Computer Law & Security Review, Volume 26, Issue 2, 2010, Pages 151-157,
http://dx.doi.org/10.1016/j.clsr.2009.11.002

[Page 151]

An ID card for the Internet – The new German ID card with "electronic proof of identity"*

Gerrit Hornung, Alexander Roßnagel

University of Kassel, Germany

ABSTRACT

The personal ID card is a document carried by most Germans[1], but rarely used. This could change in the future: According to the new law on identification cards and electronic proof of identity (Gesetz über Personalausweise und den elektronischen Identitätsnachweis, PAuswG), the ID card, with its proof of identity, will gain a new functionality, making it applicable for diverse Internet transactions. Functionally, the electronic proof of identity corresponds to existing non-electronic personal proof of identity guidelines in legal and business connections. However, its concrete, technical application opens up many issues regarding contracts and data privacy laws. On both the legal and the technical level, the German approach departs from other European countries, as it strictly distinguishes the electronic proof of identity from the electronic signature function, which the new ID card also provides. It remains to be seen whether the various projects of the EU Member States will become legally and technically interoperable in the near future.

1. Background

German personal ID cards, in accordance with § 20 para. 1 PAuswG, serve, as in other countries, as identification and legitimacy documents in public and non-public spheres of life. At the same time, for citizens, they are simply visual printouts of the "ID card system", which includes further organisations and institutions. From an organisational point of view, ID card public authorities,[2] the ID card manufacturer[3] and the respective control entities[4] are especially significant. An important

---

* Revised version of an article which was originally published in *Die Öffentliche Verwaltung* 32 (2009), pp. 301 ff.

1 However, the already existing mandatory identification measure, in accordance with § 1 para. 1 PAuswG, includes no obligation to carry identification with oneself in Germany; see W. Süßmuth/H. Koch, *Pass- und Personalausweisrecht*, 4th Edition, § 1 PAuswG para. 19. § 111 of the Federal Administrative Offence Act (Ordnungswidrigkeitengesetz) only inflicts penalties when information on identity is false or omitted when presented to official authorities, public officers and soldiers, however not when ID has not been presented; see G. Hornung, *Die digitale Identität*, 2005, pp. 47 ff. (also available at http://kobra.bibliothek.uni-kassel.de/handle/urn:nbn:de:hebis:34-2007113019808).

2 These are appointed by the German Länder authorities, in accordance with § 7 para. 1 PAuswG. ID card public authorities are usually part of the same administrative unit as registry offices. They are organisationally linked to these offices and only functionally separated, see W. Süßmuth/H. Koch (above n. 1), § 2b para. 38; H. Wollweber, in: A. Roßnagel (Ed.), *Handbuch Datenschutzrecht*, 2003, Ch. 8.5, para. 6.

3 This task was, according to previous legal status, specifically assigned to the federal print office (Bundesdruckerei GmbH), see G. Hornung (above n. 1), pp. 357 f., while, now, in accordance with § 4 para. 3 PAuswG, the Federal Ministry of the Interior decides upon the ID card manufacturer.

institution is ID card registering, which, according to § 23 para. 1 PAuswG, is to be administrated by the local ID card public authorities.

With the German reform of federalism of 2006,[5] the exclusive legislative competence for the register and identification system was assigned to the Federal Republic, through the new Art. 73 para. 1 No. 3 of the German Basic Law (Grundgesetz). With the new law on identification cards and electronic proof of identity, the Federal Parliament (Bundestag) has made use of this competence.[6] This act was pronounced on June 18, 2009,[7] and, in terms of the significant regulation contents, comes into effect on November 1, 2010. In turn, it is moving the registration reform ahead, which is also under progress at the federal level, yet still politically controversial.

With the commencement of the act, the new ID card is to gain three new functions. Firstly, like the new passport,[8] the card will be equipped with a contactless RFID chip, in which biometric facial data will be saved. Fingerprint data, which is obligatory for the passports throughout the EU Member States, is only stored upon request, in accordance with § 5 para. 9 PAuswG. Secondly, pursuant to § 22 PAuswG, the ID card will serve as a secure-signature-creation device, in the sense of § 2 No. 10 of the German Act on Electronic Signatures (Signaturgesetz) and Art. 2 No. 6 of the European Directive on Electronic Signatures, thus offering the possibility of generating qualified electronic signatures. This function of the German ID card is optional and holds additional costs for the card holder.[9] The market-based German approach as regards to certification-service-providers will not be altered, i.e. the qualified certificates for the official German ID cards will be issued by private providers.

