IDIS (2010) 3:87–110
DOI 10.1007/s12394-010-0051-1

The introduction of online authentication as part of the new electronic national identity card in Germany

Torsten Noack · Herbert Kubicek

Received: 14 October 2009 / Accepted: 11 March 2010 / Published online: 25 March 2010

Abstract This chapter provides an analysis of the long process of introducing an electronic identity for online authentication in Germany. This process is described as a multi-facet innovation, involving actors from different policy fields shifting over time. The eID process started in the late '90s in the context of eGovernment and eCommerce with the legislation on e-signatures, which were supposed to allow for online authentication of citizens. When after 5 years it was recognized that this was not the case, a new digital ID card, which had meanwhile been announced, was chosen as token for the eID. This process was dominated by the concerns for visual inspection and border control, including the storage of digital fingerprints. Under the leadership of the Ministry of the Interior (BMI) and technical guidance of the Federal Agency for Information Security (BSI), technical specifications have to a large extent been adopted from the electronic passport, which had been smoothly introduced 2 years before. However, in the legislative process some concern regarding digital fingerprints on the eID card was raised and led to an opt-in solution. In 2009, a bill on the new ID card was passed which regulates the eID function for online authentication as well. This is characterized as a radical innovation by introducing a double-sided, mutual authentication of the citizen and the service provider and implementing the principle of proportionality regarding the access of service providers to data on the chip. At the time of writing, field tests are conducted. Roll-out of the new eID card is to start in November 2010. Therefore no figures about adoption can be provided here.

Keywords ID card · Double-sided authentication · Electronic passport · Privacy enhancing authentication · RFID chip

The research presented here is based on interviews with key actors and experts between December 2007 and June 2009 and funded by Volkswagen Foundation, Germany.

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

Identification and authentication of citizens in Germany

Germany has a long tradition of registration and identification of citizens. In 1876, the state administration of the German Empire took over the registers of births, deaths, and marriages, which up to then had been held by the churches. In 1938, the National Socialist Regime (Third Reich) introduced an ID card with fingerprints, which was mandatory only for conscripts and Jewish citizens. 1939, with the beginning of the Second World War, it became mandatory for every citizen[1] and inhabitants of the occupied territories. Jewish citizens were also assigned with numbers, which were used for their deportation and administration in concentration camps (Hornung 2005; Aly and Roth 2000).

This specific historical context has influenced the debate about eID and a new electronic ID document ("elektronischer Personalausweis", ePA) in the last 10 years just as it did the earlier debate about a unique personal identifying number. Such an identifier has been banned by the Federal Constitutional Court in the context of the national census of 1981 as well as by Federal Parliament. It was also considered in the Personal Document Act. German citizens have to hold either a personal ID card or a passport.[2] The ID card has a registered serial number. However, this serial number may not be used to identify the holder in any other administrative procedure except for police and intelligence procedures. Recently, a universal tax number has been introduced, which according to the respective law[3] may only be used for tax collection purposes and therefore is considered to be sector specific.

The registration of citizens is still administered by the local municipalities and has been regulated by state laws of the federal states under a national framework law until 2006. Several of the16 federal states have established central mirror registers in addition to the local ones within the respective state. In 2006, legislative authority was transferred to the national level exclusively.[4] However, the debate on the degree of centralisation of the citizens' registries on the state or even national level continues.

The debate about eID originated within eGovernment context. When citizens apply for public services, request official documents or follow certain reporting duties, they identify themselves by filling in a form with their name, date of birth and sometimes their home address as it is registered in the civil registry and then confirm the information given by signing the document. These administrative procedures usually require no proof of the validity of the self-reported identifying data. Citizens hand over the forms at local offices or send it by post, but do not have to show their ID card.

When in the late 1990s access to public services via the Internet began to be offered, the existing paper-based forms were simply copied into online forms, which had to be filled in with the same identifying data except for the signature. When legally binding transactions had to be made, as for example an online tax

[1] ID card act 1938: "Verordnung über Kennkarten" Reichsgesetzblatt Teil I 1938 p. 913 and "Erste bis Dritte Bekanntmachung über den Kennkartenzwang", Reichsgesetzblatt Teil I 1938 p. 921.
[2] § 1 (1) PAuswG 1986 (PAuswG—Personalausweisgesetz—ID card act).
[3] § 139a, 139b, 139c, AO (AO—Abgabenordnung).
[4] Law amending the German Fundamental Law (Gesetz zur Änderung des Grundgesetzes) 2006, BGBl 1, p. 2034.

declaration, all data could be entered online, but a summary sheet had to be signed manually and sent to the tax office by mail. To overcome this parallel communication, Germany passed a law on a framework for electronic signatures 2 years before the European Directive in 1997.[5] In 1999 Federal Government provided matching grants to local municipalities for the development of legally binding online services employing electronic signatures.[6]

The first eGovernment programme of German federal government was launched in 2000. In "BundOnline 2005", federal government committed itself to put online all available public services by federal agencies until the end of 2005 (BMI 2006b). The coordination of this programme was assigned to the Federal Ministry of the Interior (Bundesministerium des Innern, BMI). Online authentication was not explicitly addressed until September 2006, when federal government passed its third eGovernment programme "EGovernment 2.0" (BMI 2006a). At this point in time, the new electronic national ID card (ePA), which had been announced to be rolled out from 2009 onwards, was confirmed as the one and only token for this functionality: "With digital identity cards, the necessary secure, harmonised online authentication functionality will be created for eGovernment and eBusiness ... innovative security technology will be used that will also help to modernise public administrations and to strengthen internal security. As such, the use of electronic identity cards will create a higher level of data protection ... businesses will also be able to give access to private eBusiness applications that use electronic identification." (BMI 2006a, 20). In February 2009, the law on the electronic personal ID card, which is establishing a complex IDMS (Identity Management System) for online authentication ("Elektronischer Identitätsnachweis"=electronic proof of identity), finally passed the Federal Council.[7] After a pilot period and application tests, the first eID cards are planned to be issued in November 2010.[8]

Within this process two main phases with different concepts of and strategies for the implementation of an eID can be distinguished.

The two phases of the innovation process

Figure 1 depicts the two phases with their most important events.

In the eSignature phase, the focus has been on providing electronic means to make the data citizens enter into online forms and electronic documents legally binding. Electronic signatures were believed, besides assigning a document to a defined person, to allow for the authentication of this person via the same certificate at the same time. According to the German Signature Law passed in 1997 an authentication is required for registering for a qualified electronic signature within a public key environment. This means that applicants have to show their personal ID card, which is photocopied by the registration authority.

[5] Informations- und Kommunikationsdienste-Gesetz—IuKDG, 1997 BGBl 1, p. 1870.
[6] Media@Komm, 1999–2003, about 50 million DM, equal roughly to 25 million EUROs.
[7] See subsection "Federal states".
[8] http://www.bmi.bund.de/cln_095/DE/Themen/Sicherheit/PaesseAusweise/ePersonalausweis/ePersonalausweis_node.html.

