IDIS (2010) 3:5–26
DOI 10.1007/s12394-010-0052-0

Introduction: conceptual framework and research design for a comparative analysis of national eID Management Systems in selected European countries

Herbert Kubicek

Received: 23 October 2009 / Accepted: 9 March 2010 / Published online: 14 April 2010

Abstract This paper introduces the objectives and basic approach of a collaborative comparative research project on the introduction of national electronic Identity Management Systems (eIDMS) in Member States of the European Union. Altogether eight country case studies have been produced in two waves by researchers in the respective countries, which will be presented in the following articles in this special issue. The studies adopt a common conceptual framework and use the same terminology, which will be presented in this introduction, just as the reasoning for the selection of the particular countries under investigation. The conceptual framework combines elements of actor centred institutionalism with path analysis, looking for path continuation, change or creation in the transition from the previous IDMS to an electronic one and explaining this as choices of actors in certain contexts. Information on the reasons for these choices in the first four cases has been collected from in depth interviews with key actors and in the four other cases from official documents. As the subject of this research is the transition of national identity management systems only countries have been included in which a national ID and a civil registry already exist before the introduction of the electronic elements, thus excluding the UK.

Keywords Comparative research · Diffusion of innovations · eCommerce · eGovernment · electronic Identity Management Systems (eIDMS) · ID Cards · Institutionalism · Path dependency · Privacy and security · Social shaping of technology

Electronic identities as a multi-facet innovation

Since the Internet and in particular e-mail and the World Wide Web have been adopted as means of information and communication in business, government and

The research presented has been funded by the independent Volkswagen Foundation, Germany

H. Kubicek (✉)
Applied Computer Science Institute for Information Management Bremen (ifib),
University of Bremen, Bremen, Germany
e-mail: kubicek@ifib.de

leisure time, there has been a discussion about electronic, digital or cyber identity. In fact there are several debates, partly overlapping, but also quite distinct, covering different areas of action and starting from different values and norms (cf. Hornung 2005; Bennett and Lyon 2008; Halperin and Backhouse 2008; Rannenberg et al. 2009). One prominent discourse was and still is about *cyber identity*. While in real life people are assumed to have one single identity, but may stay anonymous in many everyday transactions, for e-mail or in online discussion for a they have to take an identity, but remain free to choose different identities in different contexts without being considered schizophrenic or committing fraud. Instead, the possibilities of taking different identities also called *partial identities*, is appreciated as a new dimension of individual freedom and as a means to avoid the matching of personal data recorded in different contexts.

Different requirements in different contexts

What works well in one area of the virtual world causes problems and concerns in others. As applications for electronic business and government services emerged and legally binding transactions began to be offered, the free choice and change of digital or electronic identities became unacceptable in many cases. While in eCommerce vendors most of all want to be sure that they get paid for their delivery of goods and services and may not care whether the user name provided is the officially registered name, the buyer wants to know the legal identity of the vendor to claim his rights if the vendor does not deliver or if there are other complaints. With regard to public online services in most cases there is the legal requirement to identify oneself with the registered name in order to qualify for benefits or services.

Different levels of security

There are different methods and technologies for identifying users in online transactions with different degrees of security. In all Member States of the European Union online access is protected by username and password or PIN code for almost all eGovernment and eCommerce services. All experts agree that this is a rather weak level of protection not only because passwords can be hacked but also because of successful cases of identity theft, in particular phishing (see OECD 2009). Security levels are distinguished according to the number of factors employed for authentication. One-factor-methods require either something one knows (e.g. password) or something one has (e.g. a token such as a chip card). Two-factor-methods, also called "*strong authentication*", require the combination of elements of both kinds (possession and knowledge) (e.g. OECD 2006). Apart from the number of factors, the reliability of the *registration process* is another important parameter. Attributes which are connected to an officially registered and confirmed identity provide for a higher level of security than individually defined identities.

For *online banking*, where the motivation for identity theft is highest, so far there are only a few solutions for strong authentication procedures, such as one-time-password generators. However, concerns regarding the security and financial risks of online transactions create a significant barrier for citizens/consumers to using online services. Accordingly more secure, "stronger" methods of authentication are considered to raise

trust and confidence and thereby to overcome these barriers.[1] Officially certified and secure electronic identities may serve this purpose. A *PIN-protected smartcard*, based on the officially registered identity, would meet these requirements and might increase trust in the security of online transactions in eGovernment and eCommerce.

Conflicts between security and privacy requirements

In the late 1990s this kind of considerations in many countries has led governments to consider introducing national electronic *Identity Management Systems (eIDMS)*, in many cases based on the officially registered national identity of their citizens. However, if the electronic identity (eID) required for online authentication is the officially registered identity and if several different eGovernment services are accessed by the same eID, the personal data related to this identity in different sectors could be merged and profiles could be generated, something which was not possible before or at least only with extraordinary efforts. This would not be in line with existing privacy legislation, which in the EU Member States requires that only data necessary for a particular service can be collected and that these data may only be used for this specific purpose, but not for any other. Therefore eIDs raise issues of privacy and must be regulated in accordance with privacy legislation.

So there is the paradox situation that eID can contribute to *security* and at the same time may become a threat to *privacy* (see also Halperin and Backhouse 2008). Taylor et al. (2009), in addition, point to a third aspect, which may play a role in citizens´ or users´ choice to accept stronger methods of authentication: *the improvement of public services and convenience*. A single chip card for authentication in different online services relieves from remembering and searching the right password and failing in log-ins.

The conflict between security and privacy requirements is not insurmountable. It is not a zero-sum game (Halperin and Backhouse 2008). Rather there are technical and organisational means to preserve privacy in eIDMS. Several research projects are devoted to *privacy enhancing identity management*.[2] However, most of this research deals with *individual* identity management ("How do I manage my different identities including pseudonyms?") or with identity management within *organisations* ("How do organisations define and administer the different partial identities of their members, including user-centric provisions?"). There is not much discretion for similar features with regard to official identities of citizens on the *national level*. In particular *pseudonyms* are not an option for officially registered identities in this context, even though *partial identities* may be.

A few countries have taken measures to preserve privacy within their national eIDMS. This may be due to the extent to which this conflict is perceived by the respective national legislator and the general public. Although the EU privacy directive has been adopted by all Member States and been transposed into national law, there are *big differences*, e.g.

[1] For example 69% of bank customers in an international online survey would like to see their bank offering stronger authentication methods than username and PIN. See https://www.info-point-security.com/security-themen/identity/952-rsaemc-ergebnisse-der-jaehrlichen-qfraudq-studie-veroeffentlicht-.html?date=2009-02-01

[2] In particular the PRIME Project (Privacy and Identity Management in Europe) https://www.prime-project.eu/ e.g. Hansen et al (2004) and the recommendations of the FIFDIS project http://www.fidis.net, in particular the recommendations by Cameron et al. (2009)

regarding the above mentioned principle of purpose bounded collection and processing of personal data. According to Article 6 of the Privacy Directive, Member States shall provide that personal data have to be "*collected for specific, explicit and legitimate purposes and not further processed in a way incompatible with those purposes*." [3] While Austria has developed a complex system of *sector specific partial eIDs* to adhere to this principle in eGovernment, Belgium with its eGovernment legislation has introduced the principle of the *single authentic data source*, also called the Ask-Only-Once-Principle. Citizens may only be asked once for specific data, which have to be stored and kept by one responsible agency; no other agency is allowed to collect the same data again, but has to access the single authentic source, if it is entitled by law.[4] In those countries, which have a *unique personal identity number* for each citizen there was almost no concern about merging data from different areas of public administration when introducing electronic identities. By contrast, countries like the United Kingdom which have no obligation for citizens to register and to keep an identifying document, have seen strong political protests, when trying to introduce such an obligation just to improve security and legal commitment in online transactions (cf. the chapters in Part 3 of Bennett and Lyon 2008 as well as Backhouse and Halperin 2009).