In contrast, the third function, the electronic proof of identity, will be a standard part of every ID card. The use of this function is, in accordance with § 10 PAuswG, optional and will be switched off when not wanted. As the electronic proof of identity holds no additional costs outside of the regular ID card fee for the cardholder and also opens up trading possibilities in e-Government and e-Commerce, it can be expected that an increasingly large number of electronic proof of identity functions will be switched on. With such a card, the cardholder will obtain a vastly functional equivalent to the existing ID card and its use in the “offline world”.

Hence Germany will follow the approach of several European countries which provide the functions of electronic signature and electronic authentication for their citizens through the national ID cards. In different technical and legal forms, e.g. Belgium, Estonia and Finland have already introduced such documents. The vast majority of the other countries are to follow soon.[10]

---

4 Possible use of the ID card is not only limitied to police and criminal law proceedings, even though use in this area is especially common. For examples see G. Hornung (above n. 1), pp. 56 ff.

5 Basic Law Amendment Act of August 28, 2006, Federal Law Gazette (Bundesgesetzblatt) I, pp. 2034.

6 For the legislative history see Printed Matter of the Bundestag (Bundestags-Drucksachen) 16/10489.

7 Federal Law Gazette (Bundesgesetzblatt) I, pp. 1346.

8 For legal issues relating to the electronic passport, see A. Roßnagel/G. Hornung, “Reisepässe mit elektronischem Gesichtsbild und Fingerabdruck”, *Die Öffentliche Verwaltung* 28 (2005), pp. 983 ff.; A. Pallasky, *Datenschutz in Zeiten globaler Mobilität*, 2007, pp. 30 ff.; G. Hornung, “Fingerabdrücke statt Doktortitel: Paradigmenwechsel im Passrecht”, *Datenschutz und Datensicherheit* 31 (2007), pp. 181 ff.; as regards biometrics in identification procedures, H. Reichl/A. Roßnagel/G. Müller, *Digitaler Personalausweis*, 2005; G. Hornung (above n. 1).

9 For the possibilities and challenges presented by the combination of the ID card and the signature function, see in detail A. Roßnagel/R. Gitter, in: H. Reichl/A. Roßnagel/G. Müller (above n. 8), pp. 91 ff.; 219 ff.; M. Strasser/G. Müller/A. Roßnagel/R. Gitter, ibid., pp. 243 ff.; G. Hornung (above n. 1), pp. 319 ff.

10 See European Network and Information Security Agency (ENISA), *Privacy Features of European eID Card Specifications*, 2009 (available at http://www.enisa.europa.eu/act/it/eid/eid-cards-en), pp. 5 f.

On the European level, there is so far no possibility to regulate on national ID cards. However, this will change upon the entry into force of the Treaty of Lisbon, which contains a community competence in Art. 77 para. 3. In the meantime, the European Commission has tried to focus on technical issues instead of legislative measures.[11] As the interoperability of electronic identities is a key issue for the use of electronic services in the common market,[12] the Commission is running a three-year pilot project to get national ID to work in different countries. The project, called "Secure idenTity acrOss boRders linKed (STORK)", was launched in May 2008, and the final reports are due in 2012.

First results are available through the STORK website,[13] including a report on "legal interoperability".[14] The aim of project is to establish a European interoperability platform for electronic identities that will allow citizens to establish new electronic relations across borders, just by presenting their national electronic identities. Taking what the consortium calls a "user-centric" approach, STORK focuses particularly on data protection issues.[15] Within the project, the German concept of the electronic proof of identity, as explained in the further course of this article, is introduced by the German Bundesamt für Sicherheit in der Informationstechnik (BSI, Federal Office for Information Security).

2. Functions of the identification system

In order to comprehend what this developmental entails and to grasp the possible uses in electronic legal and business transactions, it is helpful to clarify the function of identification systems.[16] Fundamentally, ID cards are not necessarily required for identification processes. Very small communities can do without them as their members are familiar with one another. In somewhat larger units, ID cards are also not necessary, as long as there are reliable third parties who are well-known to both individuals and therefore able to securely confirm the identity of the other respective individual. However, the more developed, mobilised and differentiated

[Page 153]

social systems become, and the more abstractly their interaction processes develop, the more frequent individuals have contact with people whom they are not personally acquainted with. Then, it is more frequently necessary to secure the identity of one's counterpart. In such a situation, ID cards offer proof of identity in that an all-round credible, recognised authority can confirm, in a document, that a certain natural person has characteristics like surname, first name and address attributed to him or her.[17]

The first precursors to today's ID cards were written references and other signs, dating back to antique times. Through their (mere) possession, those travelling could attest their affiliation to an association or an authority. Proof of identification papers for larger groups, dating back

---

11 See, e.g., European Commission, *Action Plan on e-signatures and e-identification to facilitate the provision of crossborder public services in the Single Market*, COM(2008) 798 final, pp. 10 ff.