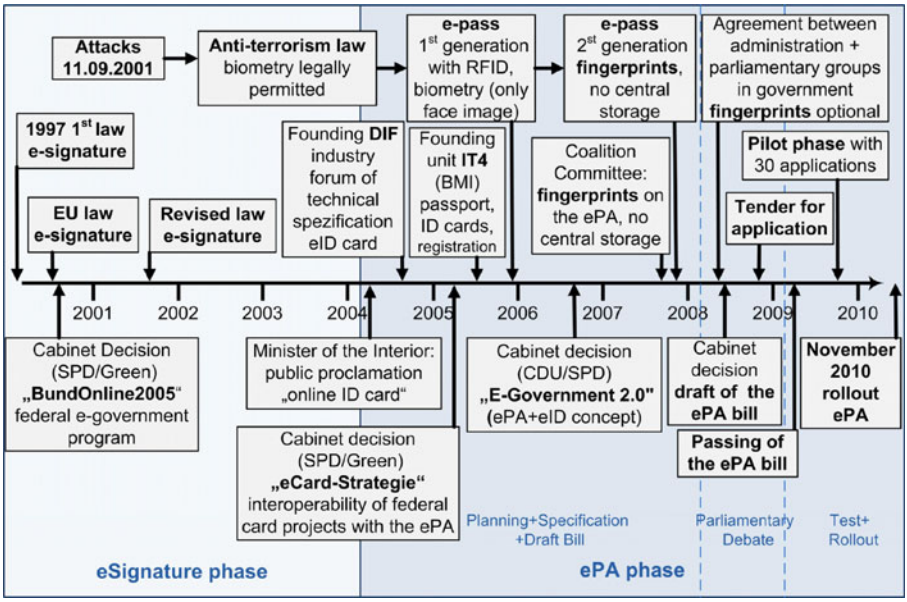

Fig. 1 Phases of the development on online authentication in Germany

It took some time to recognise that the certificate used for electronic signatures does not allow for a valid authentication of the holder, because—in contrast to other European countries—it only includes surname and first name as attributes. So if there are two citizens with the same name there is no additional attribute to distinguish and corroborate their identity. When in 1999 the EU directive on electronic signatures was passed, the German law, which only regulated qualified signatures, had to be adapted to include less secure advanced signatures as well (revised eSignature law). Although the directive requires that certificates shall allow for the authentication of holders, the legal definition of the set of data in the certificates was not extended. Government officials in charge of the adaption of the Signature Bill maintained that a handwritten signature also consists of surname and first name with no additional attributes and therefore saw no need to add any other attributes in the digital word.[9]

In order to promote the use of the eSignature, the Ministry of Research and Technology opened a competition for matching funds for local municipalities to develop and offer public services with electronic signatures in 1998. Three cities received a total of 50 million DM (25 million EUR) for offering several services between 1999 and 2002.

During the eSignature phase there was also a separate discussion about electronic ID cards as in 2002, the Ministry of Research and Technology ordered a feasibility study (cf. Reichl et al. 2005). However, online authentication was not explicitly addressed in this study because the eSignature was still believed to be an appropriate tool. At the time, trust in the eSignature was so high that even pilot projects with online voting which used the eSignature for the authentication of voters were funded.

[9] According to interviews conducted in the Ministry of Economics and Technology responsible for the legislation on electronic signatures.

This period also includes the September 11 attacks in 2001. Immediately afterwards, an anti-terrorism package bill was submitted by the Minister of the Interior within a SPD/Green Government, which included an amendment of the law on the personal ID card that allowed storing biometric data on a forthcoming electronic ID card.

From 2002 onwards, several ideas for the usage of smart cards in different areas emerged. Besides the still not elaborated plan for an electronic ID card, the Ministry of Health made plans for a digital health card[10] while the Ministry of Labour and Social Affairs planned a so-called job card by which employers were supposed to file the wages paid to an employee. Plans were made for every entitled social security or government agency to be granted access to this data instead of requesting paper-based reports ("Einkommensnachweis"). For a very short time, the Minister of the Interior pursued the idea of having one integrated card for these three areas of application (cf. Reichl et al. 2005, V). But there were too many objections and political conflicts of interest.

With the establishment of a project group on the electronic ID card within BundOnline2005 in 2003, the development of an alternative to the eSignature was started. Although the main goal was a more secure ID card, functionality for a secure online authentication was sought to be included.[11] Variations of e-card ideas (e.g. a citizen card as a multi-function card[12]) were brought forward by eGovernment stakeholders. At the end of the eSignature phase, various different and independent e-card system concepts were on the political agenda.

In summary, two discussions on eID and eID cards took place from 2003 to 2004: in the Ministry of Economics and Technology (BMWi), which was still responsible for the eSignature at the time, solutions for authentication within eGovernment were sought, while the Ministry of the Interior (BMI) focussed on the renewal of the ID card with regard to a more secure visual authentication and electronic travel document as well as online authentication on the Internet.

When it was finally recognised that the eSignature does not allow for secure online authentication, the envisaged new eID card was chosen as the only suitable token for this purpose, and the lead on the subject shifted to the BMI, which combined responsibility for ID cards as well as federal eGovernment services. There, a project group on Personal Documents and Registry was established within the IT staff, a division within the Ministry, which is also responsible for intergovernmental coordination of IT developments across ministries.

The Federal Office for IT Security (Bundesamt für Sicherheit in der Informationstechnik, BSI), which is attached to the BMI and which had positioned itself as the technical IT competence centre for federal government was commissioned to define technical requirements and specifications. It sought cooperation with the IT industry and the Government Printing Office (Bundesdruckerei), the producer of ID cards, and established the DIF, the German Industrial Forum.[13] In fact this group

[10] Mid 2009 still in the implementation phase/pilot phase.
[11] According to interviews conducted at BMI and BSI.
[12] Cf. BITKOM 2002: "Bürgerkarte für Deutschland" http://www.verbaende.com/News.php4?m=13434 , http://www.bitkom.de/de/presse/38020_2103.asp, http://www.novosec.com/documents/eGovernment_DieBuergerkarte_020930.pdf.
[13] See section "Constellation of actors".

transposed the political requirements of the BMI into technical specifications and proposals for technical standards.

The most important political decision was the so-called "eCard Strategy" taken by the cabinet (SPD/Green Party) in 2005. This "strategy" is not a concept for particular e-cards, but rather a standard interface, which guarantees that eSignature functions on different e-cards issued by the government (eID card, health card) can equally be accessed by all eGovernment services.

This marks the official start of the second, the ePA phase, which can be divided in three sub-phases: planning, parliamentary debate as well as testing and rollout.

After the election of 2005, the coalition of the Social Democratic Party (SPD) with the Green Party lost its majority and the SPD entered a new coalition with the Christian Democratic Party (CDU). The Ministry of the Interior, led by a SPD Minister before (Otto Schily) was taken over by the CDU (with Wolfgang Schäuble as Minister of the Interior). On his behalf, the new cabinet issued the federal programme "E-Government 2.0" in September 2006. In continuation of the previous cabinet decision of March 2005 ("eCard-Strategy"), the BMI was entrusted with the introduction of a digital ID card including online authentication as well as with drafting the necessary legal provision. Work on the specification according to the e-card frame had meanwhile been continued by the BSI and was intensified then. Within the BMI, a new unit (IT4) for personal ID cards, citizens' registry and passports was established. This unit concentrated on specifying and introducing the electronic passport including biometric face data of the first generation and already opted for digital fingerprints in a second generation.[14]

In fact, digital passports were introduced rather fast and smoothly. First drafts for the revision of the ID card law were produced in 2008. However, when the time for parliamentary treatment came closer, in contrast to the launch of the second generation of the e-pass, heavy public debates arose about the intended inclusion of digital fingerprints. An electronic storage of digital fingerprints outside the chip in databases of public agencies had already been excluded in connection with the e-passport. The local authentication of the holder via his fingerprints is only conducted between the chip and the scanner.