Links to public safety issues

There is another aspect which adds to the *complexity* of the issue: The debate about electronic identity in eGovernment and eCommerce as well as their linking to officially registered identities took place at a time when there was also a debate about *improving the security of existing ID documents*, in particular after September 11, 2001, in order to fight terrorism and/or illegal immigration. Electronic identity cards with a chip and biometric data were introduced in a few Member States of the European Union for the purpose of *stronger visual and/or physical authentication* at national borders and for inspection by the police. Some data on the same chip may be used for authentication in online transactions as well. Although the *biometric data* on an eID card may and cannot be used for authentication in online services, the fact that they are stored on the same smartcard links the *online security debate* with a *public safety debate* and thereby with the privacy concerns about the collection of biometric data and other intrusions into privacy. Once again there are big differences among the EU Member States: While Germany, Portugal and Spain include biometric data on their new eID cards, Austria and Belgium refused to do so and explicitly separate the online security measures from the public safety issues.

Objectives of a comparative research project

Considering the efforts of the European Union to provide for improved mobility for its citizens through *interoperability of national eIDMS*[5], these differences have to be

[3] Directive 95/46/EC (Directive on protection of individuals with regard to the processing of personal data and on the free movement of such data) http://ec.europa.eu/justice_home/fsj/privacy/law/index_en.htm
[4] For details see the Belgian case study by Mariën and Van Audenhove (2010).
[5] In particular through the STORK project (Secure Identity Across Borders Linked). See http://www.eid-stork.eu

addressed and therefore have to be assessed, analysed and understood. This calls for comparative analysis and scientifically valid explanations.

Furthermore there is another important research question: besides the more specific discussion about privacy, security and convenience outlined so far, in the academic world there is a more general, fundamental, and partly philosophical debate about the nature of human identity and about *changes of identities in the so-called information society* (see Rannenberg et al. 2009 as well as the previous issues of this Journal). Some authors argue that the Internet ("cyberspace") and the identities people assume there have become more relevant than the officially registered ones. Others argue that online authentication with one official identity which is also registered when crossing a national border provides for a *new level of surveillance* and therefore fundamentally changes *the relation between the citizen and the state* (e.g. Bennett and Lyon 2008). There are many unproven assumptions and premature generalizations in this debate, which should be subject to empirical inspection as well.

When in 2005 in Germany the replacement of the machine-readable paper-based identity card by an electronic chip card with biometric features was decided and an additional electronic identity function for online transactions was proposed, the idea arose for a comparative research project. This project should help to *understand the differences between the national eIDMS in other European countries* and *assess the scope and magnitude of changes in the citizen-government relation*. In addition, as a practical side effect and benefit, the project should take the chance to learn from those countries, which already had started introducing their national eIDMS. The independent Volkswagen Foundation[6] provided a grant for this research in its research programme on *Innovation Processes in Economy and Society.*

Defining the object of research and basic definitions

The term eID is used in different contexts with different meanings. There is not only the difference between personal, organisational and national eIDMS, but also the different parts and functions of such a system have also to be addressed; so there is a need to define the different elements which constitute an eIDMS.

For a clarification of the basic terms, we adopt the definitions of a *Study on Identity Management in eGovernment* launched by the European Commission, which has proposed a "Common Terminological Framework for Interoperable Electronic Identity Management" (Modinis Study 2005).[7] It starts from the concept of an *entity*, which may be a person, a company or even a computer: "An entity is anyone (natural or legal person) or anything that shall be characterized through the measurement of attributes."[8]

[6] See http://www.volkswagenstiftung.de/index.html?L=1

[7] Modinis is a programme by the European Commission providing financial support for the implementation of the *e*Europe 2005 Action Plan with the objectives of monitoring and comparing performance, dissemination of good practices and improvement of network and information security. (http://ec.europa.eu/information_society/eeurope/2005/all_about/modinis/index_en.htm). Among the studies funded within this programme is one on identity management in eGovernment, lead by the University of Leuven.

[8] See also Appendix D2 in Rannenberg et al. (2009, pp. 501) and the similar definitions by the OECD (2006, p. 21).

- The *identity* of an entity is defined as "the dynamic collection of all of the entity's attributes".
- An entity has only one identity, but it may have *several digital identities*.
- "A digital identity is a partial identity in an electronic form." It is a *subset of attributes*.
- "An attribute is a distinct, measurable, physical or abstract named property belonging to an entity."
- Certain attributes serve as *identifiers*:
- "An identifier is an attribute or set of attributes of an entity which uniquely identifies the entity within a certain context." (Modinis Study 2005)

We will use "*electronic*" identity (eID) synonymously with "*digital*" identity as defined here.

Focus on online authentication

Some of the benefits and concerns mentioned above only occur in certain contexts and not in others. Therefore it is important to define those *functions* and their *contexts*, which are subject of the research presented here. From the definitions above it is not necessarily clear what the adjective "electronic" refers to. Is an "electronic identity" an *identity, which is represented by electronic means* and/or *readable by electronic devices*, i.e. a number or letters stored on an electronic chip or printed in a machine-readable code on a piece of paper? Or does the adjective refer to a *field of application*, i.e. electronic services? In other words, is "electronic" an *attribute of a token* or of *the data* stored for identifying persons, or both? Depending on which interpretation we choose, we enter quite different contexts (Fig. 1).

If we look at *identity data in electronic systems*, they are entered from paper-based forms or by electronic exchange between back-office systems and only to a small extent via transmission from an electronic identity card (left box in Fig. 1). In

