IDIS (2010) 3:111–153
DOI 10.1007/s12394-010-0050-2

The path dependency of national electronic identities

A comparison of innovation processes in four European countries

Herbert Kubicek · Torsten Noack

Received: 14 October 2009 / Accepted: 9 March 2010 / Published online: 10 April 2010

Abstract This paper compares the four national electronic Identity Management Systems (eIDMS), which have been described in the previous chapters. The section "Similarities and differences between four national eIDMS" will highlight the differences between these systems conceived as socio-technical systems with regard to the eID itself, the eID cards as tokens, the authentication processes as well as the procedures for distribution and personalisation, the support provided for installing the technology and any provider-related regulation. The section "A three-fold path dependency", according to the conceptual framework presented in the introductory chapter to this special issue, compares the new electronic systems with the previous ones in each country, in order to assess the continuation or changes with regard to the organisational, technological and regulatory path of development. The following sections explain the differences between the paths chosen and the path-related changes by analysing the actor constellation of the institutional actors, in particular the policy field and the power structure, as well as the context in which the policy makers made their choices, looking at privacy and "Staatsverständnis" in particular. Finally the diffusion and usage of the eID function will be compared and analysed, discussing to what extent the new institution has made a contribution to solving the policy problem it was developed for, e.g. providing a stronger authentication in order to meet security concerns regarding e-government and e-commerce transactions and avoiding new privacy infringements. Using grounded theory, the explanations provided have the status of generalisations derived from the four cases. They have to be considered as hypotheses, which will be checked for other countries in the following papers of this special issue. The comparison of the four cases in this article shows a high degree of path dependency. Most of the differences between the new systems are just a continuation of differences between the previous systems although they are to solve the same problem and can draw on the same technologies. But most

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

H. Kubicek (✉) · T. Noack
Institute for Information Management Bremen (ifib), Bremen, Germany
e-mail: kubicek@ifib.de

astonishing is the finding that these differences between the systems do not influence diffusion and use of the eID function in the respective countries.

Keywords Authentication in e-government and e-commerce · E-signatures · Diffusion of eIDs · National ID cards · Path analysis · Policy field analysis · Privacy regulation of eIDs

Similarities and differences between four national eIDMS

In the four countries under comparison, i.e. Austria, Belgium, Germany and Spain, the eID is the same national ID as collected and administered down the years in national civil registries, also called population registers. There is a legal obligation in all four countries for all newborn citizens to be registered. The registries contain data on several attributes of citizens of the respective state, including name, date of birth, sex, address, body size, etc. There are additional registries of inhabitants with other nationalities. Some countries, e.g. Belgium, have introduced special eID cards for foreigners. However, the comparison in this chapter will exclusively look at the national eIDMS for citizens who at the same time are inhabitants of the respective country and will compare smart cards as tokens, the authentication process, the infrastructure for distribution, personalisation and activation of the eIDs as well as the kind of support provided for installing the necessary technical components and any provider-related procedures in the four countries.

Chipcards as tokens

Tokens for national eIDs can either be pieces of software or hardware. The four countries under investigation have chosen *smart cards* in the standard format of bank and credit cards as hardware tokens (Fig. 1). These cards provide for *online authentication* and at least the option of *digital signatures*. Belgium, Germany and Spain have finally chosen a newly introduced *national electronic ID card*, which is used for *visual inspection* and as *European travel document* as well (see lines at the bottom of Fig. 1). Austria has created a virtual Citizen Card and adopted a *multi-card strategy*, indeed a multi-token strategy, as at least for some time the Austrian eID could have been placed on the SIM card of a mobile phone and on a USB memory stick as well. The main reason given for the multi-card approach is that in Austria, in contrast to Belgium and Spain, there is *no obligation to hold an ID card*. Rather Austrian citizens can prove their identity with an ID card ("Personalausweis"), *a passport or another official document*, e.g. a social security card or driver's license, and only 10% have chosen an ID card (see Aichholzer and Strauß 2010). German citizens are obliged by law to hold either an ID card ("Personalausweis") or a passport. German government has chosen the new electronic ID card as the token for the eID, as more than 90% of German citizens entitled hold an ID card and are expected to renew it (see Noack and Kubicek 2010).

Figure 1 shows the front of the four eID cards. Although the *Austrian law* on eIDs mentions the national ID card as a possible token, this option so far has not

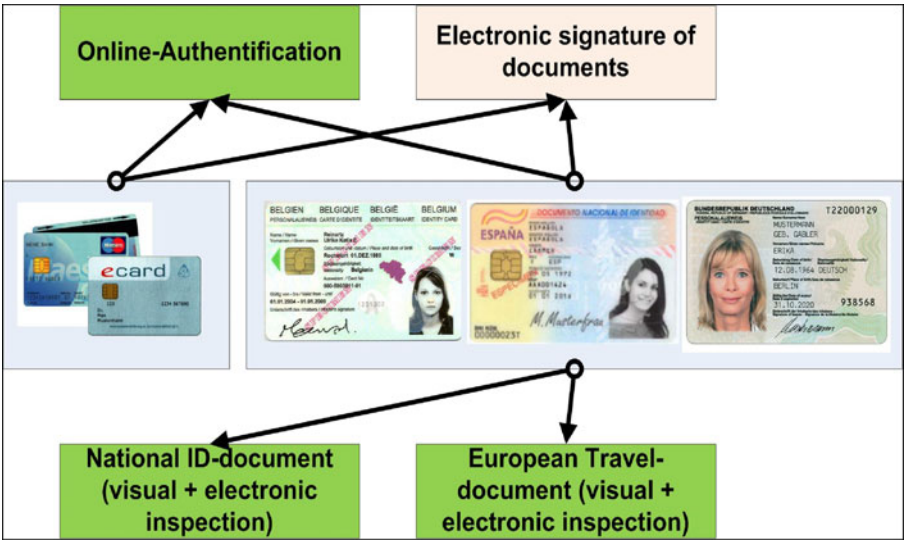

Fig. 1 Tokens for eIDs in Austria, Belgium, Spain and Germany (from left to right)

been realized. Rather the two smart cards used as tokens are the social security card (e-card) and bank cards of several Austrian banks. Neither carries a *photo* of the holder.

There are also differences regarding the *data printed* on the front and the rear of the card. While the Spanish and German cards show the address of the holder, the Belgian card does not. The address is only stored on the chip, so that the card does not have to be exchanged when the owner relocates.

In technical terms, the German smart card differs from the other ones by the *kind of chip* chosen. While the Austrian, Belgian and Spanish cards use a contact chip, the German card uses a *contactless RFID chip*.

Table 1 lists the main differences between the four eID cards.

The authentication process

Authentication in the context of eIDs has been defined as "the corroboration of the claimed identity of an entity and a set of its observed attributes". This corroboration happens in a defined authentication process, which requires possession of the card as well as knowledge of a PIN code in order to provide for *strong authentication*, which is more secure than the weaker authentication via username and password. The Belgian and the Spanish authentication processes are rather straightforward: if an online service requires authentication, the citizen puts his eID card into his card reader and enters his PIN. This starts a dialogue between card reader and client software on the user´s side with the middleware of the service provider, which finally corroborates the citizen´s eID via a certificate on the eID card. We called this a *one-sided authentication* as the service provider checks the identity of the citizen/customer, but the citizen/customer cannot corroborate the identity of the service provider beyond the SSL connection established.

Table 1 Differences between eIDs and eID Cards

		BE	ES	AT	GE
Carrier card	Identical with national ID card	Yes	Yes	No	Yes
Chip	Contact/contactless chip	Contact	Contact	Contact	RFID
Obligations	Obligatory starting from age of cardholder	Yes, >12	Yes, >14	e-Card yes >0	Yes, >16
Validity	Validity of eID (years)	5	5 or 10	Depending on card	6 or 10
Card function	Authentication (online)	Yes	Yes	Yes	Opt in
	Authentication (visual)	Yes	Yes	No	Yes
	e-signature	Opt out	Yes	Yes	Opt in
eID attributes	eID data on chip				
	• Name	Yes	Yes	No	Yes
	• address	Yes	Yes	No	Yes
	• date of birth	Yes	Yes	No	Yes
	National register number	Yes	Yes	No	No
	Visual data:				
	• Address	No	Yes	Depending on card	Yes
	• Owner's photograph	Yes	Yes	No	Yes
	PIN protected data for authentication	Yes	Yes	Yes	Yes
	Unprotected readable data	Yes	No	No	No
	Biometrics:				
	• Face	No	Yes	No	Yes
	• Fingerprints	No	Yes	No	Opt in

In contrast, the German eIDMS employs a *double-sided authentication*: a service provider can only get access to the eID data on the card of his customer as authorized by an *access certificate*, for which he has to apply to a federal agency. According to the *principle of proportionality* the access rights granted cover only the data which is necessary for the particular service. This may only be a name or in other cases only the citizen's age or address (see Noack and Kubicek 2010, for technical details see Bender et al. 2008). The Austrian virtual Citizen Card does not contain personal data but only a *personal link*, which is used to produce sector-specific PINs for the respective service in each transaction. Thereby the Austrian eIDMS provides technical means against merging citizens' data across different sectors of e-government (see Aichholzer and Strauß 2010).

Table 2 shows the main features of the authentication process in the four countries.

Distribution, personalisation and activation of eIDs

The systemic character of eID systems stems from a complex infrastructure for generating eIDs, putting them on tokens, delivering them to the citizens and having them activated for use in online authentication. Again there are significant differences between the four countries.

Table 2 Features of four authentication processes

	BE	ES	AT	GE
Possession and knowledge (card & PIN)	Yes	Yes	Yes	Yes
Length of PIN (no. of digits)	4	8–16	6	6
Changeable by user	No	Yes	Yes	Yes
One-/double-sided authentication	One-sided	One-sided	Double-sided	Double-sided
Data accessible for service provider	Complete attribute data	Complete attribute data	Identity link with source PIN	Selected data according to certified access rights

In Belgium and Germany the eIDs and the cards are produced centrally and distributed via the local municipalities. While in Belgium citizens are notified to pick up their new card when the old one expires, in Germany citizens must obtain a new card themselves. In both countries they have to pick up the new card at the local registration office and receive a PIN code separately by mail. In contrast, in Spain cards are personalised at local police stations, i.e. the eID is placed on pre-produced chip cards there (see Heichlinger and Gallego 2010). In Austria the distribution process depends on the kind of card chosen as token (social security or bank card). The cards are sent by mail and afterwards have to be activated online at a local office of the respective issuer. However, the personal link, which is put on the card, comes from the Central Registry (see Aichholzer and Strauß 2010).

There are also differences regarding *electronic signatures*. In Austria the e-signature is a constituent part of the Citizens Card concept, as is the case for the Spanish ID card. In Belgium they are distributed by default and citizens have to *opt out* if they do not wish to have one, while in Germany the card only provides the capacity and citizens have to choose a provider afterwards, register separately and download keys and certificates (*opt in*).

In all four cases the component data for the eID comes from a *civil registry* where citizens have to register by law and receive a confirming document. When picking up the eID token they have to authenticate themselves, so their identity is corroborated by ID documents as well as by visual control. All four processes can be classified as *strong authentication.*

Tables 3 and 4 show the main differences between the eID infrastructure in the four countries.

Installation of eID technology and support

For online authentication in all four cases the user has to install a *card reader* with corresponding driver software as well as a piece of *client software* for the authentication process, which via a web browser interacts with an eID server on the side of the provider of the online service.