12 On the problems, see European Network and Information Security Agency (ENISA), *Report on the state of pan-European eIDM initiatives*, 2009 (available at http://www.enisa.europa.eu/act/it/eid/eidm-report).

13 See http://www.eid-stork.eu.

14 R. Leenes, B. Priem, C. van de Weil, *D2.2 – Report on Legal Interoperability*, 2009 (available at http://www.eid-stork.eu).

15 Thus following the work of the ENISA (above n. 10).

16 For the following, see G. Hornung (above n. 1), pp. 29 ff.

17 In technical terminology, electronic authentication procedures refers to a system of "credentials", see also M. Hansen/M. Rost, "Nutzerkontrollierte Verkettung", *Datenschutz und Datensicherheit* 27 (2003), pp. 293 ff.

to as early as the 15th century, have been discovered in Europe.[18] During the time of National Socialism, a general intrastate compulsory ID card was introduced in Germany, and thereafter maintained.[19] In the Anglo-American region there are, in contrast, historically no governmental ID cards. However, this appears to be changing.[20] Nonetheless, these countries can also not do without some form of identification for economic and administrative processes. They use governmental, part-governmental and private functional equivalents to ID cards, such as social insurance numbers, driver's licenses and company or service ID cards.

When a governmental identification system exists, then an "official" identity is *produced*, which can then be *reproduced* in subsequent identification processes. The state makes use of instruments for compulsory registration and identification for each one of its citizens in order to establish such an identity. This is updated over longer periods of time not only in the form of official ID cards and passports, but also through inspections of the register by other public authorities or private individuals. Both procedures lead to the processing of personal data and, ultimately, to the spreading of knowledge amongst communication partners about the identification cardholder. Thereby, not only official identity, but also personal identity[21] is concerned. From the German constitutional perspective, this is an issue of informational self-determination.[22] Importantly, this does not only bring about questions of individual privacy, but also issues of democracy and the public good.[23]

3. Challenges posed by the Internet

The increasing shifting of human communication into various Internet applications poses huge new challenges against the background of this initial situation. Conventional identification processes are, for the most part, not applicable in the Internet. Nonetheless, the need for safe identification exists. The more often legal and business processes are carried out online, the greater the need for legal security.[24] This requires, to a great extent, that one knows, or can at least find out, who one's communication partners are.[25]

It is however exactly this requirement that has not yet been adequately fulfilled. There is no authoritative body for the virtual world which, based upon a legal obligation, determines an

---

18 Cf. on the historical development; V. Groebner, *Der Schein der Person*, 2004, and the articles in J. Caplan/J. Torpey (Ed.), *Documenting Individual Identity*, 2001.

19 See, summarised, G. Hornung (above n. 1), pp. 47 ff., with further references.

20 For the Australian and British cases, see C. Sullivan, "Digital identity – The legal person?", *Computer Law & Security Review* 25 (2009), pp. 227 ff.

21 Understood here as the socially conveyed possibility of a person to present his/her past to society or individuals so that he/she can affirm his/her presentation in the present and have the chance to gain social recognition and affirmation, see N. Luhmann, *Grundrechte als Institution*, 1965, pp. 60 ff.; see further M. Hildebrandt, "Profiling and the Identity of the European Citizen", in: M. Hildebrandt/S. Gutwirth (Eds.), *Profiling the European Citizen*, 2008, pp. 303 ff.; S. van der Hof/C. Prins, "Personalisation and its Influence on Identities, Behaviour and Social Values", ibid., pp. 111 ff. Private spheres and dimensions of life are independent requirements for living autonomously, see also B. Rössler, *Der Wert des Privaten*, 2001, pp. 127 ff., 136 ff., 201 ff. et passim.

22 For this connection, see G. Hornung (above n. 1), pp. 30 ff.; on the German concept of informational self-determination, see G. Hornung/C. Schnabel, "Data protection in Germany I: The population census decision and the right to informational self-determination", *Computer Law & Security Review* 25 (2009), pp. 84 ff.

23 See e.g. A. Rouvroy/Y. Poullet, "The right to informational self-determination and the value of self-development. Reassessing the importance of privacy for democracy", in: S. Guthwirth/Y. Poullet/P. De Hert/C. de Terwangne/S. Nouwt (Eds.), *Reinventing Data Protection?*, 2009, pp. 45 ff.