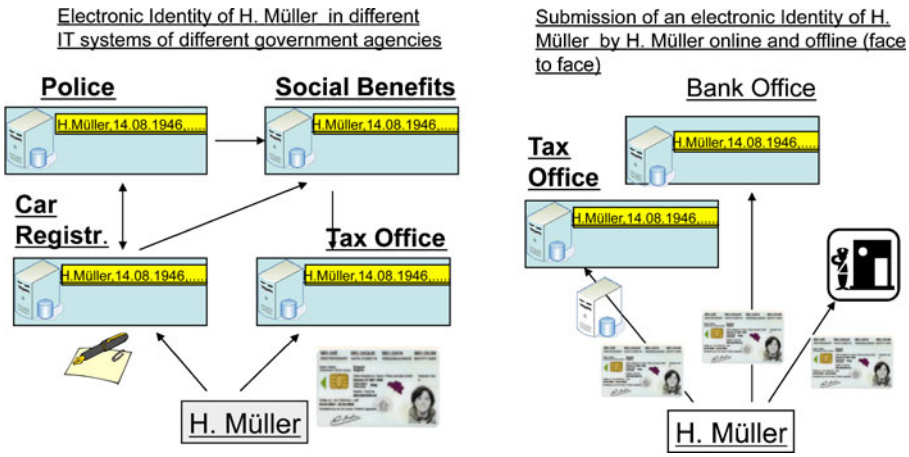

Fig. 1 Two meanings and contexts of eID

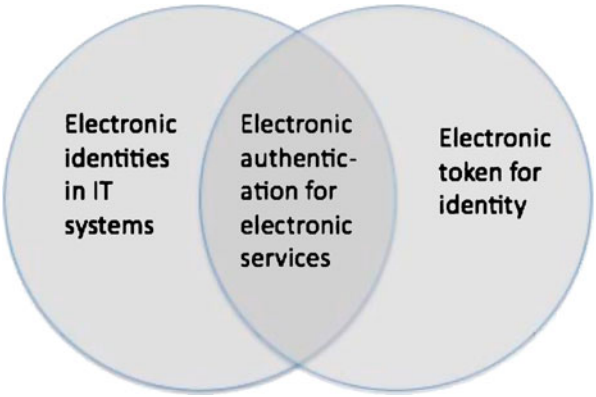

Fig. 2 Focus of this research

this context, the eID card only changes one entry channel among others, while the crucial question concerns the kind of data used for identifying citizens in different administrative systems and the regulation of the exchange of such data. Introducing an eID card does not necessarily change the back office identification and data exchange procedures, but raises corresponding concerns.

If we start from an *eID card as a new electronic token* which substitutes previous paper-based ID cards (right box in Fig. 1), we also have to take into account visual inspection of persons and checks on the authenticity of the card itself. In this context, the inclusion of biometric attributes (face image, fingerprints) on the eID card becomes an issue with contested consequences, while so far biometrics have not yet become relevant for authentication in online services.

For the research presented here, we are only looking at the overlap between the two views, i.e. the introduction of an electronic identity on an electronic token for electronic authentication designed for the online usage of electronic services (Fig. 2).

Terminology

Identification has been defined as “the process of using claimed or observed attributes of an entity to deduce who the entity is." Identification has to be distinguished from authentication and both from authorization as well as registration (cf. Modinis Study 2005, p. 10).

- "*Authentication* is the corroboration of a claimed set of attributes or facts with a specified or understood level of confidence". Authentication may refer to data or to an entity. "Entity authentication is the corroboration of the claimed identity of an entity and a set of its observed attributes" (ibid. p.7).
- "*Authorization* refers to (1) the permission of an authenticated entity to perform a defined action or to use a defined service/resource, (2) the process of determining by evaluation of applicable permissions whether an authenticated entity is allowed to have access to a particular resource" (ibid. p.8).

- "A *token* is any hardware or software that contains credentials related to attributes. Tokens may take any form, ranging from a digital data set to smart cards or mobile phones. Tokens can be used for both data/entity authentication (authentication tokens) and authorisation purposes (authorisation tokens)" (ibid. p.15).
- "*Registration* of an entity is the process in which the entity is identified and/or other attributes are corroborated. As a result of the registration, a partial identity is assigned to the entity for a certain context. In other words, the registration of an entity is the process of linking a (partial) identity to the identity of the entity by corroborating a specific set of attributes, which do not necessarily need to include identifiers. Successful completion of the registration procedures results in the granting of a means (e.g. a credential) by which the entity can be authenticated in the future" (ibid. pp 14 f.)
- "A *context* is a sphere of activity, a geographic region, a communication platform, an application, a logical or physical domain", e.g. a sector of government or a certain governmental service (ibid. pp. 8f).
- "A *credential* is a piece of information attesting to the integrity of certain stated facts. Credentials are primarily used in the process of entity authentication, and are often incorporated in an authentication token, e.g. a smart card, bank card, mobile phone, etc." But they do not necessarily have to be integrated into a token, as in the case of passwords. Certificates are a common type of credential in a PKI system (ibid. p.9).
- "*Corroboration* is the confirmation by provision of sufficient evidence and examination thereof that specific requirements have been fulfilled. The term "*verfication"* is often used as synonym of corroboration" (ibid. p. 9). The OECD terminology uses the term "*assurance*" for processes by which a relying party may check the validity of the authentication via certificates or other means "Assurance is not absolute: it is a defined level of confidence…." (OECD 2006, p. 21).

Legally binding transactions, e.g. applications, claims or contracts, often require a hand written signature on a form. There are cryptographic technologies providing for a digital equivalent to handwritten signatures within eGovernment and eCommerce. In the most advanced form they are generated and administered in an institutional environment that is called Public Key Infrastructure (PKI) with certification authorities (CA), issuing certificates, which confirm the assignment of a particular key to a registered person. Germany was among the first countries to pass legislation for electronic signatures, adopting a market-oriented approach, which allows for several CAs under state licence. Other countries established only one state owned CA. Furthermore, there are different technologies with different security levels. In 1999 a European Directive on Electronic Signatures aimed at a certain degree of harmonisation (Directive 1999/93/EC). In particular the directive distinguishes three kinds of signatures:

- A simple form of e-signature is simply called "*electronic signature*" and is defined as "data in electronic form which are attached to or logically associated with other electronic data, which serve as a method of authentication". This may

be a name written under the text in an e-mail. It only allows the authentication of a claimed identity of an entity, but not the corroboration of this identity.

- In contrast, an "*advanced electronic signature*" uniquely identifies and authenticates the signer of a message, and will allow checking the integrity of the signed data. Asymmetric cryptographic technologies, such as PKI and digital certificates, are mostly used for advanced electronic signatures. They are issued by a Trusted Third Party and may take the form of a piece of software to be stored on the hard disk of a PC or on a hardware token such as a smart card.
- A higher level of trustworthiness is provided *by advanced electronic signatures* which are based on a *qualified certificate* and which are created by a "*secure signature-creation device*" (SSCD). According to the directive and most of the national laws only these "qualified electronic signatures" are to be recognised with the same legal status and consequences as a handwritten signature. Technically an SSCD must be a smartcard or similar hardware device, and an acknowledged authority must confirm the content of the certificate.

A *certificate* is defined as "an electronic attestation, which links signature verification data to a person and confirms the identity of that person". According to the Directive 1999/93/EC, a qualified certificate must contain, among other things, the name of the signatory or a pseudonym, the identification of the CA, the state in which it is established and several attributes pertaining to the allowed use of the certificate. However, Member States are free to include additional data. Countries, which have a *unique national Personal Identity Number* frequently include this in the certificates. In these cases an electronic signature may also be used for authentication purposes. But most frequently eID cards contain two certificates, one for authentication and another one for the e-signature, which may come from different certification authorities.

EID management systems: components and architecture

The subject of this research has been termed eID management system. The Modinis terminology defines:

> "Identity management is the managing of partial identities of entities, i.e., definition, designation and administration of identity attributes as well as choice of the partial identity to be (re-) used in a specific context."
>
> "An identity management system is the organisational and technical infrastructure used for the definition, designation and administration of identity attributes" (Modinis Study 2005, pp. 11 f.).