As card reader driver and eID client originate from different developers and have to interoperate with different web browsers running on different operating systems,

Table 3 Distribution, personalisation and activation of eIDs

	BE	ES	AT	GE
One/several tokens	= 1	= 1	>1	= 1
Personalisation	Central	Local	Central (Personal link)	Central
Request and pickup	Local municipalities	256 delivering offices in police station	Different agencies	Local municipalities
Distribution of PIN	Separate by mail	Locally	Depends on card issuer	Separate by mail
Activation	By default	By default	Required	Required
Source of ID data	Central register	Central register	Central register	Local register
Electronic signature				
No of CAs	1	>1	1	>1
No of RAs	Same for eID	Different agencies	Different agencies	Different agencies
Modus on eID card	Opt out	Mandatory	Mandatory	Opt in
Access certification of service provider required	No	No	Yes	Yes

one can expect some *problems of interoperability*. These problems will be magnified if the user has to buy the components separately. They may be smaller if the issuer of the eID card provides a *package* including a card reader, driver and client software. But problems may still occur if a new browser version or a new operating system is installed. For these cases, *support* may be provided by FAQs on a website and/or a telephone hotline (Table 4).

Table 4 Installation of and support for eID Software

	BE	ES	AT	GE
Card reader and client	Package	Separate	Separate	Package (planned)
Central website for download instructions	Yes	Yes	Yes	Not yet decided
Support via:				
- FAQs	Yes	Yes	Yes	Not yet decided
- eMail	Yes	Yes	Yes	
- Telephone	Yes	Yes	Yes	

Provider-related procedures

An additional element of eIDMS is *provision for providers* of e-government and e-commerce services, which have been established in Austria and Germany via technical certificates and in Belgium via a legal application procedure.

Because the Belgian eID includes the National Registry Number which reveals the date of birth and a code for the sex of the holder, by law it may not be used for

authentication purposes by non-governmental units. Instead private sector organisations have to get *permission from the Privacy Commission* for using the ID number in electronic processes. In Spain, the eID also includes the date of birth and a code for the sex of the holder, but no legal or technical requirements restrict the use of the eID card and/or the personal identity number by private-sector organisations.

In Austria, as mentioned before, the virtual Citizen Card only contains an identity link with a source PIN, which is needed to generate a sector-specific PIN by the Central Registry of Residents (CRR). Public and private sector organisations have to *apply to the CRR* for making use of the citizen card. In Germany, providers of e-government or e-commerce services have to apply for a *certificate granting access* only to those data necessary for providing the respective service. Providers have to put the access certificate on their eID server, which enters into a dialogue with the eID card. The Federal Administration Office deals with this certification process and may also revoke certificates.

To summarize, there are differences with regard to almost every aspect of the eIDMS between at least two of the four countries. The only common features in all four eIDs are the size of the cards used as tokens, and the legal obligation to register and to hold an ID document. This is remarkable as the four countries have been selected according to the "most similar design" principle. Therefore these differences call for explanation.

A three-fold path dependency

According to our conceptual framework we assume that differences in the design of a national eIDMS as described in the previous section can be explained by their predecessors and the deliberate decision of the main actors to either continue this path, to modify or to break with it, move to another path or create a new one. These path-related decisions concern the technical components of the eIDMS, the organisational arrangements and the pattern of regulation. Therefore we speak of technological, organisational and regulatory paths. In our conceptual framework we further assume that the relevant context conditions have already influenced the predecessor systems, and thereby restrict the path-related choice and allow for different degrees of discretion. However, creating a new organisational or regulatory path means establishing new institutions and thereby changing contextual factors, such as the legal and administrative structure in the respective country. In this section we will consider the extent to which such changes happened. In the following section we will examine the interaction system and the main actors and try to explain why there was path continuation, change or creation.

As this research is exploratory and aims at hypothesis generation rather than hypothesis testing, we will summarise our findings, interpretations and conclusions from the four case studies in the form of generalisations. These may be considered as hypotheses and as Grounded Theory (Glaser and Strauss 1967) and will be subject to tests by comparison with other countries with different basic characteristics of their national IDMS in the next chapters of this special issue.

As a first rough summary of the four case studies we dare to generalise:

G 1 The decisions taken for most of the organisational arrangements, the technical components and regulatory patterns of the national eIDMS

follow established paths. In a few cases new paths had to be created because there was no predecessor. The creation of a new path only occurred with regard to privacy protecting measures.

Organisational paths

An eID, as a set of attributes assigned to an entity, is primarily an organisational innovation and only with regard to the token chosen and the authentication process a technical innovation as well. To analyse path dependency with regard to organisational paths, we have to see whether existing institutions are continued and/or assigned new tasks, whether they have been changed or whether new institutions have been established, in particular whether

- previous attributes are kept or whether new ones have been added,
- the existing administrative procedures for registration and authentication have been transposed into the online world or been changed,
- the same organisations which are in charge of the ID are administering the eID.

From the comparison of the four eIDMS we conclude that there is a high degree of continuation on the organisational path:

G 2.1 With regard to the definition of the eID and the organisational arrangements for administering eIDs, there is a high degree of path continuation. The definition of the ID has not been changed, and the eID is administered by the same institutions as the previous ID documents, except for Austria and Germany, where some additional procedures have been established to adhere to privacy requirements, still employing existing institutions.

Table 5 displays the relevant organisational features of the four eIDMS:

With regard to the *definition of the eID*, in three of the four countries nothing has changed. The eID consists of the same attributes and data as the previous national ID. Countries which previously had a *unique personal identity number* are using it for the eID as well; the others did not take the opportunity to introduce one. The only exception is Austria, which considering the difference between online and offline authentication introduced sector-specific PINs instead of one uniform eID generated via a secret personal link, which is provided by the Central Registry. *Germany* is a special case with regard to *digital fingerprints*: they are not part of the eID function and may not be used for online authentication. They can only be accessed by special card readers for personal inspection by police or for border control. But including them on the same eID card as the eID for online authentication had effects on the public and political debate and the issuing of the new revised ID Card Act.. We classify this as *path merger* and not as path creation because the digital fingerprints were already collected and stored in the RFID chip of the *recent new electronic passport*. When defining the data to be stored on the eID card, the passport path was merged with the eID (card) path, because the eID card serves as a travel document as well.

With regard to *administrative procedures* there were only a few changes, due to different technical or regulatory requirements. In all four cases citizens have to register

Table 5 Continuation, changes and creations on the organizational path

	BE	ES	AT	GE
Definition of eID				
ID from civil registry	Yes = Continuation	Yes = Continuation	Yes = Continuation	Yes = Continuation
Unique Personal identification number before / after	Yes / Yes = Continuation	Yes / Yes = Continuation	Yes / ssPIN = Path creation	No / No = Continuation
Digital fingerprints before / after	No / No = Continuation	Yes / Yes = Continuation	No / No = Continuation	No / Yes = path merger
Procedures				
Request/ Application	Local authority = Continuation	Police station = Continuation	Different issuers = Continuation	Local authority = Continuation
Personalisation	Central agency = Continuation	Police station = Continuation	Central agency = Path creation	Central agency, = Continuation
Distribution	Municipality / PIN by Mail = Continuation + addition	Police station = Continuation	Depending on card issuer = Continuation	Municipality, PIN via Mail = Continuation + addition
Provider certification for access to eID	Legal restrictions for using PIC = Continuation	Not required = Continuation	Registration = Path creation	Certificate required = Path creation
Organisational arrangements				
Registry keeping institution	National registry = Continuation	National registry = Continuation	National registry = Continuation	Local registry = Continuation
Production of token	One provider = Continuation	One provider = Continuation	Diff. issuers = Continuation	One provider = Continuation
RA and CA for signature certificate	One provider = Continuation	One provider = Continuation	One provider = Continuation	Several providers = Continuation

and to apply for a new eID card when the old one expires and the ID is taken from the central civil registries. The only difference is that the eID has to be activated after receiving the token and that in two countries the PIN is delivered separately by mail. Only Austria and Germany created a new organisational path by establishing a *registration or certification procedure for access rights*. In Spain new technical means were not considered to afford any organisational change. Instead new technology had been developed to maintain the existing organisational arrangements: paper-based identity cards had been personalised by handwriting in the local police stations, and now electronic machines were developed and installed in hundreds of police stations which personalise pre-produced eID cards there. The capture of the digital fingerprints is in line with previous procedures as well. Although they did not show on the previous card, they did on earlier ones and have for decades been collected and stored in a central register (see Heichlinger and Gallego 2010).

Technological paths

The term technological path refers to the choice of the *token* as carrier medium for the eID-based authentication and to *related functions* such as electronic signatures and data protection technology. In those countries which have chosen their national ID card as token for their eID, this has been done in conjunction with *a technical innovation of the ID document* for visual inspection, e.g. police and border control. Of course the step from a paper-based ID document, even if it has a machine-readable data zone, to a chip-based card cannot be considered as path continuation. Nor is continuation possible with regard to the functions of the card, as the eID function had no predecessor. Therefore technological path constituency does not refer to the continuity of the old token, but rather to *adherence to general trends in smart card and authentication technology.*

G 2.2 Decisions made for most of the technical components of the national eIDMS follow established paths of smart card and authentication technologies.

Table 6 shows that there was *almost no deviation from mainstream chip and PKI technology* in Belgium and Spain, but path creation in Austria and Germany. According to the *Citizen Card concept,* on the Austrian cards the Sector-Specific PIN is generated on the chip requiring a different kind of processor technology Germany is the only country to employ a *RFID chip*, but not as new path creation because of the eID, but because of the travel document function and a corresponding adoption of the path of the recently introduced electronic passport according to the *ICAO standard.* We may also speak of a *path merger* in this case. It has to be noted at this point that the other three countries so far have not introduced a new passport according to this standard, despite a *European Directive* requiring digital fingerprints to be included by June 2009 (European Council 2004).

There were two main reasons for choosing an RFID chip in Germany (see Noack and Kubicek 2010). Considering the 10 year validity of the eID there is the risk that a contact-related chip at the end of this period may cause problems owing to *abrasion*. There is no experience in this regard with any contact-related chip being used for more than 6 years. Therefore a contactless chip has been chosen which is not exposed to abrasion. The Belgian eID card also has a validity of up to 10 years,

Table 6 Path constituency of technical features

	BE	ES	AT	GE
Carrier card = new eID-card	Yes	Yes	No	Yes
Card format	ID1 = Path change to mainstream	ID1 = Path continuation	ID1 = Path change to mainstream	ID1 = Path change to mainstream
Contact/ contactless chip	Contact = Path change to mainstream	Contact = Path change to mainstream	Contact = Path change to mainstream	Contactless RFID = Merger with ePassport path
Separate eID certificates	Yes = Path change to mainstream	Yes = Path change to mainstream	No (Personal link) = Path creation	Yes = Path change to mainstream
IT security procedures	Yes = Path change to mainstream	Yes = Path change to mainstream	ECC = Path change to mainstream	EAC2/PACE = Merger with advanced ePassport path
Privacy preserving features	No = Continuation	No = Continuation	ssPIN = Path creation	Selected Access by certificates = Path creation
PIN protection of authentication data	Standard = Path change to mainstream	Standard = Path change to mainstream	Standard = Path change to mainstream	Standard = Path change to mainstream
Selected or full access to authentication data	Full access = Path change to mainstream	Full access = Path change to mainstream	No ID data on chip = Path creation	Selected access = Path creation
PKI for e-signatures	Yes = Continuation	Yes = Continuation	Yes = Continuation	Yes = Continuation

but the people in charge of the eID card did not share this concern. On the contrary, Belgian officials had doubts about the security of RFID chips, which their German colleagues did not share. The second reason for RFID chips in Germany was brought forward by the Federal Police: The prevcious ID card was larger than the new one in ID1 format and showed a larger picture. Federal Police insisted on keeping the *size of the picture* on the smaller new card to guarantee for the same conditions for visual inspection at night or under other unfavourable circumstances. Only if there were no contact space for a chip on the card, would it be possible to have a picture of the old size as well as data in a readable format on a smaller card (see Table 1, above).

G 2.3 The choice of technological path continuity, modification or creation depends on the options available at the point in time when the decision on technical components was made.

According to our conceptual framework, the technological options available to actors are assembled in the *technological pool*. In other words, the technological pool contains all technologies from existing paths and any new alternative option. Due to technological progress, the pool is not static but grows over time. Path constituency in this view means that actors compare a given path with newly available alternatives and compare the advantages and disadvantages. Therefore the point in time when decisions were taken is relevant for identifying the options available in the technological pool at that time.

