

# Realization of Legal Requirements on Digital Signatures in Electronic Commerce

Michael Gisler<sup>1)</sup>, Alexander Runge<sup>2)</sup>, Hans-Dieter Zimmermann<sup>2)</sup>

<sup>1)</sup> Foundation for Information Management, University St. Gallen, Switzerland, Michael.Gisler@sim.unisg.ch

<sup>2)</sup> Institute for Information Management, University St. Gallen, {Firstname.Lastname}@iwi.unisg.ch

## Contents

1 Introduction .....	1
2 Documents and Signatures .....	1
2.1 Electronic Documents .....	2
2.2 Digital Documents .....	2
3 Competing Laws for Documents.....	4
4 Electronic Signatures and Digital Signatures.....	5
4.1 Electronic Signature.....	5
4.2 Digital Signature .....	5
5 Legal Functions of Signatures.....	6
6 Technical Mechanisms for Realization of Legal Functions in Digital Signatures .....	8
7 Digital Signatures in the German Homebanking Computer Interface .....	10
8 Conclusion.....	11

## Abstract

Some very fundamental obstacles inhibit, or at least slow down the success and growth of Electronic Commerce. These are, among others, the lack of real comfortable and secure payment systems, as well as a lack of a trustworthy environment for business transactions. However, these requirements can not be put into practice without digital signatures. Digital signatures may be used in any of the phases of Electronic Market transactions, such as the information, contract negotiation or the final settlement phase.

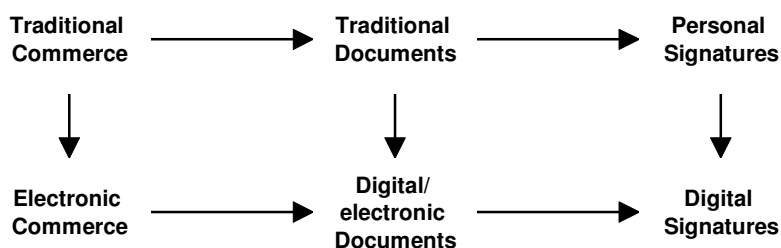
This paper deals primarily with issues of digital signatures. It discusses legal requirements on digital signatures, digital signatures itself and shows how technical mechanisms may be used to fulfill identified security and legal requirements. Finally an example of the use of digital signatures in the German homebanking sector is given.

## 1 Introduction

*„Although doing business in cyberspace may be novel and exhilarating, it can also be frustrating, confusing ...“* [Spar/Bussang 1996, 125]

On the way into the information age we are in a phase of transformation. Companies who are in the cyberspace face several problems doing their business. These problems are based on a lack of disputability, anonymity, trustworthiness, confidentiality and of course originate from a lack of awareness of possible legal issues regarding exchanged electronic documents of all kinds, e.g. electronic ordering or electronic voting.

Traditional commerce is heavily based on documents, which must personally be signed in order to develop legal relevance and legally commitment. With the ongoing shift of traditional commerce to electronic commerce traditional documents become electronic or digital documents. These electronic or digital documents must be signed by a substitute for the personal signature: The the digital signature.



**Figure 1:** Shift from Traditional Commerce to Electronic Commerce

Today, information has gained the importance of a productivity factor. Documents, the medium for information, are central to organizations and are critically important in roles such as means of communication, organizational memory and of course in business processes. *„As we continue into the information age, the future will see an explosion in the quantity, quality, and nature of digital documents produced, stored, and transmitted by organizations.“* [Igarial/ Sprague 1996, 2]. *„The total number of new documents produced annually could increase by 60 percent in one decade to reach 1.6 trillion by 1996.“* [Tan/ Bui 1996, 33] In organizations, digital documents take over functions such as communication mechanism, business process vehicles or organizational memory [Meier/ Sprague 1996, 53]. However, digital documents must be reliable, legally binding and must observe legal and security requirements. Also form requirements must be observed. Nowadays, modern information technology is available to cope with these issues from a technical point of view.

This paper discusses ways to put legal and security requirements into practice. After starting with a short overview of ways to use digital signatures (section 2), a short introduction of the legal background (section 3) as well as differences between the electronic signature and the digital signature (section 4) are presented. Legal functions for signatures are derived in section 5 in order to use digital signatures in Electronic Commerce. Section 6 shows relevant technical means and combines them in order to realize legal and security requirements on digital signatures and gives a practical example of the use of digital signatures in the German Homebanking Computer Interface (HBCI).

## 2 Documents and Signatures

Many authors are discussing issues regarding the words *digital* and *electronic*. This discussion is relevant for objects as documents (electronic or digital documents) as well as for objects as signatures (electronic and digital signatures). In this paper the distinction between *electronic* and

*digital* is based on the way of creating a specific object, whether it is a document or a signature. The origin of the object implies, whether it is a digital or electronic object.

Electronic objects are physically existing objects, which are translated into an electronic representation. For instance, electronic documents are paper-based documents, which were scanned in and from thereon represented electronically. Following that, electronic signatures are paper-based personal signatures, which were scanned in. Archived and filed checks or balance sheets, which are scanned in, are examples for electronic documents<sup>1</sup>.

In contrast, digital objects are objects, which are not existing physically and therefore are created by means of IT. In this paper digital documents are documents, which are not created by scanning in some paper document, but by creating that document with IT-means (created with some text-editor, EDI-messages). Also, digital signatures are not created by a personal handwriting, but by applying means of IT as an encryption mechanism.