These definitions cover personal, organisational and national eIDMS. From the description of the functions of an eID card in a national eIDMS it becomes obvious that on this level there is a need for

- an infrastructure for production, distribution, personalization of *tokens*, e.g. chip based eID cards,
- an infrastructure for the production and distribution of *certificates* and the accreditation of CAs,

– an infrastructure for administering identity *attributes* (e.g. civil registers) and
– provisions for distributing the technical *components* on the user side including support via hotlines etc.

These four subsystems together build the supply side of an even larger system, which includes the providers of online services as well.

Figure 3 depicts the *technical components on the side of the citizen*, including a PC or in some cases a mobile phone, an eID card, a card reader, a client software and web browser software. This system interacts with systems on the side of a *provider* of an eGovernment or eCommerce service, which consists of an eID server with appropriate middleware, which performs the authentication before the user gets access to the service he requests. In Germany, the provider of the eGovernment or eCommerce server needs an access certificate, which allows access by the eID server only to a predefined selection of the attribute data on the eID card.

The *eID card* (or other token) has to be requested at an issuing agency and may be personalised by another agency, which receives the card from a producer and the data representing the identity from a register keeping agency. When technical problems arise in the course of the installation of the components on both sides, there is usually a support hotline. If the eID card can also include an electronic signature, this possibly has to be requested from another certification authority. In some cases, additional components and institutions may be involved.

In this definition of an eIDMS, we do *not i*nclude the infrastructure employed for *visual authentication* at national borders and by police officers with special card readers and reference systems for authentication. Rather we conceive this *public safety system* with its own infrastructure as a separate but related system because investigating and comparing the processes behind the card check at the border would call for a completely different research project.

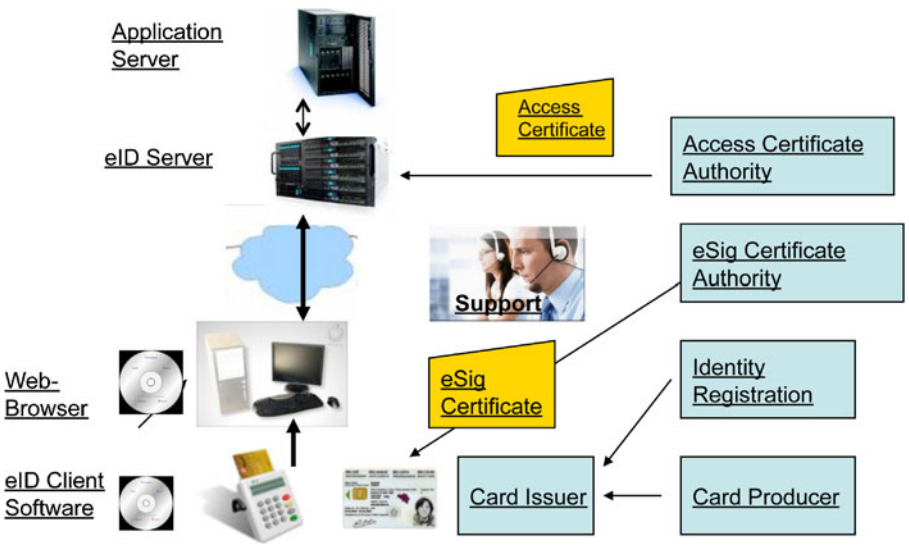

Fig. 3 Elements of an eIDMS

According to the terminology introduced here, the subject area of this comparative study on national eIDMS includes the *processes of identification, registration, authentication and authorization of citizens for using public online services of government or business via tokens with national validity and some kind of state authorization, considering the technical, organisational and regulatory aspects*.

Available research and research approaches

When the idea for a comparative European research project on national eIDMS emerged, information about the *status in the Member States* was provided by two reports published by the European Commission: the Modinis Study on Interoperability of eID Modinis Study (2006)[9] and another one by IDABC (IDABC 2007).[10] However, they contain only a compilation of comparable *descriptions* of the existing and planned systems in each Member State and focus on technical features and legal provisions. Thus they provided a good starting point but not any explanations.

Search for an appropriate conceptual framework

Checking the broader eGovernment literature did not lead to any theory driven comparisons of other nation wide innovations such as electronic signatures, the implementation of the EU-privacy directive, or authentication in online banking or e-payment etc. As the synoptical compilations in most cases came from only one expert only in each country, they are highly selective and do not cover all the aspects that may be relevant for explaining the differences from other Member States. Therefore in order to *explain differences in the eIDMS*, it would not be sufficient to do a secondary analysis of existing documents. Adopting an *actor-oriented approach*, key actors had to be identified, and the decision and implementation processes had to be analysed using data from interviews with these actors. To develop a specific conceptual framework for this analysis and for an appropriate interview guide, different social science theoretical approaches had to be taken into consideration. In particular concepts of *innovation research*, research on the *Social Shaping of Technology* (SST) and *Large Technical Systems* (LTS) as well as *Policy Field Analysis* were considered. There is no space to review these different approaches in detail here, but the basic conclusions may be summarized as follows:

- The introduction of an eIDMS can be conceived as an *innovation*, and different approaches by Member States might be characterized as either more *radical* or more *incremental innovations*. However, it was felt that the concepts and assumptions of innovation research did not adequately cover this particular kind of innovation. Recent innovation research assumes that innovations emerge from networks of

[9] The Status of Identity Management in European eGovernment Initiatives. Modinis Study on Identity Management in eGovernment, Deliverable D 3.5, June 2006, https://www.cosic.esat.kuleuven.be/modinis-idm/twiki/bin/view.cgi.

[10] http://ec.europa.eu/idabc/en/document/6484/5644. IDABC is a programme by the Euzropean Commission. The acronym stands for Interoperable Delivery of European eGovernment Services to public Administrations, Business and Citizens.

actors, with *no clear distinction between traditional phases*, e.g. invention, production and diffusion (cf. Rammert 1997, 2007, Sauer and Lang 1999), while in the case of eIDMS there still is *one dominating actor*, who has to *anticipate* many details of his planned system and to define these in legislation in advance.

- eIDMS also can be considered as *Large Technical Systems* (Hughes 1987, Mayntz and Hughes 1988, Jörges 1988). However the basic assumption there is that around a particular technical invention, e.g. electricity or railways, *a large technical and organisational system with infrastructural character emerges*. An eIDMS including the production of cards, used for online-authentication and national border control without any doubt has infrastructural character; however, it is not emerging around a new technology, but only changing an already existing institutional system; furthermore this change does not initiate new technologies, but combines different existing technologies to a new, complex socio-technical system. According to Braun and Jörges (1994) this can be called a Second Order LTS.
- More appropriate seemed a conceptual framework by Mayntz and Schneider, which has been developed on the LTS background and applied in a comparative analysis of the introduction of videotex systems in three European countries (Mayntz 1988, Mayntz and Schneider 1988, Schneider 1989). In line with the assumptions of the *Social Shaping of Technology* research they assume that these complex socio-technical systems are the outcome of an *interaction system* in which *institutional actors as stakeholders* in one or several arenas make choices between different technical options. The available options provided by a technical pool, and organisational and regulatory provisions are negotiated under the influence of *context factors* such as the legal environment, cultural norms etc. (Fig. 4).

As a political scientist Mayntz has later on generalized the institutional actor approach together with Scharpf as an approach for policy analysis in other fields as well. This approach is called "*institutionalism*" in political science and is well established in comparative analysis and *policy field analysis* (Scharpf 2000).