Figure 2 shows the point in time of the development process in relation to relevant technological innovations and standards. For example the ICAO specification for biometry on RFID chips was issued in 2003 and the EAC standard for data access to the electronic passport was issued only in 2006. Therefore the e-passport path was not an option to be considered when the Belgian or Spanish eID cards were specified.

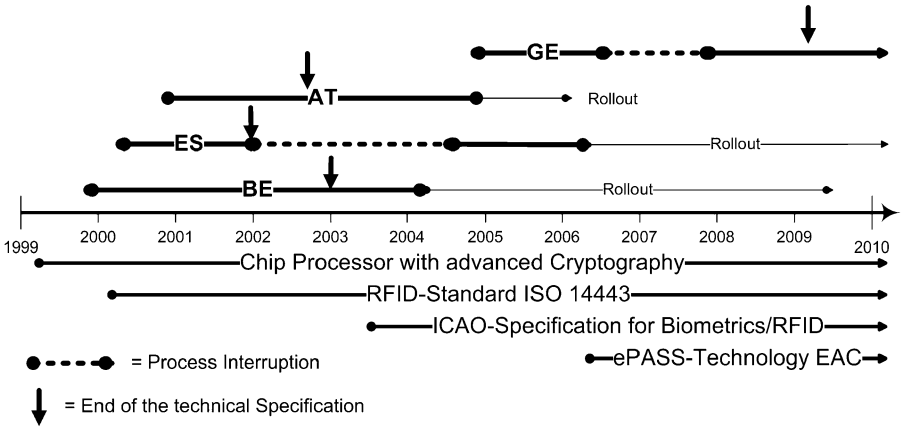

Fig. 2 eID development processes in relation to relevant technological innovations

G 2.4 Once a technical choice has been made and a new path has been created, this establishes path dependency for the future.

Rollout of the new eID cards has finished in Belgium and will soon be in Spain. The first exchanges of eID cards have already taken place in Belgium in 2009, and

both countries will have to exchange the eID cards in 2014 and 2016 respectively. As the specification and preparation for mass production of new processor chip cards takes about 5 years, considerations on path continuity or path modification have to be made right now.

In Belgium there is a discussion to integrate the SIS card with the eID card via the authentication function, but this has not been finally decided yet. There is no intention to change the token, the process or the infrastructure. In Spain and Austria there is no discussion to change the eIDMS at all. Perhaps there will be minor improvements regarding security requirements, but the eIDMS established now seem to achieve a high degree of path persistence — even at the risk that the new eID card may not be used as a travel document outside the Schengen area.

Another indicator of path persistence is the introduction of complementary eID cards according to the pattern of the primary eID card. In Belgium this is the case for the Kids Card, which is issued for children under the age of 12 years, but without e-signature, as well as for the foreigner card for EU-citizens (see Mariën and Van Audenhove 2010).

Regulatory paths

By regulatory path we mean the legal regulations concerning the obligation to register and to hold an ID document, to get the authentication functionality, as well as limitations for employing the authentication function or special certification requirements. Of course existing legislation has to be adapted if a new kind of document is introduced. We have already seen that the attributes establishing the eID do not differ from the previous official ID. In this respect legislation was not changed. However, there were some new legal provisions and adminstrative procedures related to the use of the eIDs by providers of online services in particular for privacy enhancing features (Table 7).

G 2.5 The regulatory patterns concerning the eID are kept quite stable. Existing legislation has only been adapted to cover the technical and organisational changes. But in two countries new paths have been created to provide for appropriate privacy by design.

As already mentioned with regard to the organisational path, the general obligation to register and to hold an ID document have not been changed nor the definition of the eID as taken from the civil registry in three of the four countries. With regard to these basic aspects *existing legislation had to be adapted* to refer to the new kind of documents, i.e. the eID card. The only exemption is Austria, which opened a new regulatory path by issuing an eGovernment Act. Austria also had adapted the Identity Card Act in 2001 to allow for the ID card as token for the Citizen card, but so far does not use this possibility. The Citizen Card and Sector-Specific PINs together with electronic signatures are regulated in a separate newly created e*Government Act* (see Aichholzer and Strauß 2010). In the other three countries the planning for a new technical means has not been considered opening a window of opportunity for the introduction of general changes in the national IDMS regarding the identity attributes, registration obligations etc.

Table 7 Regulatory path dependency

Country	BE	ES	AT	GE
ID card mandatory	Yes = Continuation	Yes = Continuation	Or other official documents = Continuation	Or passport = Continuation
eID function mandatory	No, opt out = Path creation	Yes = Path creation	No, opt in = Path creation	No, opt in = Path creation
Digital fingerprint on token	No = Continuation	Yes = Continuation	No = Continuation	Opt in = Path change
Signature mandatory	No, opt out = Continuation	Yes = Continuation	Yes = Continuation	No, opt in = Continuation
Limitations of use for Authentication	Permission required for using Reg.No = Continuation	No = Continuation	ssPIN procedure = Path creation	Service provider access certification = Path creation

Austria and Germany also enacted particular provisions for privacy preservation and thus responded to public concerns, i.e. via Sector-Specific PINs in Austria and the selected access rights to eID data according to certification within a double-sided authentication process in Germany. We will discuss in section "Legal context, culture and values" why governments in the four countries differ in this respect.

The interaction system: Relevant policy fields and power structure

In an actor-oriented view, these differences are the outcome of the decisions of powerful and resourceful policy makers taken in specific contexts and more or less following established paths (see Scharpf 2000 as well as the introductory paper by Kubicek 2010). However it is not obvious which actors to start with, because eIDs are not linked to specific classes of policy actors. From previous descriptive studies we know that the initiative for the introduction of a national eIDMS arose in the context of national *e-government initiatives and programmes*. However, e-government is not an established policy field. It is directed at the modernization of public services by introducing or enhancing ICT. As these public services and processes belong to different established policy fields such as tax, social welfare, home affairs, environmental affairs, e-government is a transversal effort, which may be assigned to different ministries and needs coordination in any case. In addition, it depends on which token is chosen and which other functions this token has to provide. As governments change over time, and new governments may have different priorities, the actor constellation also may change in the course of the whole development process. From the four country reports we also learned that, except for Spain, the new eID card was not the first choice as the token for the eID function.

In this section therefore we will first assess where within the policy system plans for an eID function started and which tokens were looked for. Then we will look at the relevance of different policy fields involved in each national development process, coordination mechanisms and whether changes in government offices resulted in any changes of plans for the eIDMS.

E-government as the starting point for national eID initiatives

Being EU Member States, the four countries under comparison share the same history of decisions taken by their governments at European level. The European Commission launched the initiative "eEurope 2002" in December 1999 with the aim of accelerating Europe´s development towards a knowledge-based economy, including better access for all European citizens to the new services of the information age. The Council of Ministers at the Feira Summit in June 2002 adopted the first eEurope 2002 Action Plan, aiming at (1) a cheaper, faster, secure Internet, (2) investing in people and skills, and (3) stimulating the use of the Internet. Under the third objective with reference to the Lisbon strategy it was agreed that "Member States ensure generalised electronic access to main basic public services by 2002/2003" and "promote the use of electronic signatures within the public sector". eIDs and online authentication were not mentioned in this section, but the first objective included the "availability of cost-effective smart card solutions to enable secure electronic transactions by 2002" (Council of the European Union 2000).

For all of the objectives, regular measurement of achievements was agreed upon. The first benchmarking report was submitted in 2002 (European Commission 2002). For progress of e-government a special annual benchmarking was commissioned to Cap Gemini, starting in 2001 referring to the online availability of 20 public services, 12 addressing citizens and 8 provided for business (see e.g. the 5th report, Cap Gemini 2005).[1]

Against this background we found that the policy field of e-government as part of the field of (the modernisation of) public administration has been the home domain for eID considerations.

G 3.1 The common starting point for the introduction of eIDs in EU Member States has been the policy field of e-government, i.e. the modernisation of public administration by ICT, in particular offering public services via the Internet: for this purpose stronger methods of authentication than username and password seemed necessary. The new authentication methods should be employed for e-government services in all areas and at all levels of government, national, regional and local, and perhaps also in e-commerce. The departments of national governments responsible for e-government initiated processes aiming at the introduction of a unique eID at national level.

Within the national governments of the four countries, responsibility for e-government is assigned to different ministries and there are different regulations or practices involving lower levels of public administration (state, provincial, regional governments and local municipalities), which are responsible for most of the services for citizens and business.[2]

[1] For a summary of the eEurope Action Plan 2002 and 2005 and the benchmarking of public services see http://ec.europa.eu/information_society/eeurope/2002/index_en.htm.

[2] For details see the e-government Fact Sheets for each country on the epractice portal http://www.epractice.eu/en/factsheets/

The first e-government program in Belgium was launched in 1999 and 1 year later a Federal ICT Manager was appointed to design a common ICT strategy in the Federal Public administration. In 2001, his function was assigned to the newly established Federal Department for ICT (Fedict) responsible for developing a common strategy for eGovernment, promoting and ensuring its uniform and coherent implementation within Federal Government Departments and Agencies, while developing cross-government standards, frameworks, projects and services necessary to deliver the strategy. Fedict is in the political domain of the Ministry for Enterprise and Simplification. The Minister holds the political responsibility for overseeing both the work of the Agency for Administrative Simplification and that of the Fedict. However the responsibility of the Federal Citizens Registry lies with the Ministry of the Interior.

In Austria e-government activities date back to 1995 when an Information Society Working Group was set up by Federal Government. In 2000 an initiative "eAustria in eEurope" was launched to implement the eEurope action plan in Austria. e-government responsibility shifted from the Ministry of Finance, in charge of ICT at the Federal level, to a newly established Chief Information Officer (CIO) affiliated to the Federal Chancellery and an ICT Board for coordinating the federal and the regional level. One of the main activities of the CIO and the ICT Board was the preparation of a Federal e-Government Act issued 2004 and the introduction of the Citizen Card.

The first e-government programme in Spain was launched in 1997 to support the efficient introduction of so-called multimedia services to public administration. In 2000 the Secretary of State for Public Administration was assigned responsibility for the use of ICT in the public sector and the eID card was included in the plan "Info XXI Initiative" Responsibility was taken over by the DG Police within the Ministry of the Interior, but without the necessary budget. In 2004 the new Vice President assumed political leadership of e-government and provided decisive impulse for the introduction of the eID card.

Early e-government initiatives in Germany concentrated on electronic signatures, introduced by the Signature Act of 1997, initiated by the Federal Ministry of Research and Technology. After elections in 1998 and a reshuffle of ministries, this responsibility together with the respective unit and people was shifted to the Ministry of Economics and Technology. The first federal e-Government programme "Bund Online 2005" was launched in 2000, integrating activities of the Ministry of Education and Research, the Ministry of Economics and Technology and the Ministry of the Interior and coordinated by the Federal Ministry of the Interior (BMI). The BMI in 2005 founded a new unit within the IT department responsible for ID cards, passports and civil registry, which worked on the new electronic passport as well as the new electronic identity card and its eID function.

G 3.2 The ID card was not the first choice of token for online authentication. Either social security or e-signature cards were tried first. The eID cards came on the agenda only after the first attempts had failed.

When it came to choosing an appropriate token for the eID, a next generation national ID card was not the first choice. Because of the ten-year validity of national ID cards, rollout would need quite a long time, i.e. 5 years until only half of the citizens would possess a new eID function, while the need for providing for more secure online

transactions in e-government and e-commerce should be met as soon as possible. There was the choice of creating particular tokens for the eID function or to put it on other existing or planned cards. In this case other policy fields had to be won for cooperation. In Belgium and Austria, first attempts were undertaken to place an eID function on a social security card. In Austria this preference was obvious as there is no obligation to hold an ID card. In Belgium the preference resulted from considering the possibility of a fast rollout as well as the recent positive experience of introducing a chip-based health and social security card (SIS Card). A new social security card can substitute an old one at a certain point in time for all members, so rollout of a new eID function could be completed in a few months. However, the eID still should be the national ID from the civil registry. So there are different legal provisions, different institutions involved, partly state-owned, partly not, and there was the concern that data on a social security card should not be exposed to other agencies in government or even e-commerce. Political actors responsible for social security cards had nothing to win from opting for a general eID function but rather had to fear that such an add-on could raise opposition against ongoing projects for new cards and/or new applications. As these attempts failed, e-government actors had to look for another token.