A first rough concept for the ePA was submitted in Spring 2008. The parliamentary and public debate almost exclusively concentrated on the planned inclusion of digital fingerprints—the online authentication function on the new eID card did neither receive much attention nor did it cause any concerns.[15] After parliamentary hearings and debates with the Data Protection Officers at federal and state level, a compromise was finally achieved that the inclusion of fingerprints should be optional in order to allow those citizens who wanted to use the eID card as a travel document to file them, while others did not have to (second rough concept of July 2008,[16] draft bill October 2008[17]).

[14] Following the European Directive EC 2252/2004, standards for security features and biometrics in passports.

[15] This has been corraborated by interviews with the speakers of the four political parties in Federal Parliament.

[16] http://netzpolitik.org/wp-upload/bmi_epa-grobkonzept-2-0_2008-07-02.pdf.

[17] http://dip21.bundestag.de/dip21/btd/16/104/1610489.pdf.

After Federal Parliament had passed the law in December 2008, the Federal Council (Bundesrat), the second chamber composed of representatives of the 16 German federal states (Bundesländer), agreed to the bill in February 2009.[18]

Since the end of 2008, BMI and BSI planned and carried out pilots and application tests in cooperation with service providers mainly from business, but also from public administration. At the end of 2008, a call for application tests was launched. Thirty service providers were selected in June 2009 to set up and test the electronic identification proof of the eID card for their respective services within a centrally coordinated application test starting October 2009,[19] so that well functioning services will be available when the first eID cards will be issued in November 2010.

Administrative and legal framework

The first steps of the German ID card

A personal ID document as proof of citizenship and identity was first introduced by an ordinance in 1938 under the National Socialist Regime (Third Reich) on the basis of a law passed in 1937. For conscripts and Jewish citizens, this ID document became obligatory. Up to then, proofs of identity in the form of non-obligatory passports were the rule (cf. Hornung 2005). In 1939, the ID document for persons from the age of 15 years became compulsory. It was made of grey, linen-reinforced paper (105×148 mm) and contained a photo, registration data, description of the holder, place and date of issue, issuing office, the signature of the issuing public servant and, if the holder was a Jewish citizen, a fingerprint. In 1938, a new registration ordinance as well as a new registration system were introduced, which were the basis for the issuing of ID documents. From then on, relocations were registered at police offices, hotel guests were registered and a census was held, thus providing the basis for a population register.

After the Second World War, the old ID documents were provisionally further used, until in 1951 a new version was introduced under a new ID document act (cf. Aly and Roth. 2000). From 1951 on, a smaller booklet still made of linen-reinforced paper was used as ID document for citizens of the Federal Republic of Germany. Blanks were produced centrally by the Federal Printing Office and sent to the local registration offices, where the booklets were personalised, i.e. furnished with the data and the photo of the applicant.

The machine readable ID card as direct predecessor of the ePA

In 1987 a machine readable ID card[20] in the format ID-2, which had been planned since 1978 was introduced. It was still made of paper, now embedded into special

[18] http://www.bmi.bund.de/cae/servlet/contentblob/607490/publicationFile/35245/eperso.pdf.

[19] http://www.bmi.bund.de/cln_095/SharedDocs/Pressemitteilungen/DE/2009/06/epa_anwendertest.html?nn=294838.

[20] The Machine Readable Zone (MRZ) is due to international standardization by the ICAO (International Civil Aviation Organization).

laminate. Besides the usual visual personal data (front: photo, name, date and place of birth, nationality, duration of validity, signature, ID card number; rear: address of residence, height, colour of eyes, issuing agency, date of issue) it includes a field for the automatic optical reading of name, first name, date of birth, serial number and date of expiry of the ID card. In order to prevent abuse of the ID card by readout, which is a matter of seconds, no further data concerning the holder has been included in this field (Büllesbach 1984, 113). ID cards are registered in a separate ID card register at the local registration offices with their serial numbers.[21] However, the ID card act explicitly forbids using this serial number for the automatic retrieval of files in the public sector as well as for identification purposes in any administrative process.[22] Police and custom agencies are allowed to use the ID card for visual authentication and to check the validity of the card and the identity data on the card. In the non-public sector, it is strictly prohibited to use the ID cards for automatic retrieval and setting-up of data files (cf. Kauß 1984).

In contrast to the previous paper ID document, the machine-readable ID card with a validity of 10 years is personalised, printed and laminated by the Federal Printing Office in a photo-chemical production process. Citizens apply for it at a local registration office, then the data is sent to the Federal Printing Office; after production and delivery, the ID card has to be picked up personally at the registration office, where the congruence of photo and personal appearance is checked.

As the eID function is linked with the new eID card as the mandatory token, the political structures, the administrative embedding and the predecessor ID card become increasingly important for this innovation.

Administrative structures—registration and registers

In Germany, the operation of public administration functions is assigned to the local municipalities by constitution. Legislative authority for most governmental sectors lies with the parliaments of the federal states, and except for only a few issues of concurrent legislation of national and state law, local municipalities have almost full autonomy on how to provide public services.[23]

The source of the citizens' identity data is the population register referring to the personal data of the register of births, deaths and marriages, which is kept in the registration offices. Based on this data, the ID card, which serves for authentication purposes only, is generated. When the ID card is issued for the first time or has been lost, identity has to be proven by the birth certificate. For subsequent issues the old identity card is required. The law does not allow for using the serial number for personal identification or as a unique identifier in the registries.

Citizens registers, as mentioned above, are kept by the local registration offices of the more than 5,000 municipalities, but in several of the 16 federal German states the local registration data is sent to an integrated database on state level to allow for 24 h

[21] § 2a (1) 2. PAuswG 1986 (PAuswG—Personalausweisgesetz—ID card act).
[22] § 4 PAuswG 1986.
[23] For details see eGovernment Factsheet Germany Country Profile http://www.epractice.eu/en/document/288240.

availability for police access, which some local offices can not provide as they still keep their register on paper cards.[24]

Up until 2007, the legal basis for citizens' registries lay in state law under a federal framework law. In 2007, legislative authority shifted to the national level, although organisational responsibility still rested with the federal states. A draft for a Federal Registry Act has been published, but it is not yet decided whether there will be one central citizen registry or only a federation of 16 state registers. A nation-wide standard for the exchange of registration data called X-meld, established by a federal directive, allows for the interoperability of the diverse local registration databases (Kubicek and Wind 2004).

The previous ID card law

The design of the future eID card and the corresponding administrative procedures are regulated in the ID Card Act (Personalausweisgesetz - PAuswG). The existing act for the machine-readable ID card issued in 1987 regulated (Hornung and Roßnagel 2009):

- the obligation of German citizens from the age of 16 to hold either an ID card or a passport,
- the visual data on the card and the content of the machine-readable zone,
- application procedure for and issuance of the card,
- the ID card register, especially the processing and use of data on file,
- data protection, especially for the serial number and its use,
- the ID card's use in public and non-public areas.

An important amendment of this act was made by the coalition of SPD and Green Party (SPD Minister of the Interior Schily) within the anti-terror package law of 2002, which was an immediate reaction to the terrorist attacks of 9/11. According to this amendment, the ID card may include biometric features, which were not defined at that time; rather the question of biometric features was left to be defined by another federal law later on.