24 On the need for a technically guaranteed security, see, in so far, M. Knopp/D. Wilke/G. Hornung/P. Laue, "Grunddienste für die Rechtssicherheit elektronischer Kommunikation", *Multimedia und Recht* 11 (2008), pp. 723 ff.

25 On this problem, see, e.g., A. Roßnagel, in: id. (Ed.), *Allgegenwärtige Identifizierung?*, 2006, pp. 17 ff.; see also A. Roßnagel, "Personalisierung in der E-Welt – Aus dem Blickwinkel der informationellen Selbstbestimmung gesehen", *Wirtschaftsinformatik* 49 (2007), pp. 8 ff.

official identity for and identifies every citizen, aged sixteen and older (as in § 1 para. 1 PAuswG). In fact, basically every person, under every name, can assume one or more self-made identities in the form of e-mail addresses, web sites, pseudonyms in chat rooms, accounts in social networks or other identity designations.[26] In order to confirm the trustworthiness of a communication partner

[Page 154]

in the virtual community of the Internet, there is a multitude of various authentication procedures, such as the PIN/TAN method, the HBCI procedure in the area of online banking,[27] challenge-response authentication, and the use of user name and password. To link these authentication procedures to natural persons, diversely reliable methods are used. Such methods are, among others, the "PostIdent" procedure offered by the German Post (Deutsche Post AG)[28] and the simple sending of access data by mail to the address of the authorised person. These measures however only cover respectively one limited group of people, are effective only in defined relationships, proceed according to respectively different rules, and are usually incompatible with one another. Thus, they do not form a basis for generally usable identity infrastructures. If trustworthy third parties are involved in these procedures, it does not concern, in any case, any governmental bodies. For these reasons and due to technical insecurities, a series of procedures has been assessed by German Courts as not (always) being conclusive.[29]

On the other hand, there is indeed an existing legally regulated and trustworthy solution for substituting the hand written signature in electronic processes, the qualified electronic signature.[30] In Germany however, this is such a close replication of the hand written signature, that it only discloses the information that this signature would disclose. This information is

---

[26] This fact, and the resulting problems with trust have also been recently dealt with by the Federal Constitutional Court (Bundesverfassungsgericht) in its decision in matters of "online searching", see, *Decisions*, volume 120, pp. 274 ff.; also, e.g., G. Britz, "Vertraulichkeit und Integrität informationstechnischer Systeme", *Die Öffentliche Verwaltung* 61 (2008), pp. 411 ff.; G. Hornung, "Ein neues Grundrecht. Der verfassungsrechtliche Schutz der "Vertraulichkeit und Integrität informationstechnischer Systeme", *Computer und Recht* 24 (2008), pp. 299 ff.; U. Volkmann, "Anmerkung zu BVerfG, U. v. 27.02.2008 - 1 BvR 370/07", *Deutsches Verwaltungsblatt* 2008, pp. 590 ff.; W. Hoffmann-Riem, "Der grundrechtliche Schutz der Vertraulichkeit und Integrität eigengenutzter informationstechnischer Systeme", *Juristenzeitung* 63 (2008), 1009 ff.; G. Hornung/C. Schnabel, "Data protection in Germany II: Recent decisions on online-searchings, apnr and data retention", *Computer Law & Security Review* 25 (2009), pp. 115 ff.

[27] HBCI (Home Banking Computer Interface) is a bank-independent protocol for online banking, developed and used by German banks.

[28] Within this procedure, natural persons are identified by employees of the Deutsche Post, either in one of the post offices, or at the point of delivery. This "face-to-face" authentication is widely recognised within the German legal system, see M. Möller, "Rechtsfragen im Zusammenhang mit dem Postident-Verfahren", *Neue Juristische Wochenschrift* 58 (2005), pp. 1605 ff.

[29] In this way, there is no prima facie evidence that, in the application of the user name and password, the beneficiary was actually involved, see OLG Hamm, *Neue Juristische Wochenschrift* 60 (2007), p. 611; OLG Köln, *Computer und Recht* 22 (2006), p. 490; OLG Köln, *Kommunikation und Recht* 6 (2003), p. 83; LG Bonn, *Multimedia und Recht* 5 (2002), p. 257; LG Konstanz, *Multimedia und Recht* 5 (2002), p. 837; G. Borges, "Rechtsfragen des Phishing – Ein Überblick", *Neue Juristische Wochenschrift* 58 (2005), p. 3317; O. Sosnitza, "Auktionen im Internet aus Verbrauchersicht – Aktuelle Rechtsfragen im Spiegel der Rechtsprechung – Teil I", *Verbraucher und Recht* 22 (2007), p. 145. At least for the customary TAN procedure (in contrast to the iTAN procedure), the same should apply, see G. Spindler, *Verantwortlichkeiten von IT-Herstellern, Nutzern und Intermediären*, 2007, para. 573 f.