In Germany, legal and technical e-government experts in government as well as academia believed for a long time that the e-signature according to German signature law would provide for strong authentication. Qualified e-signatures are offered by several certified certification authorities and can be placed on special signature cards or on bank cards. However, as the certificate only contains the name of the holder, there is no unique identifier and another token had to be found. For a short time the idea of an integrated health and ID card was pursued, but then the planned renewal of the existing ID card by an eID card was chosen as a window of opportunity.

For Austria it is interesting to note that when after several delays in 2005 the electronic social security card (e-card) was finally launched, it was employed as another token besides the bankcards and today is the most widely used token.

So, in Belgium and Austria there was a preference for the social security card as eID token, although at first it was not available. Austria choose bank cards and had some experiments with SIM cards, Belgium took the opportunity of a pending transition from a paper-based card to a smart card to add an eID authentication function. Germany had started with e-signature cards, while only Spain moved directly to a national ID card. By choosing this particular token, requirements regarding the security of the token and for other functions had to be considered in all three countries, but gained quite different degrees of influence.

The relevance and power distribution between different policy fields

If a national ID card is chosen as token for an eID function and if this card is employed for visual inspection by police and at border control, these functions pose additional, even conflicting requirements, and compromises have to be reached between different actors.

G 3.3 When choosing an existing token for an eID, actors from the respective policy fields have to cooperate. They make their own claims regarding

attributes and procedures and thereby increase the complexity of the innovation process. The e-government actors did not always have the greatest power to influence the design of the token.

In the interviews, experts were asked to assess the influence of the different policy fields and of actors representing these fields. The research teams in the four countries summarised these estimates on a three-point scale (Table 8).

In all four countries the initiative for a stronger eID-based online authentication function arose in the *e-government context*, and the first announcements were made in e-government programmes by the respective national governments. However, in Spain and Germany, because the *national ID card* was chosen as token, the units responsible for ID cards took over leadership, reducing the influence of the e-government actors to an influence of 2 points instead of 3 in Belgium and Austria, with a higher influence (3 instead of 2 points) of the actors in the field of public safety/police. Although Belgium also chose its new national ID card as token, there were no claims from another policy fields, so the eID project could remain a *single policy field innovation*. Interview partners in Belgium explicitly stated that no party addressed either the issue of the security of the new card or brought forward any concerns of public safety. *Biometry* was deliberately kept out in order to avoid delays and provide the online authentication function as soon as possible.

Again *the point in time*, when decisions are made, and path persistence, play an important role: Without any doubt *September 11, 2001,* changed the political importance of public safety, including the security of ID documents in order to fight terrorism. But not all countries reacted in the same way, and in some countries relevant decisions had been taken before this event, while in other countries decisions have been made later taking into account the shift of political priorities. In *Belgium* the preparation process for the new eID card, however, had started before September 11, 2001, and nobody wanted to complicate this process by introducing additional requirements. In contrast to Germany, there was no legislative reaction to September 11, 2001, at all in Belgium and thus there was no other policy field to be linked with.

In *Spain* the initiative for an eID was started in the Ministry for Public Administration. But once the ID card had been chosen as a token, the governance of the process was completely taken over by the Director General of the Police in the Ministry of the Interior, which had been responsible for issuing all previous ID cards, but did not have the necessary budget. In Spain, IT infrastructure for government is

Table 8 Influence of actors from different policy fields on the eIDMS development

Actors from policy field	BE	ES	AT	GE
Public safety/police	1	3	1	3
Public administration	3	2	3	2
Industry/commerce	1	2	1	1
Finance	1	1	1	1
Social/health	2	1	2	1
Chancellery/cabinet	1	2	3	1

Actors and their influence in the development process (1=low, 3 = high)

financed and managed by the Ministry of Industry, Tourism and Commerce, aiming at offering the eID function to public utilities and e-commerce as well.

In *Austria*, the eID function remained in the policy field of e-government, but responsibility shifted as the whole field was reassigned from the Ministry of Finance to the Chancellery.

In *Germany* after September 11, 2001, the option for biometric features on the national ID card had immediately been introduced in the Identity Card Act. This option has been taken up again 4 years later and raised some political controversies we will discuss in more detail later on. The eID function has only been specified in detail in 2008 when the final version of the law on eID cards had to be drafted and became optional.

To summarise these different assignments and influences we can say:

Spain and Belgium have placed an *eID function on a new eID card.* Austria has not decided for a particular token, but the e-card now emerges as the main carrier. Germany is introducing a *new eID card, which offers the option for an eID authentication functio*n.

Intragovernmental coordination

If several ministries and other units are involved, the success of an innovation process largely depends on the *coordination mechanisms* employed.

The initiatives for national eIDMS emerged from national e-government programmes and plans. But e-government is not an established policy field with a clear assignment to one of the traditional ministries. It has some affiliation to the domain of ministries of the interior or home office, which are in charge of public administration and public employees, but there are also IT-related tasks as well as e-commerce and Internet-related topics. Most of the e-government programmes are the outcome of *interdepartmental boards or working groups*, which also may recommend the development of a national eIDMS, but do not have the authority and the budgetary power to start such a process. Rather other more powerful actors within the relevant ministries have to be involved and reach consensus about the function and the token, financial resources, legislative action etc. In all cases, legislative action was required and had to be agreed upon between the ministries and with the majority parties in parliament.

The duration of the consensus-building part of the whole process and the degree to which e-government-related requirements can be implemented largely depends on the coordination or integration provisions, which were already there or have been established for this process.

The importance of intragovernmental coordination had not been foreseen when developing the conceptual framework. But as we are conducting exploratory research aiming at generating grounded theory, additional conceptual elements may well be introduced along with empirical findings. There are *a few theories* about the role of champions in innovation processes. Already in 1973, Witte proposed a variation of such a view assuming that in successful intra-organisational innovation processes one would frequently find a *tandem of a power and an expert promoter*. His case was the employment of mainframe computers in companies in the late 1960s. With regard to duration and outcome, successful processes showed a powerful actor in top management teamed with an acknowledged IT expert on a lower hierarchical level (Witte 1973), i.e. power and expertise formed a synergy.

With regard to general coordination mechanisms, we can distinguish *hierarchy* from *networks* or *clans* (Ouchi 1980). An alternative to the dual promoter hypothesis of Witte is the existence of a clan of actors in the organisations concerned. A "clan" according to Ouchi is a group of people with similar background, interests and objectives, who share certain values and visions and coordinate their activities independent of formal organisational affiliations and boundaries.

G 3.4 The duration of the development process depends on the coordination mechanism employed. Either a couple consisting of a power and an expert promoter or a clan of (public) managers involved can contribute to speed up the process, while the lack of such mechanisms leads to delays.

In Austria, CIO Posch can be viewed as expert promoter with power derived from Chancellor Schüssel. In Spain there was a delay until the new vice-president took over leadership. In Belgium, there was a long stability of a group of actors who might be called a "clan" in the most positive sense: Frank Robben (Head CBSS), Luc Vanneste (Central Register FOD IBZ), Bart Preneel as well as Jos Dumarties (University of Leuven) had been nominated members of the commission to develop an e-government policy in 1999, and from different positions in different ministries prepared all the decisions for the eID function and the eID card. In Germany, there was no need for intra-governmental coordination as the different areas concerned were all within the domain of the Ministry of the Interior. However, there was some kind of a clan including the head of the newly created Unit for Passports, Personal ID and Civil Registry, the head of the responsible department within the Federal Office for IT Security and the director of the Federal Printing Office, which is to print and personalise the eID card. At least from 2006 onwards, the three men cooperated intensively based on shared basic values and interests.

Political power structure: Ruling parties and changes in government

The different weighting of modernisation of public services vs. public safety and police issues might be explained by differences between ruling parties. Similarly some of the differences between the national eIDMS and most of the cases of path creation are related to privacy concerns, which may be due to different priorities of the ruling political parties. The likelihood that a change in government due to elections will change the plans for an eID and an eID card is expected to be lower if existing paths are followed. The same is true with regard to the relation between governmental units planning the system and preparing legislation on one side and the parliamentary factions on the other.

G 3.5 If governments propose an eIDMS, which follows established technological, organisational and regulatory paths, it is unlikely that there will be dissent by the majority faction(s) in parliament. In cases of path creation there will be no dissent either as long as the new paths are in line with the values held by the majority faction(s).

In Belgium, Spain and Austria there was no dissent between the government and the ruling parties in parliament. In Belgium the consent of the privacy commission was sufficient for not entering a larger parliamentary debate. In Spain nobody dared

to question the authority of the police directorate. In Austria a new path was created with complicated regulations on public and private keys as well as sector-specific PINs and laid down in the E-Government Act. As this had been elaborated in the Chancellery and agreed upon by the ICT board, it did not raise any general concerns in parliament, nor was there a controversial public debate in the media either. The whole issue had been considered to be of relevance and interest for IT specialists only. The project managers in Austria and Belgium confirmed that neither security concerns after September 11th nor privacy concerns were addressed when they presented their concepts for the national eIDMS to parliamentary bodies, because they deliberately had not linked the eIDMS to issues of public safety and terrorism and could refer to the consent of the privacy authorities.

In Germany the Social Democratic faction in parliament did not dissent to the newly created path of the eID function for online authentication but—to the surprise to the governmental actors—did not accept the proposed mandatory inclusion of digital fingerprints on the eID card. This option had been incorporated in the ID Card Act immediately after September 11th within a package law against terrorism. This package had been launched by the Minister of the Interior from the Social Democratic Party within a coalition government with the Green Party. There were some concerns in both parliamentary parties about the right balance between security and privacy, but nobody dared to oppose in this situation as the plans for the attack had been prepared in Germany. However, when 8 years later the draft bill on the new eID card was submitted and provided the details for the already announced inclusion of digital fingerprints, the Social Democrats in Parliament did not feel bound to this former decision. Meanwhile there was a newly elected Parliament and the new bill came from a minister of the Christian Democratic Party. Although in a coalition government with the Christian Democratic Party, the Social Democrats opposed the mandatory inclusion of digital fingerprints. Their concern was not only that checking fingerprints is associated with criminals. In addition, it is the specific historical memory that the National Socialist government under Adolf Hitler had collected fingerprints to identify Jews (see the German case study by Noack and Kubicek 2010).

Leading Social Democrats did not believe the Minister of the Interior, Wolfgang Schäuble, that the fingerprints would only be stored on the chip and the data collected would be deleted immediately after personalisation, as he already had introduced several extensions of surveillance. This opposition from the coalition partner was a surprise to the minister and his staff as the inclusion of a biometric photo and digital fingerprints in the electronic passport had not caused any lasting opposition. They thought that with the eID card they would only continue this path. But the Social Democrats perceived some basic differences. As US government by now required digital fingerprints to be stored on passports, such a passport would provide greater convenience for Germans travelling to the US. In addition there was also an ICAO standard for passports as well as the expectation that all other EU Member States would follow.

Its convenience could be presented as an advantage of the eID card, if it can serve as a travel document for many countries as well. From a constitutional point of view, however, a passport is not mandatory in Germany. Citizens have to hold either a passport or an ID card. As the fingerprints were made mandatory for the passport

already, an obligation to include fingerprints on the eID card would have forced every citizen above 16 years of age without exemption to give their fingerprints. This was perceived as a disproportional infringement of personal freedom. The compromise agreed upon was that the inclusion of digital fingerprints will be optional: If a citizen wants to use his eID card as a travel document to be accepted by states that are checking biometrics at their border, they can opt in.

