ARTICLE:

A SYSTEM OF TRUST:
GERMAN CIVIL LAW NOTARIES AND THEIR ROLE IN PROVIDING TRUSTWORTHY ELECTRONIC DOCUMENTS AND COMMUNICATION

WRITTEN BY:
DR DOMINIK GASSEN, BUNDESNOTARKAMMER

One of the elements of the traditional role of the civil law notary has always been to provide an additional layer of trust and security for all transactions that legally require notarial participation. While – as opposed to the role of the common-law notary public – civil law notaries are highly qualified legal professionals who advise their clients on all legal aspects of transactions and draft the necessary contracts and documents as well as take care of any procedural requirements that the transaction requires, one of the historic core roles of the notary is to accurately witness legal and factual proceedings, and produce documents with a higher level of tamper resistance.[1] The legal system imbues these documents with enhanced evidentiary value in accordance to the official role of the notary, thus granting a basis of trust beyond mere civil liability of a Trusted Third Party.

With the increased use of electronic communications and the problems with reliability, German notaries decided to take up an active part in the early stages of discussions about possible remedies. It was felt that the new medium required exactly the kind of service that notaries were traditionally providing. In a series of scientific conferences, notarial organisations introduced the idea of electronic signatures into legal discussion in Germany in the early 1990s.

The original idea was that notaries were uniquely suited to the role of trusted third parties, because the legal system already recognized them in this capacity in other areas. Another thought that was present from the very beginning, was that signature technology would probably turn out too expensive and cumbersome for the mass market (i.e. citizen-government or customer-business relations) but had a lot to offer to professional user groups with a need for secure electronic communications.

With the introduction of the first electronic signatures act in 1997, the German legislature introduced a different system that relied on privately owned certification authorities (CA). The 1997 law required CAs to obtain a license before going into business, and to use CA certificates from a German government root CA ("Bundesnetzagentur").[2]

Policies of the Bundesnotarkammer CA

Bundesnotarkammer (BNotK) decided to pursue its original approach on certification by founding a licensed CA for the purpose of issuing qualified signature certificates to notaries and related legal professionals. The notarial CA would attempt to use the most advanced security techniques in connection with established notarial procedures to ensure that any activities of notaries in electronic media would meet the highest standards of operation. Even though actual operation of the technical aspects of the service would be handled in collaboration with another provider, the service would be used as a best practice example for running a reliable CA that would not be primarily driven by economic considerations.

In order for a smart card with a qualified certificate to be issued to an applicant by the BNotK CA, the following procedure has to be followed:

[1] *In the paper medium this is achieved by a number of measures, ranging from different forms of seal to special kinds of paper and ink or methods of binding several document pages.*

[2] *See http://www.bundesnetzagentur.de/enid/72b2a65ac3cbb6d3daadd7f00ecb93d8,0/Technische_Regulierung_Telekommunikation/Elektronische_Signatur_gz.html or http://tinyurl.com/jxlwf.*

1. Applicants can only be notaries, attorneys or chartered accountants (the latter two because of their close relations to notarial practice) and notaries' employees.
2. Application data is collected in secure web forms and transferred to the CA in encrypted form. Some sensitive data is excluded from the electronic exchange.
3. The applicant prints out on paper the result of the web forms – the actual application. Additional information (blocking passwords, account information) has to be filled in manually.
4. The paper application must be signed in front of another notary who notarises the signature while adhering to the strict German legal code of conduct for notaries (Bundesnotarordnung,[3] Beurkundungsgesetz,[4] Dienstordnung für Notare).[5] The notary has to take certain additional steps to verify the identity of the applicant. Procedure dictates a personal appearance of the applicant. No proxies are allowed.
5. The application is then sent to the CA by the notary who performed the notarisation.
6. The certificate can be issued with an addition "attribute" that confirms the professional capacity of the signer as a notary. If such an attribute is applied for, the competent regional chamber of notaries has to be consulted (by the CA) to confirm the fact that the applicant is a notary in office at the time the certificate is issued. The chamber makes a note of every confirmation that is given. Should the notary retire or be removed from office, a chamber representative can revoke the certificate without the consent of the owner. That way, the possibilities of anybody posing on-line as a German notary are extremely limited.
7. When the smart card is issued, the applicant only receives the first fragment of the necessary PIN. He has to acknowledge the receipt of the smart card in writing before a second letter is produced that contains the second fragment. Only by having both fragments can the applicant calculate the complete PIN. This procedure effectively deters anyone from intercepting both card and PIN letter.

While this procedure might seem too complicated for issuing certificates to the general population, it surely reflects the enhanced responsibilities that come with the office of a civil law notary. It might also serve as a best practice example for measures to effectively prevent and counter misappropriation of identity.