[30] See A. Roßnagel, "Das neue Recht elektronischer Signaturen – Neufassung des Signaturgesetzes und Änderung des BGB und der ZPO", *Neue Juristische Wochenschrift* 54 (2001), pp. 1817 ff.; A. Roßnagel/S. Fischer-Dieskau, "Elektronische Dokumente als Beweismittel – Neufassung der Beweisregelungen durch das Justizkommunikationsgesetz", *Neue Juristische Wochenschrift* 59 (2006), pp. 806 ff.

namely, in accordance with § 7 para. 1 No. 1 of the Signaturgesetz, first name and surname,[31] not however, like ID cards, date and place of birth, address, and other identification particulars. Yet, such particulars, especially in the case of same names, are imperative for an unambiguous identification. The only such explicit particular in the context of the German concept of qualified electronic signatures is the number of the qualified certificate, in accordance with § 7 para. 1 No. 4 Signaturgesetz. However, communication partners are not familiar with this number, at least not with first contact, and therefore, in this respect, it can not be counted as an identification particular.[32]

4. Electronic proof of identity

The electronic proof of identity of the new ID cards is to fill the gap in identification possibilities for communication partners. In the real world, the ID card has always ensured identification of such partners. With the ID card's new function, this should also be made possible in the future for the virtual world.

4.1 Conception and transmission of data

Use of the electronic proof of identity is optional, in a double sense, for cardholders. First of all, they can make a general decision on the switching on and off of this function (as in § 10 PAuswG). Secondly, they can decide upon using the function in concrete, individual cases. For this, in accordance with § 18 para. 4 PAuswG, the entry of a code number (PIN) is mandatory.[33] The same provision dictates that a transfer of data is only to take place if the service provider, i.e. the communication partner, has transmitted a valid authorisation certificate to the cardholder.[34] Such certificates are, in accordance with § 21 PAuswG, only issued to service providers whose processing methods have passed a data protection assessment. It must be a matter of a legitimate business purpose which is not allowed to exist in address trading. It must be verified that the data transfer is necessary for the fulfilment of the business purpose, further requirements for data protection and data security must be met, and there must be no indication of misuse of the authorisation. Authorisation certificates contain, notably, information about the provider, the categories of the transmitted data and its purpose, as well as contact information about the data protection supervisory authority of the data controller. In turn, these authorities may demand the revocation of the

[Page 155]

authorisation certificates by the issuance authority in case of misuse of personal data. Moreover, the certificates are to be limited in length of validity.

---

31 Additionally, the possibility of pseudonym use comes into effect, in accordance with § 7 para. 1 No. 1 Signaturgesetz. On the resulting problems, see G. Hornung, "Elektronische Zertifikate, Ausweise und Pseudonyme - Voraussetzungen der Selbstbestimmung", in: A. Roßnagel (above n. 25), pp. 53 ff.

32 On this, see A. Roßnagel, "Der elektronische Ausweis. Notwendige und mögliche Identifizierung im E-Government", *Datenschutz und Datensicherheit* 26 (2002), pp. 281 ff.

33 For use, a (contactless) card reader and client software will also be necessary, see Federal Ministry of the Interior, *Einführung des elektronischen Personalausweises in Deutschland, Grobkonzept - Version 2.0*, July 2, 2008 (pp. 57 ff.); also on the following.

34 See on this, from the technical point of view, the concept of the Federal Ministry of the Interior (above n. 33); on the security mechanisms, see J. Bender/D. Kügler/M. Margraf/I. Naumann, "Sicherheitsmechanismen für kontaktlose Chips im deutschen elektronischen Personalausweis", *Datenschutz und Datensicherheit* 32 (2008), pp. 173 ff.

This system receives a positive evaluation from a legal data protection point of view.[35] With the verification of necessity, misuse of personal data is prevented and transparency is gained regarding the institutions with authorisation to access and their data protection authorities. Moreover, it is possible to limit data transfers to providers within the scope of application of the European Data Protection Directive.[36] Lastly, the authorisation certificate gives the cardholder the possibility to validate the identity of his or her interaction partner. This makes prosecution and law enforcement easier (or at least possible) if a legal dispute comes about.