The German case to some extent shows that there are differences between political parties with regard to their priorities if there is a conflict between public safety and privacy. But this did not concern the eID function but other functions of the token and it was an exception without parallel in the other countries due to a particular historic background.

G 3.6 Traditional stereotypes according to which conservative parties give higher priority to public safety features while socialist, social democratic and liberal governments are more inclined to prioritise privacy requirements and provisions do not apply to these cases. Accordingly changes in government did not affect the plans for a new eIDMS.

One might expect that conservative governments give higher priority to public safety features while socialist, social democratic and liberal governments are more inclined to privacy saving provisions. However, this stereotype did no show in the case of Austria, Belgium and Spain at all and only with regard to the finger print issue just mentioned in Germany. Rather the contrary can be observed in some cases.

Austria experienced a coalition government of the two biggest parties, the Social Democratic Party (SPÖ) and the conservative ÖVP from 1990 until 1999 and a change towards a conservative coalition (ÖVP and FPÖ) in 2000. The conservative government did not take the opportunity to introduce an obligatory ID card to improve public safety, rather just the same as the left Belgian government started from the field of e-government and did not link this to public safety. The change to another coalition government between SPÖ and ÖVP in 2006 brought back the Social Democrats into office. There was a review due of the e-government law, which raised some discussion but in the end did not lead to any significant change.

Belgium in 1999 changed from a conservative-left coalition (CVP/PSC and PS/SP) to a liberal-left coalition (VLP/PRL/FDF and PS/SP), which opened for the start of an eID initiative. In line with liberal and left politics, the modernisation of public administration became the inclusive objective. Public safety by identity control was not taken into account. But privacy-preserving features were not pursued either.

In Spain, a conservative government ruled from 1996 to 2004. Accordingly, public safety was the dominant policy field and the police directorate was the dominant actor. However, due to a lack of intra-governmental coordination of funding, the implementation was delayed and finally started by a mid-left government (PSOE) after the election in 2004.

In Germany, there was a left-green coalition from 1998, followed by a great coalition (SPD and CDU) since 2005. In contrast to the general assumption, it was a social democratic minister who put the eIDMS in the context of public safety and the fight against terrorism, while e-government was given much less attention. It is less surprising that his follower in office from the conservative CDU continued with this path.

The Influence of the IT component and e-commerce industry

Another stereotype is that the IT industry tries to influence government decisions on technology-related public procurement. Before going deeper into this, we need to distinguish between the IT industry in a more narrow sense, which produces and provides components for the eIDMS, in particular smart cards, client and middleware software, and the e-commerce industry which may apply eID-based authentication procedures.

Such an influence of the IT industry in the more narrow sense has been analyzed in particular for IT systems in military institutions, but also for large legacy systems in public administration. Against this background, one might expect that large national IT companies had tried to influence the design of the national eIDMS. From the case studies, however, we may summarize:

G 3.7 The smart card industry tries to get involved in the specification of chip cards in order to be prepared for the design and production of eID chips, but accepts the functional specification based on political preferences. They also try to adhere to or even establish international standards in order to open for other markets, but do not fight for this goal.

The smart card industry did not have a specific interest in particular attributes of an eID, but certainly has an interest to increase their returns on investment and to sell the components developed for their home market to other countries as well. For this purpose they either want the components to adhere to existing international standards or to establish newly developed components or procedures as an international standard.

This is most plausible with regard to chip producers. This industry, according to an expert interview, can be described as follows[3]:

There are four different product markets: chips for GSM/SIM cards, bank cards, public sector cards and pay TV decoder cards. National public sector chip cards include ID cards, passports, health and social security cards as well as public transport cards. For each application, chips have to be developed individually and a special production process has to be set up. The time span from a first idea to the start of mass production takes about 5 years.

There is a European Standard for a citizen card developed by CEN, but it has not been made obligatory by the European Commission. In fact, none of the tokens in the four eIDMS systems under investigation fully adheres to this standard. In Europe, there are eight different eID chips according to different national requirements. This shows that chip manufacturers did not succeed in influencing the design of an eID token in order to allow for transfer into other countries.

Most of the big multinational chip producers know and accept the role of national governments in defining requirements due to political preferences. The market in big countries such as Germany and Spain is by far large enough to pay off the development cost. Thus, in the four countries under investigation experts from the smart card industry tried to get involved in preparatory working groups, but did not try to influence the design decision.

[3] Expert interview with Dr. Detlef Houdeau, Infinion, Germany

A dialogue with the smart card industry might reduce uncertainty of technical choices. But without their own expertise, government may not be able to evaluate the recommendations by industry experts. Therefore they involve their own experts and leave it to them to include representatives from industry.

G 3.8 National governments have their own organisations with expertise on IT security, cryptology etc. and leave technical specifications to them. Depending on the existence of a national smart card industry, it is up to these organizations to enter into a dialogue with this industry.

Policy makers in government planning for a technically secure eIDMS need to build on technical expertise. In each country there is at least one state-owned organisation with expert knowledge in IT security and in particular cryptography. In Belgium, Fedict took the lead in technical specification and cooperated with ZETES, the card producer, and computer scientists from the University of Leuven. ZETES has extensive experience in the manufacturing of digital cards (e.g. SIS-card, bank cards).

In Spain the IT department of the police directorate together with the national Centre for Cryptology in the Ministry of Defence has led the specification. Consultants from IT industry were involved but did not influence the decisions taken.

As the Citizen Card in Austria is not bound to a particular token, there was no opportunity for chip manufacturers to get involved. The software architecture for the virtual Citizen Card and the sector-specific PIN was developed by computer scientists from the University of Graz.

In 2004, in Germany a working group "DIF ID Cards" (Deutsches Industrie Forum = German Industry Forum ID Cards) has been set up with Siemens, T-Systems and the Government Printing Office under the guidance of the Federal Office for IT Security to prepare for the specification of the eID card. The Federal Ministry of the Interior let the group know that Germany should have its own specification and should try to establish a European standard, which might compete with a French standard.

This strategy was successful with regard to electronic passports (EAC), but not with regard to the eID card, as several countries already had started their development processes in 2004. Furthermore, a changeover of the second generation of eID cards of Belgium or other countries to the German path was and still is very unlikely.

There is quite a different picture regarding the role of the e-commerce industry.

E-commerce faces similar security risks due to weak authentication methods as e-government. Therefore one could expect their interest in participating in any development of stronger authentication methods at national level. At the same time governments can be expected to have an interest in getting e-commerce industry involved, as e-government services alone do not create the critical mass to motivate citizens to adopt new authentication methods. However, so far private sector companies in many countries have only limited access to ID data of citizens as kept in civil registers. Although in some countries, hotels ask for the handing out of an ID card or banks ask for the presentation of an ID card for opening an account, the data on the card usually is not filed by private entities.

Against this background, the question is whether the eIDMS shall be open to e-commerce service providers in general or only under certain conditions and also whether they should be invited to participate in the development process. If not,

these providers and their associations may raise their voices and put demands into the arena. In both cases we can expect an increased complexity of the eIDMS itself and the regulation as well as increased coordination requirements in the process.

The situation in the four countries under investigation can be summarised as follows

G 3.9 The e-commerce industry and banks showed little interest during the development processes and did not try to influence the technical design nor the regulation of the eID function and the authentication process.

Belgian banks did not show any interest in the strong authentication to be provided by the eID function of the Belgian Personal Identity Card (BelPIC) during the development process. To them a bankcard serves as a credit or debit card connected with an authentication function. Several banks offer an offline TAN-generator or a similar device which serves as a reader for their bankcards. Their cards carry the brand of the bank, and the technology ties the customer to "his" bank. Therefore an eID card does not promise any advantage. When the rollout of the new card started, the e-commerce industry showed some interest in the eID-based authentication function.However, Belgian privacy law puts restrictions on the use of the unique National Registry Number (RNN) as part of the eID because it reveals the date of birth and the sex of the holder and it could therefore be used for targeted advertising. Private enterprises that want to use the RNN have to get permission by the privacy commission. So far the commission did not give permission for the use of online authentication via BelPIC. Agoria, an association of IT companies, has for some time discussed different normative or technical options for reducing privacy infringements. A normative approach would be a code of conduct to be adopted by e-commerce providers, technical solutions would either employ encryption of the ID number or the translation into a non-speaking ID.[4] The Belgian e-commerce industry, however, did not actively lobby during the development process, neither for a technical solution nor for changing the legal restriction after the introduction of the new eID card. It supported the marketing activities of the Belgian government as part of their intiatives for a more secure Internet.

In Spain the existing ID card and the personal identity code are heavily used in everyday life. There has been no discussion about restricting the use of the new eID card. The Ministry for Industry, Tourism and Commerce, which provided most of the funding for the eIDMS, did neither explicitly address this issue in the beginning nor officially consult the IT or Internet industry. As late as 2008, it launched a programme to support applications in e-commerce. So there was neither any influence on the design of the eIDMS nor on the development process.

In Austria, the cooperation of banks, some of them state-owned, was sought by government when the e-card option had failed, and bankcards were considered an appropriate token for the virtual eID card. Bank officials had not been invited to participate in the concept development and specification. Rather they had to accept the political pressure to adopt the citizen card. Most Austrian banks agreed and offered the implementation of the Citizen Card on their branded bankcard. But as the

[4] Such a transformation has been employed in Finland. See the case study by Rissanen (2010) in this issue.

function was too complex and not accepted by their customers, recently they started leaving this path, e.g. by no longer promoting the citizen card function for newly edited bankcards.

Germany to some extent is an exception from this generalisation: the eID-based authentication function has been conceived for the adoption in e-government and e-commerce from the beginning. In order to adhere to the proportionality criteria of privacy regulation and to meet security concerns of citizens/consumers regarding phishing and other forms of identity theft, the double-sided process of authentication with access certificates has been developed and laid down in the respective legislation. In so far the opening for e-commerce application led to a more complex eIDMS. However this did not influence the development process at all. E-commerce industry and banks have not been invited into the DIF working group. After specification, the eIDMS has been selected as one of the few projects, which became the subject of the annual national IT summit organised by the German Chancellery. Ebay Germany has taken formal leadership of the respective working group. There is also support for the project by BITKOM, the national IT industry association. But to our knowledge, there was no influence on the design of the eID function or on the eID card. German banks showed only limited interest in the eID-based authentication function so far.

In summary, the basic assumption in the conceptual framework is that differences in the eIDMS may be explained by differences between the interaction systems, i.e. between the instutional actors who make the choices of path continuation, change or creation. The interaction system in the four countries shows a high degree of variance with regard to the affiliation of main actors, their roles, interests, resources and strategies. The focus point to map these differences is the dominating policy field, which takes leadership of the development process, and the respective actors from the policy fields of modernisation of public sercives vs. public safety. This, in turn, depends only to a small extent on the political power structure, i.e. the values and ideologies of the ruling political parties and to an even lesser degree on actors from IT industry. Where a path creation has happened, it was related to privacy-preserving measures, with which policy makers reacted to concerns in their respective country.

Legal context, culture and values

In two of the four countries under comparison new paths have been created mainly because of privacy concerns: Austria created the Sector-Specific Pin and Germany introduced the selective access to eID data according to the certified proportionality requirements, while Belgium continued the legal restrictions of the use of the registry number and Spain did not take any action with regard to privacy. According to our conceptual framework, policy-makers act within a certain context including legal and cultural factors. Differences with regard to privacy-enhancing components of the eIDMS therefore might be explained by different privacy legislation and culture.

A second line of differences has been observed with regard to the degree to which government provides additional and supportive services, subsidises the prices for the eID function and promotes the adoption of stronger authentication on the service

provider side. This may be because of differences in the general understanding what services governments should provide and what should be left to the private sector and market-related competition, for which we use the German term "Staatsverständnis", as we could not find an appropriate English term.

Privacy legislation and culture

The development of the four eIDMS under investigation in this research took place under national privacy legislation, which has to adhere to the European Data Protection Directive of 1995 (European Council 1995). Therefore there should be no great differences in the general privacy legislation between the four countries. But a closer look at the legislative process and the role the national privacy enforcing authorities have played shows that there are differences. There are at least some indications that these general differences are related to the degree of privacy-enhancing elements of the eIDMS.