Further development of signature legislation in Germany

Responding to the EU directive on electronic signatures, the German signature law was changed in 2001.[6] The licensing requirement was given up, only to be replaced by an additional quality level of certification practice called "accredited CA". Accreditation was basically taking the former licensing conditions and shaping them into a voluntary procedure that nevertheless implied a large amount of additional technical requirements and the completion of an audit by external auditors before the status would be granted to the CA.

German signature legislation has always been characterized by wide-reaching regulations in relation to the technical aspects of electronic signatures, starting from the procedure used by the CA before issuing a signature card, to the specifications for hardware and software for smart cards, card readers and signature applications. These regulations are diligently regulated by the Bundesnetzagentur and a pool of specialised auditors.

This system affected the practical use of PKI-based electronic signatures in two ways:

1. Because high quality levels were required in nearly all transactions that could be managed electronically, signatures on a simpler technical level (as introduced by the European directive and the reformed German signature law), together with the CAs offering them, never gained any ground and were not taken up in any significant way by the legal community.
2. The cost of qualified certificates remained relatively high: the market price is about 40,- € p.a. for a basic qualified certificate. Additional costs for hardware and software can easily run to about 250,- € - an investment that most private users and a significant amount of professional users are not ready to make without the incentive of additional useful applications. Even German banks – who have a usable system of distribution through their banking cards – shied away from introducing signature technology for their own transactions, fearing that their customers would not be willing to carry the additional cost.

[3] *See http://www.bnotk.de/_PDF-Dateien/BNotO/BNOTO(19.04.2006).pdf.*
[4] *See http://www.bnotk.de/Berufsrecht/BeurkG/BeurkG.html.*
[5] *See http://www.bnotk.de/_PDF-Dateien/DONot/DONOT-2005.pdf.*
[6] *Gesetz über Rahmenbedingungen für elektronische Signaturen (Signaturgesetz - SigG) vom 16.5.2001 (BGBl. I S. 876).*

So, for the most part, digital signatures are still not a part of legal reality in Germany. Even though the legal framework and technical solutions have long been in place, there are few court decisions that involve signed data.

One of the few moderately successful applications of electronic signatures in the legal realm is a system for automatically applying for court orders to pay ("Mahnbescheide") to certain German courts.[7] Even though the system is technically proven and easy to use, only about 30 per cent of professional users (i.e. attorneys) use this procedure instead of traditional paper filing.[8]

In 2005 another revision of the signature law was adopted,[9] this time mainly on pressure from German banks and public Savings and Loan institutes ("Sparkassen"). A few of the legal provisions for applications for certificates were softened to accommodate established banking procedures. There has not been any significant effect on the broader reception of electronic signatures.

Companies register and electronic public documents

A focal point for the use of electronic signatures in a legal context in recent years has been the area of the German "Handelsregister", an advanced public form of a company database that contains legally reliable information about most German companies, their area of business, capitalization and representation. Entries into the register are compulsory and the content of the register can be relied upon when determining legal relations with a German company. One of the legal effects of a register entry is that anyone doing business with a company representative whose powers have been entered into the Handelsregister can rely on the validity of these powers unless they have been publicly revoked (in the register).

To ensure a high quality of information in the register, all applications have to be notarised before entry – a longstanding tradition in German law. In 2003 an EU directive[10] decreed that from 2007 every national register of companies had to be organised electronically and allow for electronic viewing and entry of applications. For German courts, this provided a tremendous task, because there were a huge amount of documents that were transferred and processed for the Handelsregister. The new procedures have to work on a scale that had not been attempted before in Germany.

Facing the task of transferring procedures that up to now relied on public paper documents,[11] German legislation created legal provisions for an advanced ("public") electronic form. The "Justice Communication Act" ("Justizkommunikationsgesetz")[12] introduced a new competency for notaries that allowed them to create certified copies of any document in electronic form.[13] These electronic documents would be imbued with the same enhanced evidentiary value that German procedure law attributes to public documents on paper.[14]

While German civil law has recognized electronic documents with qualified electronic signatures as equivalent to written paper documents since 2001,[15] this was the first provision acknowledging advanced formal structures in electronic documents.

In order to be recognized as an electronic public document, § 39a BeurkG requires certain additional elements from the data:

1. The document has to be provided with proof that the signing person is a notary in office at the time of the certificate was issued and was acting in this capacity.
2. The document has to contain a qualified electronic signature.
3. The signature must be based on a certificate that can be verified in perpetuity.[16]

This approach could be an interesting best practice example for an attempt to establish an advanced quality of secure electronic documents. These documents will provide the courts with better evidentiary value that is not easy to rebut.