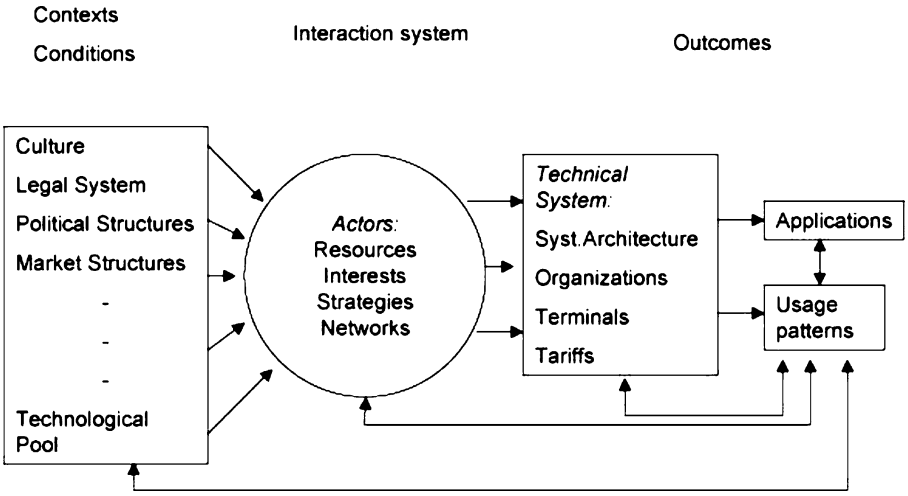

Fig. 4 Determinants of the development of technical systems (Mayntz/Schneider 1988)

Table 1 Research approaches in comparative policy analysis as distinguished by Scharpf (2000)

Institutional perspective Policy perspective	Genetic	Consequential
Problem oriented	Institutions emerge as reaction to policy problems	Institutions influence the policy adopted
Interaction oriented	Institutions emerge as the result of the interaction of policy makers	Institutions influence the interaction of policy makers

According to Scharpf, *policy field analysis* can either be *problem oriented* or *interaction oriented*. The former tries to analyse the emergence of a societal problem and the effectiveness of the policy chosen to deal with this problem. The latter instead examines the interaction between policy makers and the conditions that favour or impede their ability to adopt and implement their policy responses. The study of institutions on the one hand is focussing on the *genesis* and transformation of institutional arrangements, and on the other hand on the *consequences* that institutions may pose for actors and actions. By combining these two twofold views, four cells emerge (Table 1).

The combination of a *problem oriented* policy research with a focus on *emerging institutions* explains how new institutions arise as a result of policies which are supposed to solve new societal problems. The second cell combines problem oriented policy research with the analysis of the *consequences* of existing institutions and asks how the existence of given institutions contributes to the emergence or avoidance of certain societal problems. The third cell combines *interaction oriented* policy research with the focus on the *genesis* of institutions and tries to explain institutional change as the outcome of strategic interactions between purposeful and resourceful actors. Finally the fourth cell deals with *institutions* as one set of factors *influencing* the interactions between policy makers and the capacity of a policy-making system to adopt effective responses to policy problems.

We do not consider the four perspectives as mutually exclusive, but as different views, which may be *combined* very well within one research design. Obviously eIDMS can be conceived as *institutions*, which are *to solve new problems and emerge as the result of strategic interactions between purposeful and resourceful actors*. But these interactions *take place in already existing institutions*, and therefore the view of cell # 4 has to be applied as well.

Scharpf (2000) points to a few factors *complicating* both approaches, which have to be considered when developing a research design:

- The question of effective policy responses, hindered or supported by existing institutions, cannot be answered without reference to and *knowledge of the policy problem* and the different options for solving this problem. This knowledge lies outside political science, but in our case we can draw on this knowledge from *computer science* regarding the technical aspects of an eIDMS.
- Policy problems are not given but *construed*, they do not always correspond to policy legacies, i.e. existing structures and procedures for dealing with certain classes of problems. e-Identity and eGovernment are not established policy

fields, and the assignment of the eIDMS development to respective problems and to institutional subsystems may vary. Therefore this *assignment to a policy field* is a variable and nor a precondition in our studies.

- Institutional conditions do *not determine* the actions of persons representing these institutions. They enable and restrict their actions and there is still discretion for individual actors ´ preferences and orientations. This calls for taking into account the context influence of *cultural norms* in the Mayntz/ Schneider framework and as far as governments as institutions are considered, the affiliation of actors to *political parties and their ideologies*.

A link between the different institutional perspectives in Table 1 can be established by more recent concepts of *path dependency*. The concept of path dependency was originally developed by economists to explain technology adoption processes as well as the evolution of economic development. The theory was empirically substantiated by David's studies of the sustainability of a well-established technical standard: the QWERTY keyboard (David 1985). The key aspect emphasised in theory and evaluated in empirical studies, is the missing determinant for economic processes. Progress cannot be identified as moving continuously toward some pre-determined equilibrium but is pushed by non-linear processes (see e.g. Dosi 1982). Therefore existing systems show a *high degree of persistence* and any change meets resistances and needs additional resources as well as particular driving forces. In retroperspect this leads to the conclusion that "*history matters*", which may sound trivial. Meanwhile, a more differentiated discussion within and about path dependency theories has taken place, which states that there may be different reasons and options for path continuation and that there are cases of path continuation as well as cases of *path modification or break-up* (Meyer and Schubert 2007; Deutschmann 2007). While path analysis in most cases does not consider actors, Garud and Karnoe (2001) have highlighted the *role of actors embedded in the structure of an established path*. Accordingly one can investigate if, why and to what extent these actors maintain or modify this path or purposefully break up and create a new path. Figure 5 illustrates this broader view on path creation, path persistence and break-up.

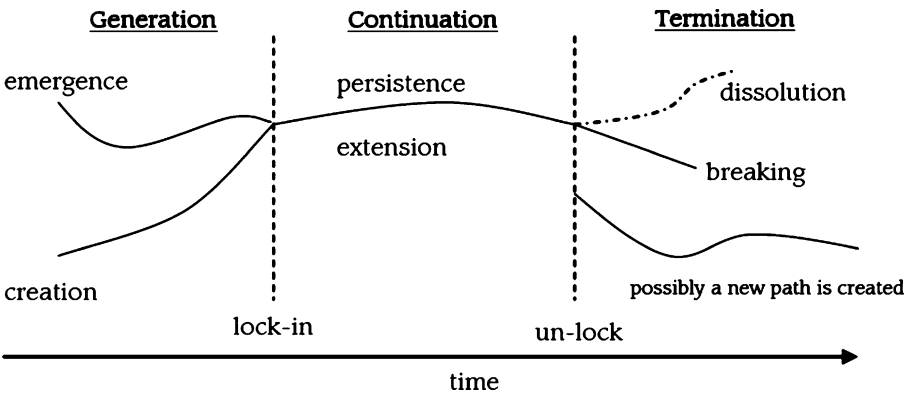

Fig. 5 Phases and forms of path development (from Meyer and Schubert 2007, p. 12)

A more differentiated analysis of technological innovations might distinguish between *different kinds of paths*. The traditional focus of path analysis is on *technological paths*, but in the light of our institutional approach the technical components are embedded in *organisational arrangements* and subject to *legal regulations*, whose relation to technological changes may be continued, adapted or be replaced by completely new ones, i.e. there is a choice of path continuation, change or creation both for an *organisationa*l and a *regulatory path*.