G 4.1 Countries with a stronger privacy governance in general also have established stronger privacy-preserving measures in their national eIDMS. However, differences between general privacy governance explain less than differences between the application of privacy provisions in related areas.

In Austria, Belgium and Germany there was no doubt that because the eIDMS concerns basic privacy rights, precise legal regulation is required. In Spain the Ministry of the Interior took the view that no additional data is collected compared to the previous ID card and the long-established filing of fingerprints in a central database is only extended to the new eID card and therefore no parliamentary consent was required. While Austria and Germany designed technical privacy-enhancing measures, Belgium kept the limitations of the use of the National Registry Number for the eID. If we consider the technical measures to be stronger than the legal restrictions, we can rank the four countries according to the *degree of privacy-preserving measures* as shown in the first line of Table 9.

To assess the strength of *general privacy governance* in the four countries, we may use three indicators:

(1) If the legal provisions of the eIDMS have to be established by a *law*, which has to pass parliaments, privacy governance is stronger compared to *decrees or directives,* which can be issued by government agencies without parliamentary consent.
(2) If the government agencies developing the eIDMS have to get *formal agreement* by the privacy authority and/or if this consent has to be declared to the legislator, privacy governance is stronger than the obligation for *formal consultation* or even *informal consultation.*
(3) If the privacy authority has to *grant ex ante permission* for using ID data by governments and private business, governance is stronger than *ex post control* of compliance to privacy regulations.

If we apply these three indicators to the four countries, Belgium ranks highest, followed by Austria, Germany and Spain (Table 9).

Table 9 Degree of privacy-preserving measures in eIDMS and the general privacy governance

	BE	ES	AT	GE
Degree of privacy-preserving measures in eIDMS	Legal (Rank 2)	None (Rank 3)	Legal + Technical (Rank 1)	Legal + Technical (Rank 1)
(1) eIDMS-related law passed by parliament or directive/decree	Law = 2	Decree = 1	Law = 2	Law = 2
(2) Involvement of privacy authority in legislative process	Formal agreement = 2	Formal consultation = 1	Formal consultation = 1	Informal consultation = 1
(3) Rights of privacy authority regarding the use of ID data in gov. and commerce	Grant permission = 2	None = 0	Grant Permission = 2	Ex post intervention = 1
Strength of privacy governance (1+2+3)	6 Points (Rank 1)	2 Points (Rank 4)	5 Points (Rank 2)	4 Points (Rank 3)

According to article 28 of the EU Data Protection Directive (95/46/EC), Member States shall provide that one or more public authorities are responsible for monitoring the application of the provisions according to this directive. They shall operate with complete independence. These supervisory authorities have to be consulted "when drawing up administrative measures and regulations relating to the protection of individual rights and freedom with regard to the processing of personal data".

Member States have adopted this provision differently in their national law. The German Federal Data Protection Law does not contain this obligation to consult the Data Protection Officer in a legislative process at all but gives him the right to address Federal Parliament. As the Austrian Privacy Commission is affiliated to the Chancellery, its *independence* is questioned by some observers.

In 2007, the non-governmental organisation Privacy International published a National Privacy Ranking considering such general aspects as well as the provisions or agreement to communication interception, access to medical data and other aspects based on the assessment of national correspondents. Table 10 shows the values for these indicators for the four countries under comparison.

The index of "privacy enforcement" summarizes answers of national experts to two questions:

* Is there a regulatory body with sufficient powers to investigate privacy infractions? Can this regulator act proactively?
* Does this regulator act in an effective way? Have cases been taken through the administrative and legal systems?

According to PI experts, Belgium, Spain and Germany rank highest with a value of 4,0 standing for "Significant protections and safeguards", while Austria only gets 2,0 points indicating "Systemic failure to uphold safeguards" (Privacy International 2007).

Table 10 Privacy International (PI) ranking

Privacy International surveillance indices	BE	ES	AT	GE
Privacy enforcement	4.0	4.0	2.0	4.0
Surveillance Index of PI	2.7	2.3	2.3	2.8

The overall index values in the bottom line include assessments of privacy enactment in different areas, again with Germany and Belgium evaluated quite good and showing very poor values for Austria and Spain.

Reasons given for the poor Austrian assessment include: "e-identity management system is heavily criticised, ... legal requirement permitting Austrian military to request subscriber data from telecommunications providers, ... centralisation of data on students that is stored for 60 years." And the indications for Spain include: "Several interception scandals over the years; including extensive access to communications without court order, laws for preventing funding of terrorism have been applied to other crimes, lack of debate around introduction of planned electronic ID card, retention period for 12 months, and plan to ban anonymous pre-paid mobile phones."

In a similar way, we may compare provisions in the area of civil registration, which at least may be considered as threats to privacy, such as the principle of "one authentic source" as compared to informational power sharing, a unique personal identifier and a central data base for digital fingerprints (Table 11).

According to these indicators, Belgium and Spain have each granted two privacy-critical provisions, while Austria and Germany did not take any of these risks. For the same reasons policy-makers in both countries may have taken privacy-preserving measures within their eIDMS. But we can not explain the difference between Belgium and Spain.

From these exercises, we may conclude that different indicators for legal privacy-preserving and enforcing mechanisms and their application in different areas do not show a consistent picture. While Germany is always ranked quite high and Spain ranked lowest, the ranking of Belgium varies a little bit and the one for Austria varies extremely. This may be due to the somewhat fuzzy assessment method of Privacy International and their reliance on national experts, which may apply different yardsticks.

Table 11 Granted threats to privacy in the area of civil registration and ID management

Granted threats to privacy	BE	ES	AT	GE
(1) "One authentic source" instead of informational power separation	Yes	No	No	No
(2) Unique personal identifier	Yes	Yes	No	No
(3) Digital fingerprints data base	No	Yes	No	No
No. of granted threats	2	2	0	0
Privacy protecting level	Rank 2	Rank 2	Rank 1	Rank 1

In our conceptual framework, we assume that policy-makers make their choices on path continuation or creation of new paths within a legal context, but as elected politicians also care for the concerns of their constituency. If they expect privacy concerns to be raised by the planned eIDMS, they will take care of privacy-enhancing provisions. Therefore, besides the comparison of the legal environment, we have to look at differences with regard to the privacy culture between the four countries under study.

G 4.2 Policy makers in Austria and Germany took stronger privacy-preserving measures than their colleagues in Belgium and Spain because of a a more sceptical and demanding privacy culture, which is indicated by survey data.

In June 2006, Backhouse and Halperin conducted an online survey with almost 2,000 respondents in 23 EU Member States (Germany 1,200, Austria 34, Spain 33, Belgium 26). The results are not published by country but by country groups, Austria, Germany and Scandinavia as one group, Benelux and France as a second group, South Europe another (Table 12).

Although the number of respondents is much too low to allow for any valid comparison, we may pose the hypothesis that citizens in Germany and Austria are more sceptical than people in Benelux States and that citizens in Southern Europe are even less concerned (cf. Backhouse and Halperin 2009 and the FIDIS homepage at www.fidis.net for more data). This ranking corresponds with the strengths of the privacy-enhancing measures taken in these countries as indicated in Table 9.

These data are in line with the more comprehensive data provided by the Eurobarometer survey no. 225 on data protection and the perception of European citizens (Gallup Organisation 2008), from which the authors conclude:

> "Austrian and German citizens seemed to be the most concerned about how their personal data was handled. Eighty-six percent of those respondents reported being concerned about data privacy issues, and two-thirds claimed to be *very* concerned (Austria 70%, Germany 65%)."(p.7)

The data for all four countries are display in Table 13, line (3). The same difference can be found for "citizens´ trust in privacy at public agencies" (line (1) Table 13). However, for other related items, the four countries to some extent show a

Table 12 Trust in privacy of exchange of ID data (Backhouse and Halperin 2009, pp. 258)

	AT/GE, Scan.	Benelux	South Europe
I believe that ID authorities will be truthful and honest when dealing with my data.	5.6	4.8	4.5
I believe my interests will be represented in deciding how ID data will be exchanged.	5.9	5.3	4.9
I feel comfortable for my ID data to be shared			
- across government institutions	5.3	5.0	4.2
- between government and businesses.	6.6	6.1	5.9

1 = strong agreement; 7 = strong disagreement

Table 13 Selected data from Eurobarometer no. 225 (Gallup Organisation 2008)

Privacy concerns	BE	ES	AT	GE
(1) Trust government agencies (social security, tax, local authorities) concerning data protection	80% Rank 3	80% Rank 3	71% Rank 2	69% Rank 1
(2) Level of data protection in home country—properly protected	63% Rank 4	48% Rank 2	62% Rank 3	46% Rank 1
(3) Concerns about personal data protection by private and public organisations (% of citizens)	22% Rank 4	35% Rank 3	70% Rank 1	65% Rank 2
(4) Concerns about personal data protection on the Internet	72% Rank 1	69% Rank 2	67% Rank 3	67% Rank 3

different ranking. With regard to the level of privacy protection in their country, Belgian and Austrian citizens are more satisfied than the German and Spanish respondents, which does not explain the stronger efforts in Austria compared with Spain. Similarly concerns about personal data protection in the Internet are slightly greater in Belgium and Spain while Austria and Germany took stronger action.

Stronger privacy concerns call for stronger measures, but do not tell what kind of measures are most appropriate. Austria and Germany employed technical measures to meet the privacy concerns of citizens, but they have addressed different kinds of concerns and chosen different measures accordingly. Austria addressed the concern for linking data across administrative boundaries, while Germany wanted to provide for compliance with the principle of proportionality, i.e. that service providers can get access only to those ID data which are necessary for authentication for a particular service. When looking for technical solutions actors leaned on existing organisational principles and implemented them into technical features.

G 4.3 The privacy-preserving measures are chosen on established paths of privacy arrangements in the ID environment.

The introduction of sector-specific PINs in the Austrian virtual Citizen Card concept followed the existing structure of 26 sectors in the data protection registry, where public entities and businesses have to register electronic files containing personal data. They were introduced for implementing the purpose-binding principle when the central civil register was established and were applied for the Citizen Card concept as well.

The German requirement for restricted and selected access to the eID data on the chip according to the requirements of the respective service is simply the application of existing privacy legislation and legislative tradition. German privacy law requires that public entities may only collect personal data necessary for a concrete purpose and that this data is defined in a specific law regulating this service. This is the case for hundreds of public services and laid down in respective laws and directives, including the old ID Card Act. Regulation of authentication for online access to public services in the revised eID Card Act has just been handled in this tradition drafted by a lawyer within the Federal Ministry of the Interior, who has been "borrowed" from the data protection authority of the federal state of Schleswig-Holstein. Being involved in research on user-centric identity management before, the

creative part was to carry the legal requirements into technical functionality. Although it produces some additional administrative burden, this regulation provides an answer to the security and privacy concerns of citizens and therefore could be justified very well in the legislative process. Indeed the experts interviewed confirmed that this regulation has not been questioned at any time by any participant in the legislative process.

"Staatsverständnis": Opt in or opt out

The four eIDMS under comparison also differ with regard to the modus of the authentication and the e-signature function, whether they are mandatory or optional with an opt-in or and opt-out choice. These differences may be explained by the respective understanding of policy makers which services should be provided or at least regulated by the state and what should be left to private business. Of course different political parties have different views on this, and citizens have different expectations as well. In Germany, this basic belief concerning the extent to which the state intervenes in societal processes and in particular business is called "*Staatsverständnis*". As we did not find an appropriate English translation, we use this term here, which might roughly be translated with "the accepted or expected level of state intervention". But our case studies do not corroborate this assumption completely:

G 4.4 Differences with regard to the "Staatsverständnis" did not influence the eID-based authentication function itself, but the opening for e-commerce, the provision for electronic signatures as well as the supporting provisions for components, hotlines etc.