[7] *See http://www.profimahn.de (page in German).*

[8] *Some information, without statistical data, can be found here: http://www.justiz.nrw.de/Online_verfahren_projekte/projekte/agm/index.php visited on 20 September 2006.*

[9] *Erstes Gesetz zur Änderung des Signaturgesetzes (1. SigÄndG) Von 4. Januar 2005 available on-line at http://www.bundesnetzagentur.de/media/archive/2248.pdf.*

[10] *Directive 2003/58/EC of the European Parliament and of the Council of 15 July 2003 amending Council Directive 68/151/EEC, as regards disclosure requirements in respect of certain types of companies (4.9.2003 OJ L 221/13), available in electronic format at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2003:221:0013:0016:EN:PDF.*

[11] *"Public" meaning being issued by a notary with public authority.*

[12] *See http://www.bundesgerichtshof.de/gesetzesmaterialien/Justizkommunikation/bgbl105s0837.pdf or http://tinyurl.com/nhonx.*

[13] *Gesetz über die Verwendung elektronischer Kommunikationsformen in der Justiz Einfache elektronische Zeugnisse Vom 22.3.2005, verkündet in BGBl I 2005 Nr. 18 vom 29.3.2005 39a BeurkG, available in electronic format at http://bundesrecht.juris.de/beurkg/__39a.html*

[14] *Beweiskraft elektronischer Dokumente 371a Abs. 2, available in electronic format at http://bundesrecht.juris.de/zpo/__371a.html*

[15] *Art. 1 des Ersten Gesetzes zur Änderung des Signaturgesetzes (1. SigGÄndG) vom 04. Januar 2005 (BGBl. I S. 2) 126a BGB, available in electronic format at http://bundesrecht.juris.de/englisch_bgb/index.html#Section% 20126a.*

[16] *This provision takes up the problem that most CAs will store certificate information only for a limited period of time. In German law, the minimal period is five years, accredited CAs have to retain certificate information at least 30 years, § 4 Signaturverordnung (http://www.gesetze-im-internet.de/sigv_2001/__4.html).*

Because notaries were required by law to offer the necessary technical provisions to produce these new electronic public documents,[17] smart cards and signature applications are now widespread in German notary offices. Though representing a deeply traditional profession, notaries have lately been on the forefront of modern developments in e-Justice in Germany.

Replacing e-mail with a more secure system for communication with the courts

Another problem that had to be solved, was how to secure confidential communication between courts and legal professionals. While e-mail seemed the obvious solution, it had a few obvious drawbacks:

1. Encryption is technically difficult to establish between the courts and a large number of legal professionals.
2. There is no reliable information on the source of a message because e-mail header data can easily be forged.
3. There is no system to provide the sender with a receipt of entry that can be used in a court.

For these reasons, e-mail has become increasingly unpopular in German e-government applications recently. A number of government agencies have gravitated towards a new communications protocol called "OSCI-Transport" [18] that offers remedies for all the drawbacks:

1. All messages are automatically wrapped in two layers of asymmetric encryption so that even on the OSCI server ("Intermediär"), no cleartext can be viewed.
2. Messages have to be provided with qualified electronic signatures; technical solutions that are compatible with German signature law are supported (as opposed to the signature functions in Microsoft products).
3. The sender receives an automatically generated receipt for his message. The receipt also bears a signature (of the server), so it can be used in court to prove a certain message has been sent and received at a certain point in time.

While OSCI-Transport lacks (for now) the seamless integration into the OS that e-mail offers – there is a special client program that has to be used to author messages – the security features are worth the trade-off, at least in a professional context that relies on confidentiality. This system has been favoured over other solutions that provided security by using closed networks for courts and legal professionals. While attempts in this direction have been made, the federal structure of 16 German "Bundesländer" with varying approaches to networks and security, an infrastructure approach proved too complicated.

E-Justice communication as an integrated system

Perhaps a characteristic trait of IT solutions from Germany, the chosen approach to e-justice and e-government was not quite as fast as solutions proposed in other countries. It offers a well thought-out overall design, that solves a number of problems, and has a good long-term perspective. German notaries have actively grasped the opportunity to shape the new procedures on a legal and technical level. The collaborative effort of courts, judicial administration and notarial organisations has been a positive example on how satisfactory solutions can be reached when all partners sit down together and join in parallel development efforts.

The system also strengthens a thought that is inherent to the German legal system and the notarial profession:[19] It is often a better solution to spend more effort in preparing and controlling legal transactions to prevent legal action, than to exclusively rely on later litigation. Often the involvement of a notary can effectively reduce the transaction costs because his neutral stance and duty to prevent results that are unfavourable to one side reduces the necessity for additional legal representation for both sides.

Dr. Dominik Gassen is a notarial candidate (Notarassessor) from Cologne, Germany. With a background and a doctoral thesis about legal questions concerning digital signatures, he works as an expert on e-government matters and related procedures for the German chamber of notaries (Bundesnotarkammer). He is also CEO of the chamber's IT subsidiary, "NotarNet GmbH" that is actively involved in the development of e-government applications for German notaries.

[17] *§ 15 Abs. 3 Bundesnotarordnung available in electronic format at http://bundesrecht.juris.de/bnoto/__15.html*

[18] *Abbreviation for the vague „Online Services Computer Interface", www.osci.de.*

[19] *„Freiwillige" or „Vorsorgende Gerichtsbarkeit."*