A *combination* of the institutional approach with path analysis allows for a more powerful synthesis. Path analysis is enhanced by focussing on *actors´ choices between path continuation, change or path creation*, and the institutional approach can combine the generic and the consequential perspective by referring to these path related changes. Choices are made by actors on behalf of the existing institutions, they represent, but these choices do concern the future of these institutions as well as continuing, changing or creating other institutions as parts of the eIDMS.

To be more precise: We assume that there is a number of *policy makers* (institutional actors) in government and parliament, who interact in order to develop an eIDMS as a policy response to the *societal problem* of security concerns related to the Internet. They represent existing institutions and interact under existing regulation. But some of them have the *power to change existing organisations and regulation*, to create new organisations as part of a new socio-technical system, i.e. they do not only choose between technological options but also between continuation, change or creation on the organisational and regulatory path.

This integration of the institutional perspectives and path analysis leads to a *revised conceptual framework*, which is depicted in Fig. 6 and is composed of five main categories of variables:

(1) the *interaction system* including the main institutional actors and the process of interaction,
(2) the *new socio-technical system eIDMS* as outcome of the interaction process, consisting of technical, organisational and regulatory components,
(3) the *relation of the new eIDMS to the previous one* in respect of technological, organisational and regulatory path continuity or change,
(4) *context factors* under which the actors negotiate and make their path related choices,
(5) the *diffusion of the eIDMS*, i.e. the adoption of the ID function by service providers in eGovernment and eCommerce, the number of tokens issued and the frequency of use of the eID function.

The context factors highlighted in the Mayntz/Schneider framework, e.g. legal structure, market structure, culture, political structure (Fig. 4), are assumed to have already influenced this existing system. In Fig. 6 accordingly on the left side there are arrows marking an influence of the *technological pool* out of which a *technological path* for the old system, had been created, a *regulatory path* for the old pattern of regulation coming out of the *legal structure*, and an *organisational path* emerging from the existing *structure of public administration* establishing the institutions to administer the eIDs.

In order to explain the *actors´ choice* to continue with, modify or break from these existing paths we assume that in particular "*culture and values*" as well as the "*political*

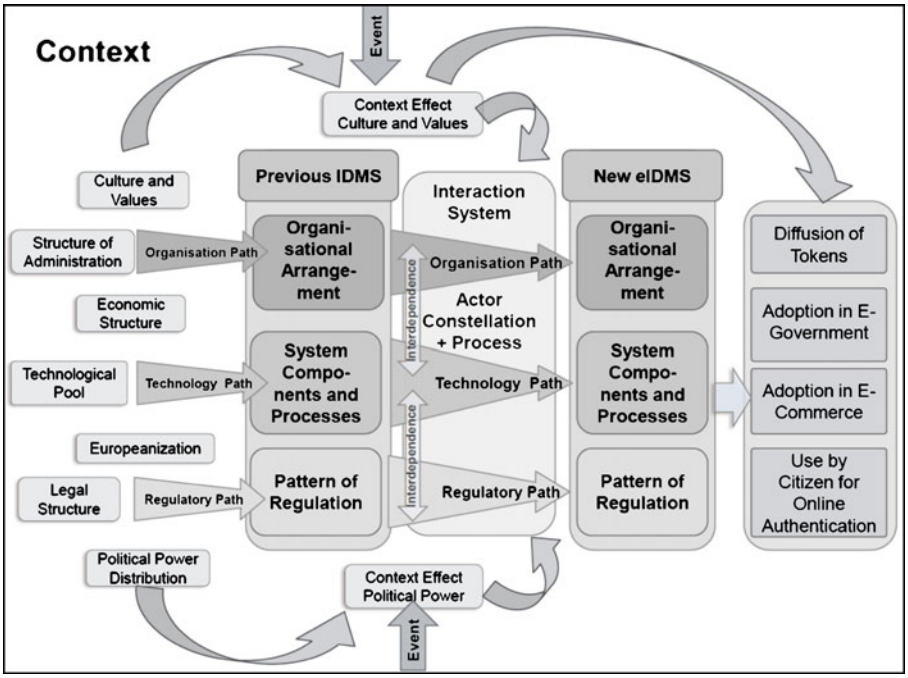

Fig. 6 Context-dependent path-choices in the transition of a national IDMS to an eIDMS

power distribution" are most relevant. From the first interviews we learned that at least in some cases *events* such as September 11 changed the priority of values and led to changes of the relationship between privacy and security culture. We also learned that *changes of government* after elections changed the actor constellation and thereby the priorities in the development process, which caused delays or initiated speedups. Therefore arrows are drawn in Fig. 6 for these two context factors directly pointing to the interaction system, and separate arrows mark the influence of certain events.

Although the focus of this study is on the development process and the eIDMS as its output, an attempt has been made to assess the *acceptance and usage of the system* by providers of online services and their users as well. For a comprehensive analysis of the diffusion, acceptance and usage of an eIDMS, different research methods and interviews with others actors and surveys on citizens´ attitudes and behaviour would have been necessary. This was outside the scope of this project, but some statistical data was collected to allow for a few conclusions regarding the effectiveness of the choices taken and the contribution the innovation has made to solve the problem it was developed for.

To explain higher or lower *rates of usage of the eID function* by citizens we employ Rogers´ theory of *the diffusion of innovations*. Rogers (2003) puts particular emphasis on the way in which an innovation is communicated. He proposes that 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,

- are not too *complex* and do not afford new skills and
- are *triable* and *observable*.

In a study for the European Commission on barriers to the *diffusion of electronic signatures* the German Fraunhofer Institute has applied Rogers´ theory and concludes that electronic signatures are associated with high costs, are hard to understand and hard to get started, and that there is a lack of support (Fraunhofer Institute FOKUS 2006). It may well be that the eID based authentication meets the same barriers to diffusion.

Aspirations and design of the empirical research

The conceptual framework depicted in Fig. 6 does not provide detailed hypotheses about the kind of relation between the factors mentioned or the different values that the variables mentioned might take. Given the little available knowledge on the factors that influence this kind of decision it did not seem appropriate to *formulate detailed hypotheses in advance* and test them in a comparative research design. Instead we aimed at *exploring possible influences along the categories* defined in the conceptual framework and to arrive at some g*eneralisations* about influences that provide for a plausible explanation of differences between the national eIDMS. This may be called *grounded theory* (Glaser and Strauss 1967).

As the interviews in the countries under study were to be conducted by researchers in the respective countries an *interview guide* has been developed containing more than fifty questions relating to the different categories and elements of the framework, in order to attain at a high degree of comparability. In addition categories of possible *relevant actors* have been distinguished, based on the descriptive reports available. At the beginning of this cooperative research a workshop was held to reach a common understanding of the framework and the questions and to define the 10 to 15 most important actors in each country to be interviewed. From the available documents we were able to identify the ministries involved in the process. In addition, representatives from organizations administering the former/present IDMS, e.g. civil registry, and government organizations offering online services, in most cases tax authorities, were identified as well as representatives from the private sector, in particular IT industry and eCommerce and banks. Fortunately almost all actors approached agreed to be interviewed. In order to assess whether the interview guide fits to the different situations the author of this paper and coordinator of the whole project participated in two or three interviews in each of the four countries under investigation. After the first three to five interviews in each country a second workshop was held in order to review the interview guide and to enhance the conceptual framework.