Data protection

In Germany, data protection legislation was initiated in the Federal State of Hessen in 1970, influencing the federal data protection law in 1978. Its basic approach is that the collection and processing of personal data is prohibited unless a law is passed that for specific circumstances explicitly says otherwise. There are different rules for the public and the private sector. For the public sector, permission has to be granted by law separately for each case ("Gesetzesvorbehalt") according to the principle of proportionality and the principle of collecting and processing not more data than needed for a specific circumstance. In the private sector, permission may be given by contract or be assumed if it is in the interest of the operator and no infringement of the interests of the person concerned is to be expected.[25] The need

[24] For details see Country Profile IDA BC report and the Good Practice Case description of Lower Saxony (EGOV-IOP).

[25] § 28 BDSG (Bundesdatenschutzgesetz—federal data protection act).

for legal permission as well as the principle of appropriation and a division of power concerning citizens' data were confirmed by the census decision of the Federal Constitutional Court in 1983 (Sule 1999: 49f.). German constitution allows members of parliament to submit any law issued by Federal Parliament to the Constitutional Court to check the accordance with these principles. In the past, several laws initiated, elaborated and confirmed by federal government and passed by Federal Parliament were rejected by the Court as not conforming with the constitution and thus had to be revised. However this did not happen with regard to the law on the new electronic identity card.

To supervise the data protection regulations, the German Data Protection Law stipulates a Federal Data Protection Commissioner who has free access to all public institutions and documents, can address the German Parliament at any time and can advise and recommend improvements of data protection regulations to the federal government, but does not have to be formally consulted in the legislative process. Usually, there is an informal consultation, and he is also invited to public hearings of the parliamentary committees. He submits an activity report to the Federal Parliament once every 2 years.[26]

The new eIDMS and the new eID card

eID card characteristics

Figure 2 shows the old ID card, Fig. 3 the new eID card. The new ID card will be smaller than the old one and have the size of a credit card (ID-1). The characteristic features for visual inspection including the photo of the holder remain unchanged, although arranged and designed differently due to the changed card body. The Federal Police Office insisted on keeping the size of the photo of the previous ID card as well as the letter size to allow for the same ease of use and quality of visual inspections. As a contact chip would have taken too much space on the smaller card, this problem was resolved by using an RFID interface.

However, the main reason for introducing the RFID interface was to seek conformity with the electronic passport. On both documents, the RFID chip allows for the storage of biometric features (face photo and fingerprints).[27]

The contactless RFID chip according to ISO 14443 allows for three functions:

- an authentication function, which can be either activated or deactivated (at the registration office) without access to biometric data (opt in);
- electronic travel document control according to the ICAO standard with biometric data (photo mandatory and fingerprints optional), compatible with the e-pass;
- an eSignature function as the chip is certified as a secure signature creation device. However, the certificate has to be purchased separately by the eID cardholder (opt in).

[26] § 21–26 BDSG.
[27] See subsection "The travel function and identity data access".

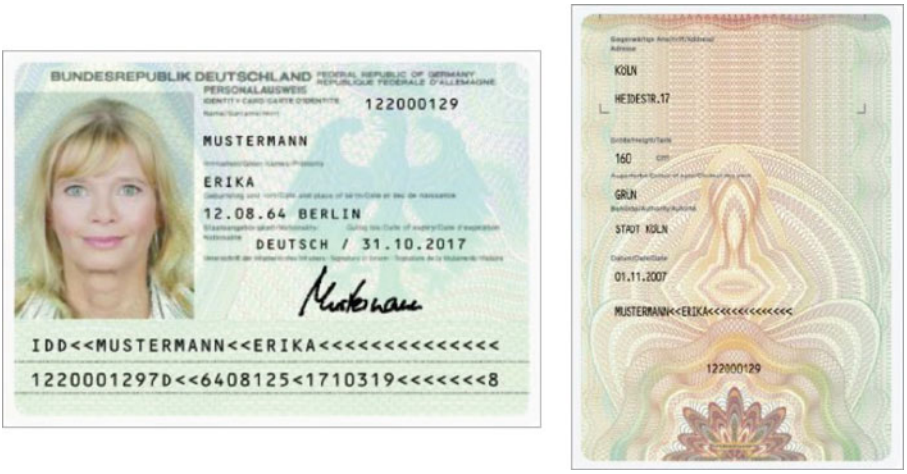

Fig. 2 Present ID card

The machine-readable zone is kept on the backside of the card. Data of the machine-readable zone, which are stored electronically on the chip as well is: type of document, issuing state, surname, first name, document number, nationality, date of birth, expiry date, control sum (ICAO standard). Citizens who hold a passport do not have to hold an ID card in addition. eID cards are valid for 10 years. The cost for citizens has not yet been fixed. The target is to balance costs and benefits for the citizens,[28] estimated to range between 20 and 30 Euros.

Legal basis: the new ID card act

The new ID Card Act[29] takes many regulations from the old law apart from the regulations of the three new functions. It explicitly addresses the eID card's authentication function even in the title and deals with electronic signatures as well (cf. Hornung and Roßnagel 2009). The regulations concerning the ID card register, data protection and limitations for use in the public and non-public sector have been further elaborated.

The electronic authentication function

Paragraph 18 regulates the eID card's authentication function: "The holder of the ID card, who must be at least 16 years of age, can use his ID card to electronically prove his identity to public and non-public units" (translated by authors). In order to adhere to privacy principles, complex technical and administrative procedures have been established and precisely regulated in the act: service providers always have to get authorised to access the identity data on the chip.[30]

[28] http://www.bmi.bund.de/cae/servlet/contentblob/136590/publicationFile/15285/Innenpolitik_3_2008.pdf.

[29] Gesetz über Personalausweise und den elektronischen Identitätsnachweis (PAuswG), 2009 BGBl 1, p. 1346.

[30] § 21 PAuswG implies a legal business purpose (no address trading) with necessity of data and observance of data protection regulations.

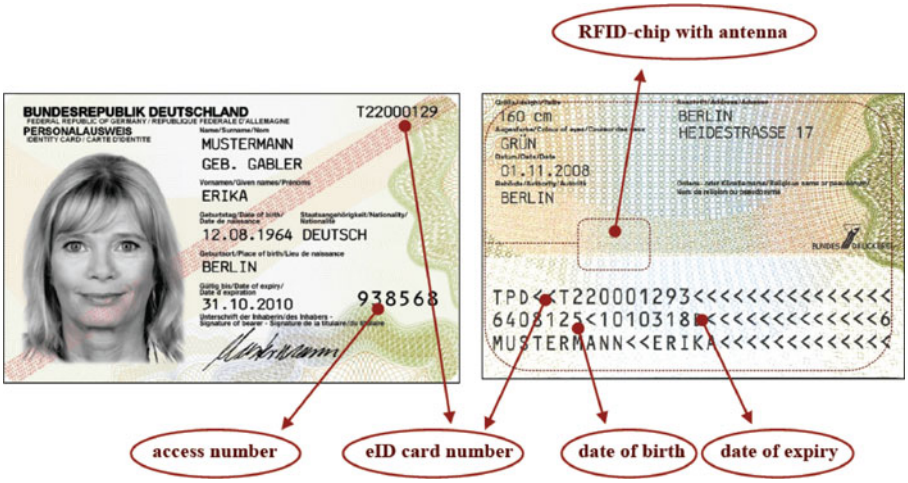

Fig. 3 New ID card (starting Nov. 2010)

Authentication is voluntary and can be either activated or deactivated in the registration office. The data is only transferred if a 6-digit PIN for the eID card is entered.[31] A data-protection friendly pseudonym function is included allowing for the recognition of the eID card without any transfer of personal data, e.g. for age verification.[32]

For the new eID component of the eID card, some established technologies of the second-generation e-pass are employed. However, they have been further developed because they are used with non-governmental card readers and with the Citizens' card readers for eGovernment and e-business applications as well (cf. Eckert and Herfert 2008; Feld 2009). As the data is exchanged via the insecure Internet, the communication connections have to be protected.