The electronic proof of identity of the German ID card has two further data protection friendly functions.[37] First of all, it is possible to use a "service and card specific code" (pseudonym). This provides, according to § 2 para. 5 PAuswG, distinct electronic recognition of an ID card by the service provider for whom it has been generated, without the necessary transfer of additional personal data. Secondly, it provides the technical possibility of selective transfers of individual data sets. In other words, an authorisation certificate can be restricted to certain data fields, for example the specification "of age", or a certain location. In this way a provider of services for adults or for residents of a certain region can simply find out whether this is an existing attribute. This allows certain offers, especially those which are free of charge for the user (i.e. paid for through advertising), to be used without having to enter identifying characteristics.

It is clear that, all in all, the people responsible for this conception have endeavoured to shape the electronic proof of identity function data protection friendly. The double voluntariness, the pseudonym function, the selective data release option with mandatory PIN entry, the preliminary examination of service providers with the allocation of authorisation certificates, the possibility to take away access authorisation through responsible data protection authoritative intervention, and the technical blocking of data transmissions thereafter are all evidence of this. Some of the privacy-friendly features will become effective for every use of the electronic proof of identity, while others depend on the availability of pseudonymous and anonymous services. In any case, the actual use of these functions, as well as the electronic proof of identity as such, will depend on its usability for the average ID card holder. Issues of usability will be addressed within the application tests (see below).

4.2 Functional possibilities and limitations

The German concept of the electronic proof of identity follows a specific real world procedure, i.e. identification through visual control of the ID card. It does thus not represent an equivalent of the conventional copy of the ID card in areas of security and not at all an equivalent of the signature of the holder. Although this conception opens up multifaceted fields of application, it also limits the area of use of the new function. Both legal practitioners and providers of future applications for electronic proof of identity must be aware of these possibilities and restrictions. This holds also true for service providers in other EU Member States who wish to interact with German ID card holders in the future.

Because the function corresponds with the presentation but not the copying of the ID card, it is not possible to provide direct technical evidence (such as an electronic signature) that a concrete electronic proof of identity has been used in a transaction process with a service pro-

---

35 See, in detail, A. Roßnagel/G. Hornung/C. Schnabel, "Die Authentisierungsfunktion des elektronischen Personalausweises aus datenschutzrechtlicher Sicht", *Datenschutz und Datensicherheit* 32 (2008), pp. 168 ff.

36 Directive 95/46/EG of the European Parliament and of the Council lf 24.10.1995 on the protection of individuals with regard to the processing of personal data and on the free movement data on such data, OJ L 281/31 of 23.11.1995, p. 31; for the background, see, e.g. C. Kuner, *European Data Protection Law*, 2nd Edition, pp. 19 ff., 114 ff.

37 See A. Roßnagel/G. Hornung/C. Schnabel (above n. 35), pp. 168 f., 171.

vider. If a service provider wants or has to show this evidence, he or she is reliant upon indirect evidence, such as recording instruments which functionally comply with, for instance, a record notice of an administrative authority or corporate employee on the identification of a person by means of the visual presentation of an ID card. The consequential problems of evidence in this case are immediately clear. The recording is carried out by one party of a potential legal dispute, which has a specific interest in one beneficial part of the record's content and which is, without appropriate security measures, able to regenerate or alter such a record without leaving a trace.

It is left open as to how German Courts will deal with this problem. At any rate, in the structurally comparable case of legal disputes between telecommunication providers and their customers, it has been repeatedly acclaimed by courts that individual connection evidence generated by the provider for itemized bills grants prima facie evidence.[38] In this respect, individual financial interest of the party which has conducted the recording is, at least, no reason to bar prima facie evidence out of principle considerations. It can thus be assumed that Courts may handle records of the use of electronic proofs of identity accordingly.

Generally, it is to be expected that electronic proof of identity is going to have a double-sided effect in evidence issues, such as the German "eBay cases"[39] and other, comparable constellations in which the identity or authorisation of a user has been verified through a PIN and TAN, user name and password, and other such mechanisms. On the one hand, the ID card will henceforth provide a secure identification method which will surely be taken into consideration by the courts. Due to its security mechanisms (protection through chip card possession and a PIN), it will presumably be

[Page 156]

assessed analogous to the use of EC cards and thus provide prima facie evidence.[40] On the other hand, due to the availability of this secure method, there will be an even greater mistrust in the authenticity of conventional procedures, as long as these do not possess comparable security mechanisms.

The essential functional restriction of the German electronic proof of identity can be recognised in its distinction from the qualified electronic signature. Conceptually, identification and declaration of intention must be separated in technical implementation and legal evaluation. Simply through its name, it is recognisable that the electronic proof of identity serves as evidence of identity (or certain characteristics). Identification for access to an Internet portal is, for example, not proof of closure of a concrete contract within the portal and not at all proof of its content.

