisions on the development. By introducing the options of path continuation, path change, path creation and path merger with regards to a technical, organisational and regulatory path, we were able to describe in a comparative way the choices political actors could take with regard to the national eIDMS and thereby fill the gap which the institutional actors theory presents, i.e. the undefined subject of the policy problem and policy solution (Scharpf 2000). Introducing path analysis into the actor-oriented institutional analysis allows concentrating on the cases of path change or path creation. In this regard the contextual approach introduced by Mayntz and Schneider (1988) becomes relevant. The assumption that privacy legislation and culture as well as “Staatsverständnis” can explain the differences between the solutions chosen could be observed but not validated by strong empirical correlation, as privacy governance or privacy culture are hard to operationalise across different European cultures.

Within this view, path changes and path creation have to be explained while path continuation is the default assumption with reference to the previous system. However, in a more comprehensive comparative analysis one would like to know the reasons for the differences between the previous systems as well, i.e. why is there an obligation to hold an ID card in some countries but not in others, why do some have a universal identity number which is openly used, while others restrict its use, and why does a third group of countries ban such a number altogether? To answer these questions, historical research is needed which goes beyond the available, more eclectic and anecdotal studies of the history of citizens registration, passports and other ID documents available so far.

Finally with regard to diffusion and usage, Rogers’ theory has proven able to explain low take-up and usage quite well (Rogers 2003). The eIDs do not provide sufficient additional value to citizens, in particular as long as other methods for authentication are offered. This competitive factor in Rogers’ theory does not play such an important role as it did in the case of online authentication. However, Porter, in his analysis of competitive strategies emphasizes substitute products as a relevant threat (Porter 1998). In this regard we note that authentication for online banking is an important influencing factor for eIDs and that in all countries under comparison banks are not ready to employ the stronger authentication offered by chip-based

eIDs. On the contrary, some governments drew back their commitment for introducing this kind of stronger authentication and accept the weaker methods of online banking. Therefore it would be an interesting question for another study not only to take a closer look at the different strategies governments deploy in respect of the banking sector but also to compare and explain the high degree of path continuation in online banking authentication.

Open Access This article is distributed under the terms of the Creative Commons Attribution Noncommercial License which permits any noncommercial use, distribution, and reproduction in any medium, provided the original author(s) and source are credited.

References

- Aichholzer G, Strauß S. The Austrian Case: Multi-card concept and the relationship between citizen ID and social security cards. *Identity in the Information Society, Special Issue*, 2010. doi:10.1007/s12394-010-0048-9
- Gallup Organisation. Data protection in the European Union. Citizen's perceptions. Analytical report, Survey conducted by the Gallup Organization Hungary upon the request of Directorate-General Justice, Freedom and Security. Flash-Eurobarometer no. 225. 2008. http://www.ec.europa.eu/public_opinion/flash/fl_225_en.pdf. Accessed 20 Jan 2010
- Grönlund Å. Electronic identity management in Sweden: governance of a market approach. *Identity in the Information Society, Special Issue*, 2010. doi:10.1007/s12394-010-0043-1
- Heichlinger A, Gallego P. A new e-ID card and online authentication in Spain. *Identity in the Information Society, Special Issue*, 2010. doi:10.1007/s12394-010-0041-3
- Hoff J, Hoff F. The Danish eID Case: twenty years of delay. *Identity in the Information Society, Special Issue*, 2010. doi:10.1007/s12394-010-0056-9.
- Kubicek H. Introduction: conceptual framework research design for a comparative analysis of national eID management systems in selected European countries. *Identity in the Information Society, Special Issue*, 2010. doi:10.1007/s12394-010-0052-0
- Kubicek H, Noack T. The path dependency of national electronic identities. A comparison of innovation processes in four European countries. *Identity in the Information Society, Special Issue*, 2010. doi:10.1007/s12394-010-0050-2
- Mariën I, Van Audenhove L. The Belgian e-ID and its complex path to implementation and innovational change. *Identity in the Information Society, Special Issue*, 2010. doi:10.1007/s12394-010-0042-2
- Martens T. Electronic identity management in Estonia between market and state governance. *Identity in the Information Society, Special Issue*, 2010. doi:10.1007/s12394-010-0044-0
- Mayntz R, Schneider V. The dynamics of system development in a comparative perspective: interactive videotex in Germany, France, Britain. In: Mayntz R, Hughes T, editors. *The development of large technical systems*. Frankfurt: Campus; 1988. p. 263–98.
- Noack T, Kubicek H. The introduction of online authentication as part of the new electronic national identity card in Germany. *Identity in the Information Society, Special Issue*, 2010. doi:10.1007/s12394-010-0051-1
- Porter M. *The competitive advantage of nations*. New York: Free Press; 1998.
- Rissanen T. Electronic identity in Finland: ID cards vs. bank IDs. *Identity in the Information Society, Special Issue*, 2010. doi:10.1007/s12394-010-0049-8
- Rogers EM. *Diffusion of innovations*. 5th ed. New York, London et al.: Free Press; 2003.
- Scharpf FW. Institutions in comparative policy research. *Comp Polit Stud*. 2000;33(67):762–90.