Selection of countries

The extent to which generalizations prove to be valid crucially depends on the selection of the cases from which they are derived. As resources did not allow

for a full analysis of all EU Member States introducing an eIDMS, we developed a two-stage research design. In a first stage four in depth case studies have been conducted with between 10 to 15 expert interviews in each country. The findings of these cases have been compared and a number of generalizations have been derived. In a *second phase* experts in four other countries have been asked to summarize the development of the eIDMS in their respective country and to reflect on what extent these generalizations apply to their case as well.

In comparative political analysis there is an intensive debate about *appropriate selection methods*, mostly discussing the two ideal type approaches of the "*most similar*" and the "*most different*" design (Jahn 2006, pp. 223ff.). But first of all the *basic population* has to be defined. The units of analysis are national eIDMS of Member States of the European Union. As the study should provide empirical evidence on the introduction of eIDMS, conceived as the process of transition from an existing IDMS to a new electronic IDMS, and not deal with public debates about planned eIDMS, only those countries belong to the basic population which in 2007 had an established national IDMS and which had started introducing a new eIDMS. Based on

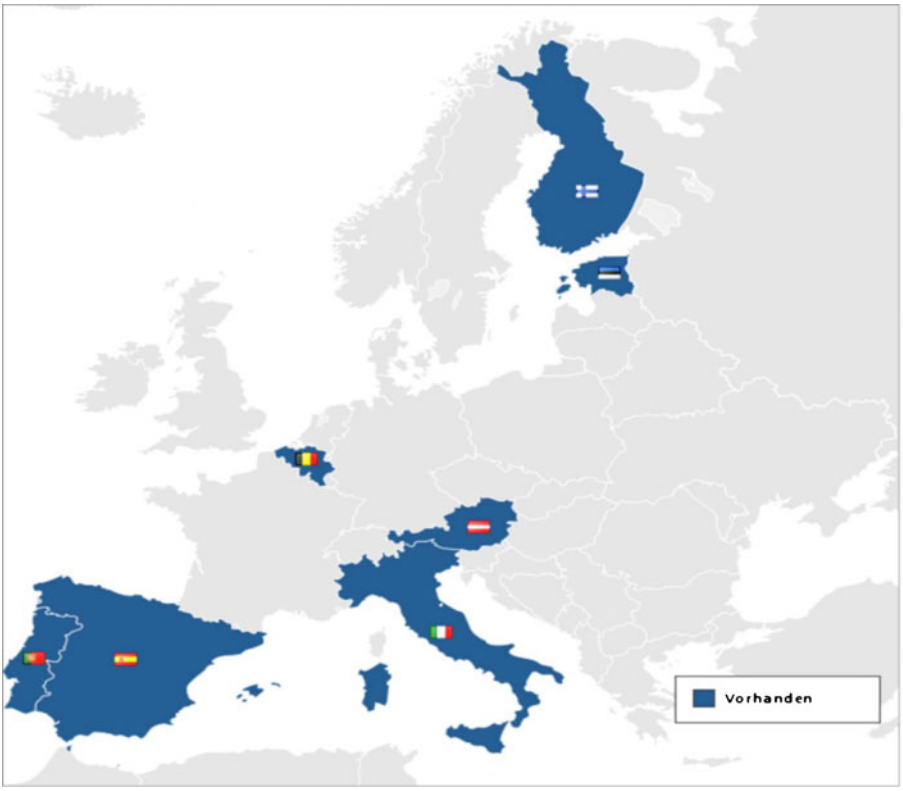

Fig. 7 EU Member States with eID cards in 2007 (vorhanden=existing)

the IDABC country reports (IDABC 2007), there were seven countries (Fig. 7):

- Austria
- Belgium
- Estonia
- Finland
- Italy
- Portugal
- Spain.

For budget reasons, it was not possible to conduct intensive case studies in all seven countries. For actors interviews besides Germany only three could be selected. In order to draw lessons for the still planned eIDMS in Germany a *"most similar design"* seemed most appropriate. Most relevant seemed a similarity with regard to basic characteristics of the existing legal national IDMS, e.g. the obligation of citizens to register and to hold an ID card as well as basic features of the eIDMS. As the planned German eID was to use the national eID card as token and would include digital fingerprints on the card as well as particular technical privacy provisions, these variables were used as reference points to assess the similarity.

Table 2 presents the data, which have been collected from the IDABC country profiles (IDABC 2007). No country profile completely matched with the German profile, but Austria and Spain are *similar with regard to four respectively three variables.* Among the other countries with only two matching variables Belgium was chosen because of its more advanced rollout.

For scientific purposes, such a *German centered selection* may be not be satisfactory. In order to check to what extend this selection distorts the findings and hinders generalisations at the European level, a *second set of case studies* has been

Table 2 eIDMS country profiles (based on IDABC 2007)

	Point of reference	Countries with eID rollout in 2007						
	Germany	Spain	Austria	Belgium	Estonia	Finland	Italy	Portugal
Obligation to register	Yes	Similar	Similar	Similar	Similar	Similar	Similar	Similar
Obligation to have ID card	optional[a]	Different	Similar	Different	Different	Different	Different	Different
eID card = ID card	Yes	Similar	Different	Similar	Similar	Similar	Different	Similar
Unique Personal Identity Number	No	Different	Similar	Different	Different	Different	Different	Different
Biometrics on eID card	Yes	Similar	Different	Different	Different	Different	Different	Different
Technical privacy provisions	Yes	Different	Similar	Different	Different	Different	Different	Different
Similarities		3	4	2	2	2	1	2

[a] ID Card ("Personalausweis") or Passport

carried out. For this purpose a "most different approach" has been adopted. Estonia and Finland have been chosen from the first basic population listed above because they show a *high degree of involvement of the private sector* in operating a national eIDMS. Sweden and Denmark have been added, which although similar with regard to the legal IDMS (i.e. obligation to register, unique personal identifier), so far *have not succeeded in introducing a planned eID card*. The United Kingdom has not been included in this second phase, because it differs with regard to all relevant variables by not having a national ID and no obligation to register. Therefore introducing an eID in this country is not an innovation of or within a national IDMS or a transition from one national IDMS to new electronic one but a radical change of citizenship, where the issue of online authentication only plays a very minor role (see Bennett and Lyon 2008).

Overview and outlook

The following four papers by Mariën and Van Audenhove (2010), Aichholzer and Strauß (2010), Heichlinger and Gallego (2010) as well as Noack and Kubicek (2010) will present the *four case studies* of this first part of the comparative research. They will start with the *historic context of citizens´ registration and identification* and on this background describe the *new eIDMS* which is being introduced in terms of the eID itself (i.e. attributes = data), the token(s) (in most cases eID cards), the process of applying for an eID as well as the distribution and personalization. The *actors constellation* will be mapped and the *policy field* taking the lead in the innovation process, as well as the stages, main events and eventual controversial issues within this *process* and *competing eID systems*, The *legal framework* including privacy regulations will be referred to and finally the *diffusion* of new cards and the use of their online authentication function will be assessed.