To enhance privacy and security, the law requires a double-sided, mutual authentication. While in the other European countries, the eID is used for authentication of users by the service provider, in the German solution citizens are enabled to authenticate the service provider as well and check his data requests. To fulfil these requirements, new security protocols were introduced and combined with existing ones. The EAC (Extended Access Control) protocol used for chip authentication with the e-pass of the second generation was amended by a new protocol called PACE (Password Authenticated Connection Establishment) developed by the BSI: with the PACE procedure requesting a PIN entry, a safe connection between RFID reader and eID card is established by which the terminal of the service provider can authenticate itself to the eID card by means of a terminal certificate. In the next step, the eID card authenticates itself at the terminal by verifying the authenticity of its chip. Moreover, the eID card sends a lock identifier

[31] § 2 (10) PAuswG.

[32] § 2 (5) PAuswG: Each service provider has to register and gets an identification number which is part of his authorisation certificate and which together with the individual code of each ID card serves to calculate an area-specific code. This code is communicated to the service provider as a pseudonym.

to the terminal, which then starts a query in an eID card revocation list. Only if the eID card with its eID function is not blocked, the eID card is accepted as authenticated. Now a safe and encrypted channel is established and the intended data transfer can start.

The security procedures used enable

- a safe connection between eID card, card reader and provider terminal; any unintended readout is prevented by the required authentication.
- By using a personal 6-digit PIN, authentication can be linked to a person (2-factor authentication: possession and knowledge).
- Access to the data fields of the eID card is only possible with the authorisation certificate of the service provider and can be defined separately for each data field.

From a user perspective, the double sided authentication process can be described in the following way[33]: When an individual wants to order a product or to apply for an official document, he accesses the eCommerce or eGovernment website of the corresponding service provider, which at some stage of the process demands an authentication. For this purpose, the service provider sends its access certificate[34] providing information on its service and its access authorisation to selected data fields of the eID card. At the same time, the service provider sends a certificate to the RFID reader. At this point at the latest the citizen is asked to put his eID card on the RFID reader. Before a safe channel between eID card and eID server of the service provider is established and thus a data transfer becomes possible, the citizen has to allow the access by entering his PIN. This PIN also gives permission to send the requested data.

The travel function and identity data access

Just as the previous ID card, the new one may serve as passport substitute[35] when travelling within the EU and can be used for border crossing outside the EU on the basis of bilateral agreements as well. Therefore, the standards set by the e-pass according to the ICAO specification have been transferred to the new eID card. Resulting from the revisions of the anti-terror law in 2002, the storage of biometric features had already been announced. The eID card act explicitly regulates the electronic storage of photo and fingerprints: fingerprints are only stored if the citizen requests it,[36] e.g. if he wants to use the eID card as an electronic travel document with the ICAO standard as in the e-pass. If he holds an electronic passport, then he may not opt in for fingerprints on the eID card.

The access to identity data is restricted. Government agencies can read the identity data of the optical Machine-Readable Zone (MRZ) as before, or access, with the consent of the citizens (PIN entry), the electronic identity data in the chip with a certified reader. Access to the biometric data is not possible. Only sovereign

[33] Now, at the time of writing, in January 2010, the ordinances regulating the details according to § 34 PAuswG have not yet been passed. Therefore certain details of the process are not yet definitely laid down.
[34] The service provider has to apply for this certification at the Federal Administration Office (Bundesverwaltungsamt, BVA) beforehand.
[35] Directive 2004/38/EG dated 29 April 2004.
[36] § 5 PAuswG.

authorities with a certified reader can access the identity and biometric data on the chip without the PIN of the citizen through the calculation of an access key by a cryptographic technique from the MRZ or the access number printed on the card.[37] Further details for the electronic ID card in January 2010 still await regulation by BMI ordinances.[38]

Signature function

The new ID card act only regulates the design of the eID card as a Secure Signature Creation Device (SSCD) according to § 2 no. 10 of the signature act.[39] The eID card as a SSCD shall be capable of carrying certificates by any registered Certification Authority (CA) in Germany. Any other aspects of digital signatures are regulated in the German Signature Act of 2001.

Applying and issuing procedure of eID card[40]

The procedures for applying for and issuing of the new eID card have not been changed much compared to the previous machine readable ID card. The new features, in particular the digital fingerprints, did not afford any new procedures or equipment, as these are identical with those for the ePassport, which has to be applied for and is issued at the same local registration offices and printed by the same federal printing office.

When citizens apply for the first or a subsequent eID card, the personal data are recorded and checked with the civil register and an eID card file[41] is prepared. In contrast to the hitherto existing process, the biometric data (scanning of photo, manual signature, fingerprints) are electronically recorded; fingerprints are only included if the citizen agrees in writing. These fingerprints are only stored on the chip of the eID card; they are deleted from the files of the registration office and the central printing office after the eID card is issued. Then the citizen receives comprehensive information material on the new functions of the eID card, especially of the authentication function. Finally the citizen checks the data, signs the application and pays the fee for the eID card. The registration office generates an eID card number, checks the data with the eID card register and sends the application electronically to the Federal Printing Office.

After checking the order, the data and the serial number, a pre-produced card body is personalised by writing the biometric data and the eID data on the chip and a key pair for the chip as well as a certificate, and the PIN/PUK plus the code word for the blocking of the eID card[42] are generated. Then the eID card is sent to the issuing

[37] § 2 (11) PAuswG.

[38] § 34 (5) PAuswG.

[39] § 22 PAuswG.

[40] Cf. rough concept for the eID card: http://www.bmi.bund.de/cae/servlet/contentblob/122648/publicationFile/9169/Grobkonzept_Personalausweis.pdf and PAuswG.

[41] Basis for the identity card register, see subsection "Administrative structures—registration and registers".

[42] The responsible registration office and the cardholder can induce a blocking of the eID card by sending the blocking code word to the provider of an eID/eID card blocking list if the document is lost.

registration office while the PIN/PUK letter with a blocking code word is sent to the citizen informing him of the delivery to the registration office. The Federal Printing Office also generates and administers a register of eID card numbers, which collects information on the whereabouts of the produced eID cards without storing personal data.

Later the new eID card is handed over at the registration office. The identity of the citizen is checked by means of the new eID card, the old ID card is turned in or obliterated. With the help of the received information material, the citizen can decide on the use of the eID function, which can be switched off and switched on again at any time at the registration office. The blocking code word, an eID switching-off note and a revocation note are added to the ID card register. Finally the citizen is offered to have a look at the data stored on the chip.

Independent of the issuing procedure at the registration office, citizens can purchase an eSignature certificate on the provider market by registering online using the authentication function and have it uploaded on the RFID chip, which is accordingly prepared.

Application tests

At the end of 2008, BMI launched a call for application tests of the authentication function of the new eID card.[43] Service providers from private and public sectors were invited to develop and test the integration of the authentication function into existing or new online or offline services in order to ensure a sufficient number of useful applications to be ready at the time of issuing the first new cards in November 2010. Of approximately 100 interested organisations from all sectors, thirty have been selected, each for predefined categories, such as simple age verification, bank account opening, insurance services etc. These are technically supported by a competence centre run by a contractor to the Ministry beginning in October 2009. There is also a tender for developing a citizen client, which will be tested in this environment.