In order to execute declarations of intention in combination with the electronic proof of identity, there are therefore two possibilities, namely with and without using qualified electronic

---

38 For this, Courts accept expert evidence through a complete inspection of the provider's system which confirms that there is neither any evidence of malfunction, nor of manipulation through a third party (see, e.g., Bundesgerichthof, *Decisions*, volume 158, pp. 201 ff.; OLG Köln, *Neue Juristische Wochenschrift-Rechtsprechung* 1998, 1363 f.; H. Mannes, "Anforderungen an die technische Prüfung gemäß § 16 TKV", *Multimedia und Recht* 9 (2006), pp. 657 ff..

39 See, e.g., OLG Hamm, *Neue Juristische Wochenschrift* 60 (2007), 611; OLG Köln, *Computer und Recht* 22 (2006), 490.

40 See Bundesgerichtshof, *Neue Juristische Wochenschrift* 57 (2004), p. 3623 (3624); Kammergericht, *Neue Juristische Wochenschrift* 45 (1992), p. 1051 (1052); LG Bonn, *Neue Juristische Wochenschrift* 48 (1995), p. 815; LG Darmstadt, *Wertpapiermitteilungen* 54 (2000), pp. 911 (913 f.); LG Frankfurt, *Wertpapiermitteilungen* 53 (1999), pp. 1930 (1932 f.); LG Hannover, *Wertpapiermitteilungen* 52 (1998), pp. 1123 f.; *LG Köln*, *Wertpapiermitteilungen* 49 (1995), pp 976 (977 f.); different opinion: OLG Hamm, *Neue Juristische Wochenschrift* 50 (1997), pp. 1711 (1712 f.); LG Berlin, *Wertpapiermitteilungen* 53 (1999), pp. 1920 f.

signatures. As the electronic ID card offers this functionality as an option, in accordance with § 22 PAuswG, for those cardholders who wish for it, the combined alternative can be obtained in one card. The advantage of this is that, with the ID card, both the legally compliant identification, as per the specified procedure, and also the execution of a declaration of intention is possible. Moreover, the written form of the declaration of intention, in accordance with § 126 para. 3 and § 126a of the German Civil Code (Bürgerliches Gesetzbuch, BGB), is substituted and also, in accordance with § 371a of the German Code of Civil Procedure (Zivilprozessordnung, ZPO), the qualified electronic signature provides prima facie evidence as regards the integrity and the authenticity of the declaration.

If the cardholder decides against the activation of the signature function (which requires a contract with a private certification-service-provider and thus comes with a fee), it is still possible, as hitherto, to execute a declaration of intention by way of a web form, as long as no written form is required. In this case, execution and content of the declaration may, as so far, be proven through log files which correspond with the requirements set out by German courts in the itemized bills cases. Security of the whole process is somewhat heightened as application can only be carried out at the portal subsequent to the use of the electronic proof of identity.

ID cards which have already been issued remain valid. Therefore the issuing of new ID cards, and, with them, electronic proofs of identity, will take place in the normal way, i.e. via issuing upon application. For cardholders aged 24 and over, the conventional document remains valid for ten years, in accordance with § 2 para. 1 of the former ID Card Act. For this reason, it will take up to the same amount of time until all citizens, obliged to possess ID cards, hold the new document. Nonetheless, it is perceivable that following increasing use of various Internet applications which require secure identification, the use of electronic proofs of identity will increase and bit by bit, the old (non-secure) process will be phased out. This could also put pressure on those who regularly use the Internet to apply for new ID cards, early on.

4.3 Concrete application

It is somewhat speculative as to which concrete contexts and applications electronic proof of identity will be adopted in. This is natural as it has been designed as an infrastructure method. Conceivable applications can be found everywhere where identification is necessary for initial contact or recognition. This means, in initiating business contacts in e-Commerce (for example by eBay and other similar providers), in accessing an online bank account, a web mail application, in Internet portals like the planned German citizen's portal,[41] and in all other forms of telemedia. Meaningful fields of application are emerging, especially in e-Government, because secure identification by initial contact has been a considerable issue in this area up until now. This could be solved through the electronic proof of identity. Examples of this are: electronic licensing procedures, electronic inspection of records, the execution of data subject's right to access personal data, as well as special administrative services, such as the preliminary filling out of Internet application forms or the possibility of tracking the progress of administrative processes.[42] In summer 2009, the German Federal Minister of the Interior started application tests. Out of 96 applicants, 30 businesses and government agencies were chosen to develop applications for the new electronic proof of identity. Those examples are very diverse and include, inter alia, an online age verification system, the authentication in local e-government applications, ATM's, student's university enrolment, online gambling, single sign-on processes at the work place, a password manager for Windows, online insurance applications, the access to personal data, online banking, the recording of working time,

---

41 See M. Knopp/D. Wilke/G. Hornung/P. Laue, (above n. 24), pp. 723 ff.

42 For this, see also A. Roßnagel (above n. 32), pp. 281.

online identification processes of flight passengers, and electronic ticketing.[43] Those participating in the application tests had to commit themselves to having the applications available upon the issuance of the first new ID cards, i.e. November 1, 2010.