In these four cases the reader will encounter big differences on almost all components. In a first comparative analysis we will depict the *differences in the four eIDMS*, examine how these can be explained by the conceptual framework presented here, and derive a set of *generalizations* across the four cases (Kubicek and Noack 2010a). As we cannot be sure that the four cases cover the whole range of eIDMS being introduced in the European Community these days, *four other cases* studies will follow, which are not based on personal interviews but on documents and which will explicitly refer to some of the generalisations proposed (Hoff and Hoff 2010, Rissanen 2010, Grönlund 2010, Martens 2010). Finally there will be a review on how the generalisations presented before cover these cases as well and to what extent the *conceptual framework* employed has *proven to be useful* or in which respect further development seems necessary (Kubicek and Noack 2010b).

Regarding the potential of the integration of institutional analysis and path analysis, there will be no completely satisfactory explanation of every difference reported. When the existing older IDMS is considered as an important influencing factor one would like to know more about *its origin*. As for example the obligation to register and to hold an ID document in some countries dates back into the 16th or 17th century this would require historical analyses, which could not be conducted within this cooperative project. Nor can we explain why some countries have a

unique personal identity number for each citizen while others have banned such a regulation. Despite questions for further research arising from this analysis strong evidence emerges, that there is little room for *technological determinisms*. Not only have different technological paths been chosen to develop a national eIDM, but more important, *for similar technical systems quite different organisational and regulatory patterns have been established*. This is not only of relevance for academic disputes within technology related social science debates corroborating the *social shaping school*. It also undermines all those comments in academia and the media, *predicting or expecting fundamental changes in the citizens-government relation, such as an increase in surveillance*.

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, editor. Identity in the information Society: challenges and opportunities. Dordrecht: Springer; 2009. p. 245–68.

Bennett J, Lyon D. Playing the identity card. London: Routledge; 2008.

Braun, I, Jörges, B. Technik ohne Grenzen. Frankfurt a. M.: Suhrkamp; 1994.

Cameron K, Posch R, Rannenberg K. Proposal for a common identity framework. A user-centric identity metasystem. In: Rannenberg K, editor. Identity in the information society: challenges and opportunities. Dordrecht: Springer; 2009. p. 477–500.

David PA. Clio and the economics of QWERTY. The American Economic Review. 1985;75(2):332–7.

Deutschmann, C. Dynamische Konzepte institutioneller Einbettung. MPifG, Köln, 2007 (conference paper) http://www.mpi-fg-koeln.mpg.de/maerkte-0702/papers/Deutschmann_Maerkte2007.pdf

Dosi G. Technological Paradigms and Technological Trajectories. Research Policy, 1982: 11, pp. 147–162.

Garud, R, Karnoe, P. Path creation as a process of mindful deviation. In: Garud, R., Karnoe, P. (eds.) Path dependence and creation. Mahwah N.J. / London 2001: 1–40.

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.

Halperin, R. Backhouse, J. A roiadmap for research on identity in the information society. Identity in the Information Society. 2008; 1 (1)

Hansen M, Berlich P, Camenisch J, Clauss S, Pfitzmann A, Waidner M. Privacy-enhancing identity management. Inform Secur Tech Rep. 2004;9(1):35–44.

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.

Hornung G. Die digitale Identität. Baden Baden: Nomos; 2005.

Hughes TP. The Evolution of Large Technological Systems. In: Bijker W, Hughes TP, Pinch T, editors. The social construction of technological systems. Cambridge: MIT Press; 1987. p. 51–82.

IDABC. Analysis and assessment of similarities and differences—Impact on eID interoperability. Report, Brussels: European Commission; 2007 (http://ec.europa.eu/idabc/servlets/Doc?id=29618)

Jahn D. Einführung in die vergleichende Politikwissenschaft. Wiesbaden: VS Verlag für Sozialwissenschaften; 2006.
Jörges, B. Large technical systems: Concepts and issues. In: Mayntz, R, Hughes, T P (eds.). The development of large technical systems. Frankfurt a. M., New York: Campus. 1988: 9–36.
Kubicek H, Noack T. The path dependency of national electronic identities. A comparison of innovation processes in four European countries. Identity in the Information Society, Special Issue, 2010a. doi:10.1007/s12394-010-0050-2.
Kubicek H, Noack T. The Different countries—Different paths. Extended comparison of the introduction of eIDs in eight European countries. Identity in the Information Society, Special Issue, 2010b.
Mariën I, Van Audenhove L. The Belgian e-ID and its complex path to implementation and innovational change. Identity in the Information Society, Special Issue, 2010. doi:10.1007/s12394-010-0042-2.
Martens T. Electronic identity management in Estonia between market and state governance. Identity in the Information Society, Special Issue, 2010. doi:10.1007/s12394-010-0044-0.
Mayntz, R, Hughes, T (eds). The development of large technical systems. Frankfurt: Campus; 1988.
Mayntz, R, Schneider, V. The dynamics of system development in a comparative perspective: Interactive videotex in Germany, France and Britain. In: Mayntz, R, Hughes, T (eds): The Development of large technical systems. Frankfurt: Campus: 1988.
Meyer U, Schubert C. Integrating path dependency and path creation in a general understanding of path constitution. The role of agency and institutions in the stabilisation of technological innovations. Sci Tech Innovat Stud. 2007;3:23–44.
Modinis Study on Identity Management in eGovernment. Common terminological framework for interoperable electronic identity management. European Commission / University of Leuven; 2005. (https://www.cosic.esat.kuleuven.be/modinis-idm/twiki/bin/view.cgi/Main/GlossaryDoc)
Modinis Study on Identity Management in eGovernment. The Status of identity management in European eGovernment initiatives. Brussels / Leuven: European Commission /University of Leuven; 2006 (https://www.cosic.esat.kuleuven.be/modinis-idm/twiki/bin/view.cgi/Main/ProjectDocs)
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. Electronic authentication and OECD guidance for electronic authentication. Paris: OECD; 2006.
OECD. Online identity theft. Paris: OECD; 2009.
Rammert W. Innovation im Netz. Neue Zeiten für technische Innovationen: heterogen verteilt und interaktiv vernetzt. Soziale Welt. 1997;48(4):397–416.
Rammert W. Technik-Handeln-Wissen. Wiesbaden: VS Verlag; 2007.
Rannenberg K, Royer D, Deuker A. The future of identity in the information society. Dordrecht: Springer; 2009.
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 innovation. 5th ed. New York: Free Press; 2003.
Sauer D, Lang C, editors. Paradoxien der Innovation. Perspektiven sozialwissenschaftlicher Innovationsforschung. Frankfurt: Campus; 1999.
Scharpf FW. Institutions in comparative policy research. Comp Polit Stud. 2000;33(6/7):762–90.
Schneider, V. Technikentwicklung zwischen Politik und Markt: Der Fall Bildschirmtext. Frankfurt a.M.: Campus; 1989.
Taylor, J A. Lips, M, Organ, J. Identification practices in governmenet: Citizen surveillance and the quest for public service improvement. Identity in the Information Society, published online 24 February 2009 http://www.springerlink.com/content/2pl2731712732452/?p=5cff93b8b6c84d2da8449761a416e341&pi=9