Constellation of actors

Figure 4 shows the most important institutional actors during the complete process in the main phase of the development, the ePA phase. This phase differs from the eSignature phase in the mid 90's where originally the Ministry of Research and Technology had the lead on the technological development and the legislation concerning the information society including digital signatures. When the SPD/Green government came into office in 1998, the whole unit was transferred to the Ministry of Economics. But when in 2003 the new ID card was chosen as the token for an eID and online authentication, the BMI became the main actor.

[43] http://www.cio.bund.de/cln_093/DE/IT-Projekte/Leuchtturmprojekt_ePA/Anwendungstest_ePA/anwendungstest_node.html.

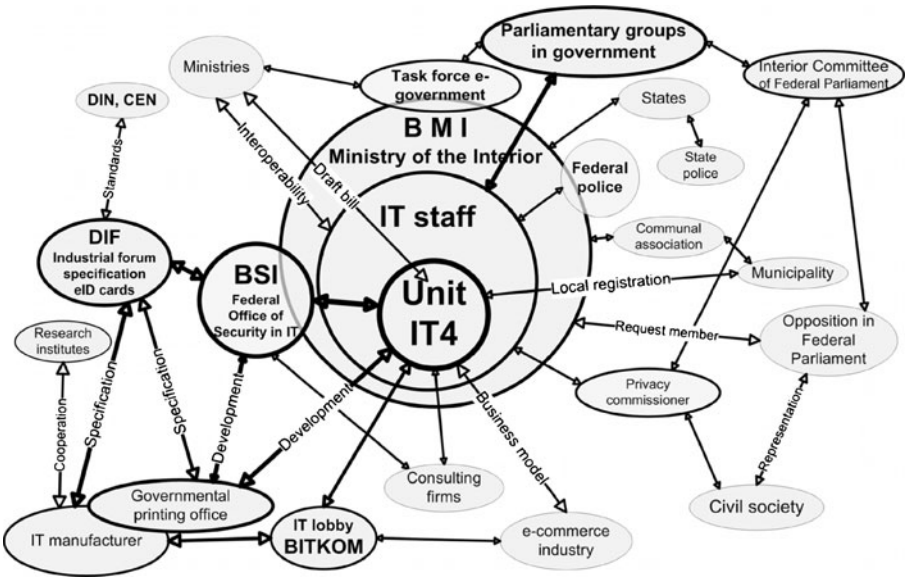

Fig. 4 Main actors in developing the German eID card

Federal Ministry of the Interior—BMI (IT staff, unit IT4)

The unit IT4 of the Ministry of the Interior, since 2005 responsible for the introduction of the eID card, is the leading actor of the process. Combining the responsibility for eID card, civil registry and passport in one unit within the IT staff was a clear political message. The increasing importance of IT for secure authentication as well as for the organisation of administrative processes[44] had already been acknowledged when an independent directorate for IT (IT staff) had been established in 2002.[45] This directorate has been responsible for IT strategy, IT policy and IT security in government, including the development and administration of eGovernment programmes in cooperation with the Ministry of Economics.

Bundesamt für Sicherheit in der Informationstechnik (BSI)

The Federal Agency for Information Security (Bundesamt für Sicherheit in der Informationstechnik—BSI[46]) is a central federal government agency affiliated to the Ministry of the Interior under the guidance of the IT Group. It is the central IT security service provider of the federal government[47] but also acts as a certification authority for IT security certificates requested by any public or private organisation according to common criteria and ISO standards. As a core developer of security

[44] Cf. eGovernment programs since 1999.
[45] http://www.bmi.bund.de/cln_165/SharedDocs/StrukturAbteilungen/itstab.html?nn=109676.
[46] http://www.bsi.de/bsi/leitbild.htm.
[47] Regulated in the act "BSI-Errichtungsgesetz" (BSIG) of 1990, BGBl 1, p. 2834.

technology of the eSignature, the e-passport and the eID card, the BSI is one of the most important technology related actors since the mid-90ies.[48]

IT industry

Relevant parts of the IT industry are the manufacturing industry (chip, hardware and software) and the eCommerce industry. The BSI had involved the manufacturing industry via the DIF (Deutsches Industrieforum) for the technical specifications. Especially the manufacturers of chips and cards, infrastructure and developers of security technology were included in the process.

The applying industry, mainly consisting of eCommerce providers, was involved only in 2008, when the rough technical concept and the draft bill had been finalised and the BMI started looking for attractive applications. Although in several documents by IT industry associations, identity theft was considered to be a high barrier for citizens and consumers to use the Internet for online transactions, and as the authentication function was designed to improve Internet safety and security, big players in eCommerce did not show strong interest by themselves.[49] Rather federal government had to get them on board at the annual IT summit, which was organised by the Federal Chancellery.[50] Ebay Germany could be won to chair a working group dealing with the e-card as well as the authentication function[51] but still did not participate in the application test. German banks raised technological and organisational objections regarding the use of the eID card for online authentication and showed more or less a wait-and-watch attitude.[52] Other big companies from the service sector had to be motivated for participation in the application test by political representatives resp. the BMI.[53] This reluctance can be explained by negative experiences made with the eSignature.

Deutsches Industrieforum (DIF)

In 2004 BMI and BSI invited the German manufacturing IT industry to come together in the German Industry Forum (Deutsches Industrieforum, DIF).[54] With the support of the BSI, industry should get involved in developing the technical and functional specifications (interface definition of chip card, terminal and middleware) for the eID card. Founding members were the card producer Giesecke & Devrient, the Federal Printing Office and the chip manufacturer Infineon. Working group

[48] https://www.bsi.bund.de/cae/servlet/contentblob/487526/publicationFile/27989/BSI_annual_report_2006–2007_pdf., project interviews BSI and BMI.

[49] http://www.javelinstrategy.com, http://www.ftc.gov/sentinel/reports/sentinel-annual-reports/sentinel-cy2008.pdf.

[50] https://it-gipfelblog.hpi-web.de/wp-content/files/documents/dritter_gipfel/kurzvorstellung_ag4.pdf.

[51] EBay Germany was president of working group 4: “Security and Trust in IT” on the 3rd IT-Summit.

[52] http://www.zka-online.de/uploads/media/081103_Stn_Elektronischer_Personalausweis.pdf.

[53] Project interview with representatives of industry.

[54] http://www.bitkom.org/files/documents/3_ECC_Meister_GD%281%29.pdf.

Table 1 Government coalitions in German federal parliament

Year	Government coalition	Orientation
1994–1998	CDU/CSU+FDP	Conservative-liberal
1998–2002	SPD+Green Party	Left-ecological
2002–2005	SPD+Green Party	Left-ecological
since 2005	CDU/CSU+SPD	Conservative-left (great coalition)

members, resp. members of a commenting circle, are enterprises such as Philips, Siemens BS, Microsoft and T-Systems (2005–2007). It was and is their intention to establish the features of the eID card as German standards (DIN) and to bring them into European standardisation bodies (CEN) in order to promote the German eID solution internationally.[55]

IT industry association BITKOM[56]

BITKOM (Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V.) bundles the interests of the IT industry and represents them vis-à-vis government. With regard to eID and the eID card, two working groups were established: the technical committee on chip cards and ID card systems and the technical committee on electronic identities. Members were partially identical with those of the DIF. Since 2006, BITKOM accompanied the introduction of the eID card by supportive activities of its working groups. The improvement of security on the Internet is the main reason for their support.[57]

Political parties

The influence of political parties depends on their representation in government. Although there was a change from a SPD/Green to a CDU/SPD government coalition during the development process (Table 1), this did not affect the development of the authentication function, but only the storage of digital fingerprints.