If we apply a simple dichotomy, we can envisage a welfare state model where government takes care of secure online authentication in e-government as well as in e-commerce, provides electronic signatures in combination with eIDs provided by a state-owned Certification Authority, subsidises the CA services as well as the eID function on the eID card and provides customer support for citizens and service providers from public and private sector without any charge. In contrast, according to a liberal state model, government would only regulate the administration of citizens ID as well as the production and distribution of the eID card and perhaps enact some privacy provisions. Certainly the liberal state would not intervene into the authentication processes in e-commerce, leave electronic signatures to the market and charge cost-related fees.

Table 14 reminds us of the relevant features of the four eIDMS in this respect.

We have already seen that with regard to the relation between e-government and public safety objectives, it is not possible to relate such values and preferences to the different political parties involved, as the priorities have not changed when there were changes in government and former opposition parties took over government offices. There is no clear pattern according to which one country adheres completely to the liberal or the welfare state model. And there are no surveys or statistics available addressing these values and their distribution among citizens. Table 14 shows that Belgium comes closest to the welfare state model. But perhaps we are on the wrong track with looking for values to which policymakers respond. Whether authentication functions should be applied in e-commerce as well as in e-government may not be a

Table 14 Government´s support for different features of the eIDMS

	BE	ES	AT	GE
Authentication explicitly open for e-commerce	No	Yes	Yes	Yes
Electronic signature	Opt out	Mandatory	Mandatory	Opt in
Funding of card readers, client software etc.	Recently	Recently	No	Planned
Support hotline	Yes	Yes	Yes	Planned
Governance of e-signature	State-owned monopoly	Several CAs	One CA	Several CAs
Price for e-signature certificate	Subsidised by government	Paid by government	Free on e-card	Market price paid by citizens

question of such basic beliefs, but a question of motivating people to apply for an eID card with its authentication function at all. As it seems unlikely that people opt in for the authentication function for one or two online transactions with local as well as federal governments per year, offerings in e-commerce are needed as trigger. The more comprehensive provisions in Belgium therefore may just be the consequence of the greater influence of the e-government objectives and the ambition to make the eID as attractive to citizens as possible by low cost and additional functions.

With regard to the differences in dealing with electronic signatures, the German opt-in provision continues the path established in the signature law: it is not a task of the state to provide the means for the electronic authentication of documents. For paper-based documents there are notaries, for electronic signatures a private certification authority under state control. Although this model has not been successful regarding the diffusion of electronic signatures, there has been no initiative to leave this path.

In contrast to that, in Belgium electronic signatures have been provided by one single state-owned CA from the beginning. For the delivery on the eID card, Fedict has bought certificates for every cardholder at a dumping price. Due to the dominance of the e-government policy field, the belief that e-government needs provisions for authentication of persons and signing of forms and documents from the same card and the same provider determined the eIDMS concept.

With regard to the provision of card readers, client software and telephone hotline support, all four countries first refrained from such a service, probably not because of ideological reasons but because of budget problems, procurement law and logistical problems. But slow diffusion and complaints made them change their minds. In Germany the coincidence with a public recovery investment programme to fight the economic crisis provided funds for subsidization of a starter kit and for hotline services.

Problem-solving effectiveness

The policy field analysis according to our conceptual framework adopts an interaction as well as a problem-oriented perspective (see Scharpf 2000 and the introductory chapter by Kubicek 2010). The problem-oriented perspective looks at the emergence

of a societal problem and the effectiveness of the policy chosen to deal with this problem, in particular the creation of new or the change of existing institutions. eIDMS are new institutions, which have been created to handle the societal problem of lack of security of transactions in the Internet, which in turn are perceived as barriers to full exploitation of the high potential of the Internet for economic growth and societal progress (i.e. the "information society"), as maintained by the eEurope Action Plan 2002 (European Council 2000) The concrete socio-technical solution developed is a stronger authentication function on eID cards. There is no doubt that an eID-based authentication is technically more secure than a user name and password and that a gain in convenience is to be observed if users do not have to memorise several different passwords and run the risk of identity theft. But do citizens recognise and appreciate these gains and is the eID function in technical terms an appropriate and effective solution to the problem as perceived by citizens?

In this section we will first look at the diffusion and usage of the eID function, discuss the effectiveness of the solution for solving security problems as well as the status of e-government as the initial policy field.

Diffusion and usage of eIDs

As shown in Table 1, the eID function for online authentication in the four countries under comparison is offered on different grounds:

- In Belgium it is provided on an opt-out basis with the new eID card for citizens older than 11 years.
- In Spain it is mandatory on the new eID card, issued to citizens aged 14 years or older.
- In Austria every citizen can apply for a Citizen Card implemented on a social security card (e-card) or bankcard.
- In Germany citizens beyond the age of 16 will have to opt in, when applying for a new ID card.

Thus the number of eID cards, except for Spain, differs from the number of eID functions issued, and the diffusion of eIDs does not tell anything about their use for online authentication. From the four country studies we have learned that usage is extremely low.

G 5.1 Despite the differences between the eIDMS, the use of the eID-based online authentication function is extremely low. For example for online tax declarations, the share of online authentication by eID is less than 10%.

To compare usage patterns, we have collected data on electronic tax returns, which are one of the most heavily used online e-government services in the four countries. Table 15 depicts the rollout of eID cards, the activation of the eID-based authentication function, the percentage of taxpayers providing electronic tax returns and the percentage of those who use the eID for authentication, which was only about 7% in Belgium, 0,2% in Spain and 1,0% in Austria in summer 2009.

These differences cannot be explained by different features of the eIDs and eIDMS. The higher rate of use of the eID function in Belgium is probably due to the longer rollout period and higher diffusion rate of eIDs. It may well be that the four eIDMS, despite the differences we have highlighted so far, share some common

Table 15 Rollout of eID cards and use of the eID function

	BE	ES	AT
State of rollout early in 2009	9.3 million, 90% of the Belgians entitled to an ID card	8 million, 25% of the Spaniards entitled to an ID card	8.4 million e-cards, 100% of all citizens
eID function activated	7.5 million = 80%	not necessary	approx. 74,000, (0,9%), thereof approx. 20,000 office ID cards
Use rate for electronic income tax	2008: 24% 2009: 56%	21%	25.7%
eID use rate for income tax (% of electronic apps.)	2008: 3.6% 2009: 14.2% (half of them by service on site of tax office)	2008: 0.1% 2009: 0,2%	2008: 0,7% 2009: 1,0%

features which are more important than the differences. In our conceptual framework, we have included Rogers´ theory of the diffusion of innovations (Rogers 2003) and assumed that the eID-based authentication function might meet the same barriers to diffusion which electronic signatures have failed to overcome (Fraunhofer Institute FOKUS 2006). According to Rogers, the rate of adoption is higher for innovations which offer a clear relative advantage, are compatible with past experiences and with the needs of potential adopters, which are triable and observable, but which are not too complex and do not afford new skills.

G 5.2 All four eIDMS under investigation, despite their big differences, share the barriers to diffusion as mentioned by Rogers:

- They are not compatible with established values and procedures.
- The technical process of authentication is complex and not easily understood.
- The relative advantage of higher security is not visible and not observable.
- The technical components are not easy to install and easy to use.

Usability and interoperability may be improved in the future, but the missing "*relative advantage*" is a more deeply rooted problem, which is not only a matter of perception. Relative advantage is a matter of effectiveness of a solution and a question of balancing cost and benefits. From media research we know that media selection in most cases is not based on rational choices only and that media behaviour is a very conservative or in other words habitualised behaviour. Changes only occur if problems have been experienced, if other options promise much greater gratification or if peers adopt a new medium.

G 5.3 As long as previous modes of authentication are still offered, there is no incentive for users to change to a more secure eID-based option, as this requires additional financial investment and a change of habits.

The main reason for low usage is that all previous modes of authentication are still offered, e.g. by tax authorities as well as for online banking. As citizens have not encountered any security or privacy problems with the tax offices personally and as there were no security scandals reported in the mass media with regard to these services either, citizens do not have any reason to change an established pattern of use.

The effectiveness of the eID-based solution to security concerns

Our assumption so far was that the eID function solves the security problems, which policy-makers wanted to solve. Their main objective was to increase the volume of transactions over the Internet for the sake of economic growth. The first assumption in looking for a solution was that most of all security concerns keep people from performing online transactions. The second assumption was that stronger authentication methods can reduce these security risks. So far both assumptions have not been questioned. There are no comprehensive and valid data to check both assumptions. However an OECD background paper, "Measuring Security and Trust in the Online Environment: A View Using Official Data" (OECD 2008), gives some hints. The working party regrets that in contrast to the significance of the perception of security and privacy of online services there are no reliable and comparable statistics in the Member States. From available statistics they conclude, "that in general privacy or security concerns are not an important reason for not having Internet access at home". The most important barriers in 2000 were "lack of interest, lack of money and lack of skills" (p. 9). However, there are national differences with regard to privacy or security concerns (p. 10).

The security or safety concerns of citizens according to surveys relate to phishing attacks, mistrust in service providers regarding the delivery of goods and services or handling complaints (Table 16). The most frequent personal experience relates to the abuse of personal data, fraudulent payment and unsatisfactory responses to complaints. The Eurobarometer data on privacy concerns also show that almost two thirds of the respondents in all for countries are concerned about personal data protection on the Internet (Spain 72%, Belgium 69%, Austria and Germany 67%) and that there is little trust in mail order companies. Only 21% in Belgium, 14% in Spain and 18% in Austria and Germany say that they trust data privacy protection by mail order companies (Gallup Organisation 2008).

With regard to the second assumption, there is no doubt that stronger authentication provides for a higher degree of security. But the question is "*For whom*?" The three one-sided authentication processes established in Belgium, Spain and Austria do not provide a solution to these problems. They do neither protect from phishing attacks nor do they provide for more trust or more certainty regarding complaints. They only allow for more safety for service providers with regard to the identity of their customers. In other words, citizens/consumers are expected to make investments to increase the safety of service providers. Only the access certification of providers in the German eIDMS offers clear safety benefits to the citizens/consumers as well. This may well explain the low usage rate.

G 5.4 eIDMS with a one-sided authentication function do not provide a solution for security/safety and privacy concerns of citizens but increase the safety

Table 16 Safety and security oncerns in the online environment (OECD 2008)

	BE	ES	AT	GE
Security concerns for not buying/ordering goods online (% of Internet users)	–	70%	20%	27%
Privacy concerns ...	–	60%	18%	23%
Trust concerns and complaints	18%	17%	10%	20%
Internet users victim				
- of abuse of personal information (% users)	–	15%	2%	2%
- of fraudulent payment (% of Internet users)	–	1%	1%	1%
- % of those who ordered goods	–	7%	4%	–
Security problems encountered	1%	2%	1%	1%
Unsatisfactory response to complaints	1%	7%	2%	6%

of service providers. They do not offer a relative advantage to citizens and show an asymmetric distribution of cost and benefits where users have to invest to increase the benefits of service providers.

The asymmetric distribution of cost and benefits of eID functions is the same as for electronic signatures. But would a change to a double-sided authentication process alone change the situation? This is not very likely because in particular those services, which raise problems of trust, would have to offer the double-sided authentication processes. Not the federal agencies, the local municipalities, the Ebays and Amazons are the subject of concerns, but the service providers with unknown names. Could they be forced to offer eID-based authentication? Can consumers force them by exit?[5]

G 5.5 There is a vicious circle: As long as existing methods of authentication are offered in parallel, there is no need to adopt eID based authentication. However, providers of frequently used e-government services cannot close other ways of authentication as long as not all potential users have installed the equipment for the eID based mode auf authentication and are ready to use it.

By selecting a new eID card as token for the eID function, policy makers accepted a rollout period of five to 10 years until every citizen is equipped with the new token and before other methods of authentication can be closed. But even where the rollout is completed, as in Belgium, the weaker methods of authentication are still offered, even by other federal agencies. This raises questions concerning the power of e-government actors and the structure of this policy field.