Legislature itself has regulated merely two applications for the electronic proof of identity. In accordance with the amendment to § 6 para. 2 No. 2 of the German Act on the Prevention of Money Laundering (Geldwäschegesetz), necessary identification of the contract partner of one of the obliged parties (the latter is usually a bank), can be carried out via electronic proof of identity if the contract partner is an natural person who is not personally present for the determination of identity. Furthermore, the electronic proof of identity can be

[Page 157]

used to identify an applicant for a qualified certificate pursuant the new § 3 para. 1 of the Electronic Signature Regulation (Signaturverordnung). This applies to both a qualified certificate for the ID card itself and for a separate secure-signature-creation device.

However, one essentially important use will no longer be possible with the new ID card. According to § 1 para. 1 PAuswG, the ID card holder can no longer be forced to deposit his or her ID card or, in other ways, to give up custody of it. There is one valid exception only for authorities who have the right to determine identity, and for those legitimately carrying out the confiscation of the ID card. Because the card entails both the electronic proof of identity and, optionally, a private cryptographic key for the generation of qualified electronic signatures, the sole ownership of it represents indispensable security. In order to prevent misuse, it is no longer allowed to demand the ID card to be handed over at the front desk or gate of a building or used as a deposit when borrowing an object.

5. Outlook

Electronic proof of identity "extends" the current functions of the conventional ID cards in Germany and other countries in the world of e-Government and e-Commerce. Ultimately, this represents a challenge for the identification system as a whole. There are new administrative tasks, new processes, and new connections for communication and interaction. For example, the German regulation on the electronic signature function in § 22 PAuswG leaves open the issue of co-operation between ID card authorities and certification-service-providers, as well as the form of a possible co-operation. If ID card authorities opt for this co-operation, there will be extensive questions to be clarified about control duties (that are incumbent on certification-service-providers, according to the Signaturgesetz), and liability or recourse.[44]

Furthermore, the electronic proof of identity is to be seen in conjunction with other identification infrastructures. Of mention are for Germany: the planned electronic health insurance card,[45] electronic proof of income for social insurance applications (ELENA, previously termed "JobCard"),[46] the government planned citizen's portal,[47] but also the planned federal

---

[43] The complete list is available at http://www.cio.bund.de/cln_103/DE/IT-Projekte/Leuchtturmprojekt_ePA/Anwendungstest_ePA/anwendungstest_node.html.

[44] For a closer look, see A. Roßnagel/R. Gitter, in: H. Reichl/A. Roßnagel/G. Müller (above n. 8), pp. 151 ff.; see also G. Hornung (above n. 1), pp. 323 ff.

[45] For this, see G. Hornung (above n. 1); C. M. Borchers, *Die Einführung der elektronischen Gesundheitskarte in das deutsche Gesundheitswesen*, 2008.

[46] See G. Hornung (above n. 1); W. Ernestus, "JobCard – Schlüssel zur elektronischen Kommunikation", *Datenschutz und Datensicherheit* 28 (2004), pp. 404 ff.; G. Hornung/A. Roßnage, "Die JobCard – "Killer – Applikation" für die elektronische Signatur?", *Kommunikation und Recht* 7 (2004), pp. 263 ff.; see also C. Schaefer, "Verbesserter Grundrechtsschutz durch ein elektronisches Bescheinigungsverfahren", *Zeitschrift für Rechtspolitik* 39 (2006), pp. 93 ff.

[47] On this, see also M. Knopp/D. Wilke/G. Hornung/P. Laue (above n. 24), pp. 723 ff.

register of residents. The total image of “official identity” mentioned above is changing with this overall development and with it, interaction mechanisms between citizens and administration. All in all, these processes of change are just at the beginning of their development in Germany and throughout Europe.

Dr Gerrit Hornung *LLM (European Law) (gerrit.hornung@uni-kassel.de) and* **Prof. Dr. Alexander Roßnagel** *(a.rossnagel@uni-kassel.de) University of Kassel, Germany.*