The possibility of including digital fingerprints had been laid down in a law on behalf of a Minister of the Interior from the Social Democratic Party. But details had been left to future legislation. When the revision of the act on personal documents took up this issue, the Social Democrats in Federal Parliament had moved into a big coalition with a new Minister of the Interior from the Christian Democratic Party and was no longer ready to agree on a mandatory collection of digital finger prints. The compromise was that the storage on the eID chip became optional.

[55] Project interviews BITKOM and industry experts.
[56] http://www.bitkom.org/de/wir_ueber_uns/17703.aspx.
[57] http://www.bitkom.org/files/documents/Positionspapier_ePA_2009.pdf, http://www.bitkom.org/de/presse/56204_53405.aspx.

The opposition parties had several concerns about privacy but hardly any power to influence the outcome of the legislative process.

Federal Criminal Police Office (BKA) and Federal Border Guard (BGS)

In Germany, the police force is in the responsibility of the federal states. They are the employers of policemen and responsible for the technical infrastructure and legislation under national framework law. Thus the federal states have to adapt their technical infrastructure to the new means of visual authentication, in particular for reading data from RFID chips and checking digital fingerprints. The Federal Criminal Police Office (Bundeskriminalamt, BKA) is a subordinate agency of the BMI, and to some extent aggregates the requirements of the police, even if not heavily involved in visual inspection itself. As mentioned before, the requirement of keeping the size of the photo and the letters for the written data on the card came from the BKA.

The Federal Border Guard (Bundesgrenzschutz, BGS) is also affiliated to the BMI. Since the eID card as a travel document has the same features as the e-passport, there has been no reason for them to take additional influence.

Federal states

The legal authority for ID documents lies at the national level, and the authority for civil registries recently has been shifted to that level as well. But as the federal states are in control of the public administration and have the authority over the police, they have a strong voice on matters of identity and authentication. Their regular arena to seek consent is the Conference of the Ministers of the Interior, where the federal minister and his colleagues from the 16 federal states come together to discuss issues of public safety, administrative reforms, coordinate ordinances as well as to agree on shared funding. The concepts and draft bills for the eID card have been agreed to by this conference.

In addition, the law had to be agreed upon by the Federal Council after passing Federal Parliament. There was some discussion about additional cost the states and local authorities will be bearing for new equipment, but finally the law was agreed upon without any changes.

Municipalities

Although the local municipalities have to provide for the application and issuance process including the digital collection of fingerprints, they have neither been consulted formally, nor have they raised their voice. This is due to the fact that they are also responsible for the issuance of the electronic passport and had to employ the necessary equipment and set up the respective processes already for this purpose. As providers for eGovernment services, they are expected to employ the authentication function. They did not oppose the certification procedure in public debates. Only a few local communities have shown interest in participating in the application field test. They all have negative experience with digital signatures and at present take a wait-and-watch position similar to the banking industry.

Table 2 Importance and power of political actors by policy fields

Political actors by policy fields	Significance of actors (1 = low, 3 = high)[a]
Security/police/interior	3
Public administration	2
Economy/industry/trade	1
Finance	1
Social issues/health	1
Chancellery/cabinet	1

[a] Derived from actor constellations and interviews

Federal Commissioner for Data Protection and Freedom of Information (BfDI)

The tasks and the institutional position of the Federal Commissioner for Data Protection and Freedom of Information,[58] as laid down in the federal data protection act, have already been described (cf. 3.5). Although he is independent in his decisions, his office is also affiliated to the BMI in administrative terms. Right from the beginning of the discussion, he opposed the capturing and storage of digital fingerprints. He saw the danger of total capture of all fingerprints although for the ID cards in contrast to the passport no EU obligation exists. But he reacted positively on the regulation of the authentication function as the eID function is designed privacy-friendly.[59]

Influence of policy fields

The introduction of the eID card is a "multi-field innovation": originated in the field of eGovernment, which itself cuts across the established policy fields. Federal eGovernment programmes were coordinated by the Ministry of the Interior, funded by programmes in the budget of the Ministry of Education and Research with a heavy involvement of the Ministry of Economics, which has been responsible for e-commerce, telecommunication regulation etc.

The eID in the form of the eSignature had been located in the fields of eGovernment and Commerce. When the eID card was chosen as token, the eID issue was considered only as an add-on in the development of a new more secure ID card and an option for extended personal inspection. Accordingly, the policy field of security and police matters became dominant (Table 2).

Although the authentication function according to the introductory remarks of the ID card act is supposed to improve the security of e-commerce, the policy fields of economy, industry and trade were of marginal influence in terms of the participation of representatives of the respective ministry, parliamentary committees or even enterprises themselves. Officials in the Ministry of Economics, in charge of

[58] http://www.bfdi.bund.de/IFG/Dienststelle/Aufgaben/Aufgaben_node.html.
[59] http://www.heise.de/newsticker/meldung/Grosse-Koalition-ringt-um-Einigung-beim-elektronischen-Personalausweis-178009.html.

eSignature, media law and e-commerce, did not try to influence the design of the authentication function, the certification process for service providers from the private sector or the regulation for providing an eSignature on the eID card.

Conclusion: paths changes and creations

The development of an eID function for online authentication in Germany has taken more than 10 years. Five years passed because of the misunderstanding that the eSignature would allow for the authentication of individuals without requiring further measures. When such a need was finally recognised and the new eID card was selected as the only token for authentication, it was influenced by a controversial public safety debate, concentrating on the collection and storage of digital fingerprints, which never had been considered to be used for online authentication but only for local inspection and border control. Even when the eID card had been chosen, the electronic passport was given higher priority and the fingerprint discussion concerning the eID card led to further delay in the legislative process afterwards. The eID authentication function was not discussed in public during this time. The time span between the passing of the law (February 2009) and the start of the roll-out (November 2010) is due to logistical problems described in the introduction chapter.

According to the conceptual framework presented in the introductory chapter (Kubicik 2010), we assume that innovation processes with a high degree of path continuation develop more smoothly and faster than those with path changes or creating new paths. In our conclusion we will look at the innovation process from this perspective with regard to organisational, technological and institutional aspects.

Organisational paths

The definition of an ID as well as the procedures of administering IDs is first of all an organisational and not a technological issue. With the introduction of the eID and the new ID card, the definition of the identity of a citizen, i.e. the attributes assigned to an individual, have not been changed for online authentication, but for local physical authentication. Thus in some sense the eID is not simply a case of path continuation. The visual data on the new ID card and in the machine-readable zone are the same as on the previous ID card. However, they are stored on the chip as well. New attributes are a digital photo and digital fingerprints. They do not constitute the creation of a new path but have to be considered as a path change or merging of two paths: the old ID card and the e-passport. These attributes have already been introduced as new features of the e-passport without much opposition. Local municipalities have deployed the technology for collecting digital fingerprints for the new passports and will use it for the new eID card as well. The procedures for application, production and delivery remain unchanged. Why opposition emerged against the inclusion of digital fingerprints will be discussed in the context of the institutional path.