Preliminary conclusions and outlook

In this final section we will summarize the policy field analysis, draw some conclusions in this respect and provide a preliminary answer to the two research

[5] Diffusion and adaption was not the main focus of this research. To do more thorough analysis, a different research design would be necessary. To take such a closer look may well be the objective of a follow-up project.

questions at the outset of this project. These answers are qualified as preliminary, as there will be a second phase of analysis by looking at four other cases in this special issue, selected by a "most different design". Only after this second step we may dare a grounded theory on the path dependency of European eIDMS.

Policy field analysis of e-government and Internet security

When introducing the problem-oriented perspective of policy field analysis, Scharpf mentioned the problem that political scientists in most cases cannot judge by themselves whether a solution chosen by policy makers is an appropriate and effective answer to the problem they wanted to address (Scharpf 2000). In our case this depends on the definition of the problem. If we define the problem as "weak authentication for online" services, stronger authentication by eIDs is an appropriate response. If we define the problem as security and privacy concerns of citizens, which make them refrain from online transactions in e-government and e-commerce, we have to maintain that a one-sided authentication is no effective response, regardless how strong the authentication method is. If we define the policy problem as underutilisation of the Internet because of security and privacy concerns, we have to consider whether security concerns are indeed the strongest barrier to online transactions or at least among the top barriers. Policy makers in three of the four countries under study followed the advice of technical security experts who reduced problems of safety and security on issues of encryption and certificates, while the concerns of citizens regard issues of trust in remote service providers. But trust is a complex phenomenon and there are no recipes to create a trustful environment in the social sense. While *a trusted environment* in *the technical sense* can be established via a PKI infrastructure, we do not know how to develop a climate or culture of trust within a certain socio-ecomic context or environment.

G 6.1 An eIDMS is no appropriate and no effective response to security and safety concerns of citizen in relation to e-government and e-commerce. Policy makers following the advice of technical experts reduced the societal problem to a partial technical problem.

Coming back to e-government as the policy field where the initiatives for eIDs started, it seems that within this field, technical aspects of security gained more attention and weight than the modernisation of public services. Picking up the discussion of different "strategies of modernizing the state" by Margetts and Hood (2010), we can argue that establishing an eIDMS emphasises *technical integration* and *interconnectedness* by technological development, but to a much lesser degree considers *economic efficiency*. In the case of the eIDM, the temptation to reduce the problem of trust to technical security features was particularly great where the policy field of public safety and police gained leadership, in which the security of ID cards is a crucial issue which never has been subject to economic efficiency considerations.

In addition policy makers from the e-government field were not able to get all federal agencies and local municipalities to favour the eID-based authentication and to close the less secure ones. This is due to the *structure of the e-government policy field*. National governments who have successfully introduced an eIDMS are only in charge of a few e-government services dedicated to citizens. Most of the public services selected by

the Council of Ministers for e-government benchmarking are offered by offices at the state, regional, provincial or local level. These units are quite autonomous with regard to which services they offer online and which authentication method they make use of. What national governments can do is to regulate the eID as a tool but not the larger eIDMS including the areas of its application.

G 6.2 The introduction of more secure online authentication via an eIDMS was an element in national e-government plans. But these plans are quite different from plans and roadmaps in other policy fields. They are just a compilation of a number of projects and do not have the support of the most important policy actors for implementation.

The introduction of stronger authentication in e-government may well be in the interest of e-government actors as there is a need by governmental agencies to authenticate the citizens applying for certain services. Therefore the development of the eIDMS has been conceived as a cross-cutting project within national e-government programmes. However the eIDMS has to be placed in a larger e-government landscape including those services where the authentication function has to be applied. But this is where the policy approach has failed. As mentioned in G 5.2.2., there is a vicious circle, which might be overcome by a more comprehensive strategy of modernising the delivery of public services. The low take-up of eID functions in general has to be assessed in connection with a slow-down in progress of e-government services in general. The dispersed distribution of authority between different levels of government concerning the question of which public services are offered online and what kind of authentication is required creates a structural barrier to the employment of the eID. There is not much to gain for local governments by changing their existing procedures.

Therefore either a legal obligation to adopt stronger authentication methods for at least certain public online services and/or financial incentives would be necessary to get out of the vicious circle. But so far national governments did not even succeed in making eID-based authentication mandatory for the public online services at the national level. The only exception is the My-file-service in Belgium. It seems that e-government is not even a policy field of high priority at the national level.

Answering the research questions

Starting from the observation that concerns about the security of online transactions are a barrier for many people to use e-government and e-commerce services, stronger methods of authentication have been considered as a solution. The policy response was the introduction of eID-based authentication methods and the establishment of a national eIDMS. Such systems raised sometimes many, sometimes only a few or none privacy concerns in the Member States of the European Union and beyond. In addition it was expected at least by some observers that eIDs would fundamentally change the relation between citizens and state. Recognizing that there are significant differences between the eIDMS established in the Member States, the research project aimed at answering two questions:

- How can these differences be described and explained?
- To which extent do these systems change the citizen-state relationship?

The comparative analysis for four selected countries has shown that most of the differences can be explained by previously existing differences between the national ID-related administrative systems. Regarding organisational and regulatory aspects, the changes were incremental rather than radical. They either continued existing patterns or transposed them into the digital world. A high degree of path continuity could be stated for the ID-based online authentication. This finding provides an answer to the second research question as well:

G 6.3 In contrast to expectations and fears that eID might change the relation between the citizens and the state in the virtual world or even beyond in the physical world, the range and degree of changes and effects in the four countries analysed so far is still very modest and will probably be so for at least another 10 years. When a newly inroduced eID card is chosen as token for the eID, by most citizens it is still considered and used as a means for interpersonal authentication as was the previous eID card, now only with a chip.

But this is a preliminary statement because of the selection of the four case studies: The four countries under investigation have been selected because all of them already had an established ID management system with an obligation to register, a central registry, a regulation on holding a national ID document. The introduction of an eID did not change these basic conditions. However, if the introduction of an online authentication becomes an occasion for or is combined with introducing more fundamental obligations to register or to hold certain ID documents, we have to deal with a *radical innovation*. This is the case in the UK. Therefore the hypotheses developed here do not apply to the UK. However, we also have to recognise that the British literature on eID takes a particular view, which is not representative for the rest of Europe.

There is a second reason why the eID function has not changed the citizen-government relation, and this is due to a *misconception of this function* by those expecting this change. In the discussion about the conflict between security and privacy and the potential changes in the citizen-state relationship, which has been addressed in the introductory paper (Kubicek 2010), the different meanings and contexts of eIDs are not clearly separated and thereby cause misunderstandings. The present analysis deals with eID-based *online authentication*. This is an element of the *front offices* of e-government. Much of the concerns, however, regard the exchange of personal data of citizens *between different back offices* in public administration. As shown in Fig. 1 in the introduction (Kubicek 2010), this data comes from diverse sources, from paper-based forms, from other back offices and only to a small degree via online services and even less via eID-based online authentication. More importantly, eID-based online authentication does not change the kind and frequency of data exchange between back offices. Only the Austrian eIDMS via Sector-Specific PINs tries to reduce this risk.

In a previous, unpublished study, the Institute for Information Management Bremen lead by the senior author of this paper has analyzed the exchange of person-related data between 16 sectors of public administration in Germany in order to assess eventual problems with the identification of citizens in the different databases and legacy systems. Name, date of birth and sometimes address were considered by

representatives of these offices to allow for sufficient identification. There were problems regarding the update of changes and the data assigned to these persons, but no demands, for example, to introduce a unique identifier. The analysis showed that there is a complex network of exchange of person-related data between the agencies, entitled by several laws and directives, and that there are no technical means to prevent surpassing these legal limitations. In other words:

G. 6.4 Privacy concerns addressing the exchange of person-related data between different government back offices are without any doubt justified, but they are not influenced by the eIDMS for online authentication in the front offices. Rather front office and back office processes are quite independent with regard to privacy intrusion and provisions.

This is also the case for privacy concerns regarding the use of eID cards for visual inspection at border controls, including biometric data. Data are transmitted between different police and customs offices between different countries in a non-transparent way. However, this process has started with the previous machine-readable ID cards, is extended with electronic passports and will be further supported by eID cards. But the respective functions of the ID card differ from the online authentication and more important: again it is the exchange between the different back office systems, which has to be addressed.

So one additional contribution of this research to the discussion about electronic identity beyond the empirical analysis of one partial area may lie in distinguishing different domains and diverting attention from the front office applications of electronic identities to the identity-related data exchange between back offices in the context of public services in general and border control in particular.

Reflecting the research approach

Because the four countries analysed so far cannot be considered to be representative, there is a need for extending the sample. There are no criteria for the representativeness of countries with regard to ID systems or eID systems. But it is obvious that Scandinavian and Eastern European countries are missing. Therefore in a second and final step of this project, experts in Denmark, Estonia, Finland and Sweden have been asked to summarise the development in their countries and to review the generalisations developed here and to assess to which degree they apply to the processes in their country or which modifications are necessary to get hold of differences which have occurred there. These cases will be presented in the following sections of this Special Issue (see Hoff and Hoff 2010; Grönlund 2010; Martens 2010; Rissanen 2010). Only after including these cases in a more comprehensive comparison, we may evaluate the fruitfulness of our research approach and the conceptual framework.

With regard to the fruitfulness of the research approach and the conceptual framework, however, a few conclusions may be drawn already. The combination of an institutional actors perspective with path analysis has allowed for plausible explanations of differences between the four eIDMS. The differences identified with regard to technical, organisational and regulatory aspects prove that there is no technological determinism and support the Social Shaping of Technology School's

basic assumption that technical choices exist, even if we are not able to explain any detail of the outcome of these choices right now.

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

Backhouse J, Halperin R. Approaching interoperability for identity management systems. In: Rannenberg K, Royer D, Deuker A, editors. Identity in the information society: challenges and opportunities. Dordrecht: Springer; 2009. p. 245–68.

Bender J, Kügler D, Margraf M, Naumann I. Sicherheitsmechanismen für kontaktlose Chips im deutschen elektronischen Personalausweis. Datenschutz und Datensicherheit. 2008;32:173–7.

Cap Gemini. Online Availability of Public Services. How Is Europe Progressing? Report of the Fifth Measurement. October 2004. Prepared for European Commission, Directorate General for Infomation Society and Media, March 2005.

Commission of the European Communities. eEurope Benchmarking Report eEurope 2002. Communication (2002) 62 final, Brussels 5.2. 2002.

Council of the European Union, Commission of The European Communities. eEurope 2002. An Information Society for All. Action Plan, Brussels 14. 6. 2000.

European Council. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Official Journal of the European Communities 1995, No L 281/31–39.

European Council. Council Regulation No 2252/2004: on standards for security features and biometrics in passports and travel documents issued by Member States. 2004.

Fraunhofer Institute FOKUS. Study PKI and Certificate Usage in Europe 2006. 2006.

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. http://www.ec.europa.eu/public_opinion/flash/fl_225_en.pdf Brussels 2008, accessed Feb. 28 2010.

Glaser BG, Strauss AL. The discovery of grounded theory. Strategies for qualitative research. Chicago: Sociology; 1967.

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

Margetts H, Hood C. Paradoxes of modernization: unintended consequences of public reform. Oxford: University Press; 2010.

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

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

OECD. Measuring security and trust in the online environment: a view using official data. Paris; 2008.
Ouchi WG. Markets, bureaucracies and clans. Administration Quarterly. 1980;25:129–41.
Privacy International. Leading Surveillance Societies in the EU and the World 2007. The 2007 International Privacy Ranking. 2007. http://www.privacyinternational.org/survey/rankings2007/phrcomp_sort.pdf. Accessed 20 Jan 2010.
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. Free Press; 2003.
Scharpf FW. Institutions in comparative policy research. Comp Polit Stud. 2000;33(67):762–90.
Witte E. Organisation von Innovationsentscheidungen. Das Promotorenmodell. Goettingen: Schwartz; 1973.