A path creation took place with regard to the certification requirements of service providers asking for online authentication. There is no predecessor for a similar

certification procedure for online access to personal data in other sectors in Germany or anywhere else in the world. In order to adhere to the principles of proportionality of German data protection law (cf. Simitis 2006: 328ff), service providers may only access those ID data that are necessary for providing this particular service, i.e. the age in one case, only the name in another case or perhaps only the postal code of the home address to prove that the individual is citizen of a certain local municipality. The novelty lies in employing a technical procedure to guarantee proportionality based on an administrative procedure for a certification process. However, an already existing organisation, the Federal Administration Office (Bundesverwaltungsamt) has been selected as certification authority.

Technological paths

When a paper-based machine-readable ID card is to be substituted by a chip-based card, there cannot be full technological path continuation. Path dependency in this context refers to following technical standards and mainstream trends. As the technological development of IT in general and IT security in particular is highly dynamic, it is important to know at which point in time decisions have been taken. In the context of this research, this concerns in particular the technical specification of the eID function and the token, i.e. the eID card.

When deciding on the technology for national infrastructure innovations, established and fully developed technologies are generally preferred. Important criteria for the degree of establishment of a technology are the international standardisation and the diffusion and acceptance of the standard. In Germany, the specification for the eID card started in late 2004, when the option to decide on the use of RFID on the basis of an ICAO standard established since 2003 was available. As the existing ID card was broadly used as a travel document at that time and this functionality was meant to be continued although a systemic change of border control via the electronic passport had been decided by ICAO, it seemed obvious that the new ID card should be based on the same technology, i.e. RFID chip with digital face and digital fingerprints, both already in full preparation at that time.

The e-pass including a biometric photo was introduced in 2005; digital fingerprints were added in the second generation in 2007. The advantage of choosing this path did not only lie in the compatibility and reduced costs of the equipment for authentication in border control. The positive experiences during the development process, the smooth cooperation with the different partners in the supply chain, the successful technical implementation of the e-pass and broad acceptance by citizens and the public gave reason to expect a similarly technically successful introduction of the eID card.

This choice was corroborated by the requirement of the police to keep the previous size of the photo on the smaller space of the new card, leaving less space for a contact chip. Another discussion concerned the life cycle of contact chips. Credit cards and bankcards usually have a validity of 1–3 years. There is no experience with contact-related smart cards over a period as long as 10 years. Any dysfunction or failure at border control however would cause severe problems. Thus, technical reliability had absolute priority, and the e-pass already had proved this reliability.

These arguments brought forward in interviews with the project managers in the BMI and the BSI, by industry experts and the head of the government printing office are completely convincing. But this raises the question why they have not influenced the decisions taken in other European countries.

However, they do not concern the eID function for online authentication, in particular the dialogue between the chip, the card reader, the citizen client and the middleware on the eID server. In this regard, the e-card API (interface) had to be applied with some additional features, which also adhere to established protocols.

Institutional paths

The technology and the organisation of the eIDMS had to be regulated by a revision and amendment of the existing identity card act. For the eID function, there was no technical and no organisational predecessor. While there were almost no regulatory changes regarding the definition of the eID and its administration, except for the digital fingerprints, a completely new path has been created for the access certification of service providers.

The inclusion of digital fingerprints followed the organisational and technological path of the e-pass, but still aroused strong resistance. This opposition was based on the regulatory consequences of making the fingerprints mandatory on the ID card as well. The same obligation would have changed the freedom of the individual dramatically. German citizens are obliged to hold either an ID card or a passport, and fingerprints on passports are mandatory. Making them optional on the ID card at least leaves the chance to not carry a passport and still being able to travel in the European Union and to several other countries. If the fingerprints on the eID card would have been made mandatory as on the passport, there would have been be no choice left. The constitutional right of informational self-determination only allows for a limitation of individual freedom for the sake of fundamental public concerns. But there is no strong public concern for collecting the fingerprints of the whole population. Rather due to the specific history of mandatory collection of fingerprints in the Third Reich, this was conceived as a threat to collective freedom as well. It was this coincidence of constitutional considerations and historic context that led to the compromise of the storage of digital fingerprints becoming optional. Citizens who do want to use their eID card as a travel document may opt in, while others do not have to do so.

The regulation of the access certificate for service providers established a new organisational path. The regulatory pattern applied, however, is a simple application of the requirements of the federal data protection act. Whenever a public entity wants to process personal data, a law or directive is required which precisely defines which data is to be processed for what purpose and only this particular data may be listed in the respective permits that are necessary for the purposes. As the purpose of the authentication function is the corroboration of the identity of users of different online services, the provider of each service may only ask for those personal data that are necessary for providing this particular service. Accordingly the legal permission of online authentication has to be limited to the data that is necessary in each service context. The innovation was that this obvious legal requirement, only written in the law, has been transposed into technical functionality and thereby

provides a more reliable and trustful way of meeting the objective of increased safety of online transactions on the Internet.

The use of eID

The use of the eID cannot be assessed nor even estimated at this point of time when the application tests have not yet become operational. The justification of the new ID card act expects a medium-term activation of the authentication function of about 60% of the eID card holders, which equals the percentage of Internet users in German population.[60] The double-sided authentication function may become a specific gratification and lead to a demand beyond the regular renewal. But the authentication function is optional, completely new, in terms of Rogers' innovation theory complex, unobservable and not triable (Rogers 2003). Therefore diffusion will depend on the added value which online authentication provides for online services as well as on supportive and promotional measures.

References

Aly G, Roth K-H. Die restlose Erfassung. Volkszählen, Identifizieren, Aussondern im Nationalsozialismus. Frankfurt: Fischer; 2000.

BMI. E-Government 2.0 The Programme of the Federal Government, BMI. 2006a.

BMI. BundOnline 2005 Abschlussbericht und Ausblick. BMI. 2006b.

Büllesbach A. Den Anfängen wehren. Die Entwicklung des neuen Personalausweissystems aus datenschutzrechtlicher Sicht. In: Taeger J, editor. Der neue Personalausweis. Reinbek: Rowohlt; 1984.

Eckert C, Herfert M. Innovative Lösungen mit dem Elektronischen Personalausweis—der Darmstädter Campuspilot. http://www.sec.in.tum.de/assets/lehre/ss09/sms/Eckert_ePA.pdf. 17.04.2009. 2008.

Feld S. Extended Access Control (EAC) und der elektronische Personalausweis (ePA)—Ein starkes Team für eine sichere Zukunft im Netz? IT-Sicherheit. 2009;37–39.

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

Hornung G, Roßnagel A. Der elektronische Personalausweis in Deutschland: Gesetzgebungsverfahren, Einflussfaktoren und Pfade, Paper written under contract with the Institute for Information Management Bremen, funded by Volkswagen Foundation. 2009.

Kauß U. Das neue Ausweissystem—eine Lücke wird geschlossen. In: Taeger J, editor. Der neue Personalausweis. Reinbek: Rowohlt; 1984.

Kubicek H. Conceptual framework and research design for a comparative analysis of national eID management systems in selected European countries. Identify in the Information Society, Special Issue, 2010.

Kubicek H, Wind M. Integriertes E-Government auch im föderalen Staat? DFK. 2004;43:48–63.

Reichl H, Roßnagel A, Müller G. Digitaler Personalausweis. Eine Machbarkeitsstudie. Wiesbaden: DUV; 2005.

Rogers E. Diffusion of innovations. New York: Free; 2003.

Simitis S. Bundesdatenschutzgesetz. Kommentar. Baden-Baden: Nomos; 2006.

Sule S. Europol und europäischer Datenschutz. Baden-Baden: Nomos; 1999.

[60] Estimation without giving details in Draft bill PAuswG 07.10.2008: http://dip21.bundestag.de/dip21/btd/16/104/1610489.pdf.