## 2.1 Electronic Documents

According to [Bons/ Lee/ Wagenaar, 1994] two kinds of electronic documents may be distinguished in international trade:

- **Electronic Documents with a Performative Nature**

Claims and duties which may be allocated among different market participants, need to be transmitted between certain communicating partners. Electronic Documents, which transmit rights and duties perform a change in the legal status of each participating party and thus are of a performative nature. To put performative documents into practice requirements such as non-repudiation, confidentiality and integrity must be observed<sup>2</sup> for instance via digital signatures.

- **Negotiable Documents**

Electronic documents of performative nature manage the exchange of negotiable documents. Negotiable documents are holder securities, which grant the owner certain rights or duties and may be seen as a subgroup of performative documents.

Roles and examples of performative documents in Electronic Commerce comprise of orders, order acknowledgments and contracts or agreements. Negotiable documents on the other hand comprise of checks or figurative money bills, which give the owner certain rights such as the ability to pay. It is not necessary to mention, that negotiable documents (president of the federal reserve) or performative documents (the issuer of an order) must be signed.

## 2.2 Digital Documents

This paper uses the term digital document as defined in [Sprague, 1993] as an information set pertaining to a topic, represented by a variety of symbols, stored and handled as a unit with dimensions as defined in [Palmer 1997, 119]. For further discussions, the environment and use of digital documents in Electronic Commerce are relevant especially in forms such as contracts and agreements [Meier/ Sprague 1996, 54].

Digital documents must be reliable, legally binding and must observe legal and security requirements<sup>3</sup>. In this environment examples for digital documents are EDI messages. The authors [Baum/ Perrit 1991, 181] identify security requirements for EDI messages according to table 1.

However, technical mechanisms to fulfill these requirements are available as will be discussed below in section 6, and are very much based on digital signatures.

---

<sup>1</sup> See section 4 for examples of electronic signatures.

<sup>2</sup> See also [Smedinghoff 1996, 29pp].

<sup>3</sup> See [Kalakota/ Whinston 1996, 361pp] for a short discussion of the legal status of EDI Messages.

Within Electronic Commerce digital documents will eventually play a major role in Electronic Contracting. „*Electronic contracting involves the exchange of messages between buyers and sellers, structured according to a prearranged format so that the contents are machine-processible and automatically give rise to contractual obligations.*“ [Baum/ Perrit 1991, 6]. One way to implement Electronic Contracts is the use of technical means such as the digital signature (see section 4).

Generally, agreements or contracts have no form requirement in Swiss [Koller 1996, 150] and German (§ 125 BGB) law. However, both laws require some specific contracts and agreements to be settled with specific form requirements. The purpose of form requirements is to protect contracting parties from contracts, which are settled to fast and do not observe any requirements. Form requirements also create evidence. „*In contract law, for example, the Statute of Frauds provides that contracts or the sale of goods for the price of \$500 or more are not enforceable unless there is a writing sufficient to indicate that a contract has been made between the parties, and that writing is signed by the party against whom enforcement is sought.*“ [Smedinghoff 1996, 31]

Swiss law identifies three kinds of form requirements for traditional contracts. One form requirement in Swiss law is the simple writing requirement, which means, that negotiated contents need to be written and, most important, hand-signed personally. In Swiss law, only under exceptional reasons can mechanically-created signatures be used ; mechanically created signatures are not sufficient generally. Swiss law also covers qualified writing. The qualified writing requirement consist of the simple writing requirement enhanced with special extra requirements such as special words, which must be used (i.e. exchange bills) or must be written by hand (i.e. last will and testament). The most sophisticated form requirement in Swiss law is public certification. This requires, that a certain content is written and certified by a notary public, who is put into office by the country.

Type of Message	Authentication	Confidentiality	Integrity
Inquiry; Request for Quote or Comment			X
Price Catalog			X
Offer/ Order	X	X	X
Functional Acknowledgment	X	X	X
Change Modification; Application Acknowledgement	X		X
Acceptance of Change/ Modification	X		X
Notification of Status of Performance	X	X	X
Pymment/ Remittance	X		X

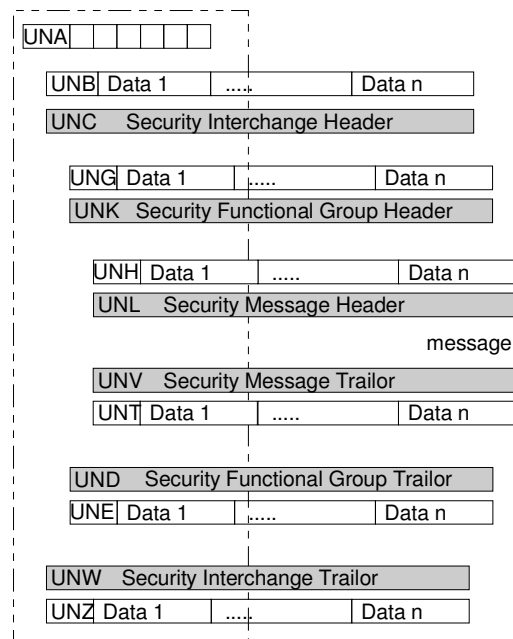
**Table 1:** Message security requirements

Digital documents are transmitted in data representations such as the UN/ EDIFACT standard. UN/ EDIFACT defines EDI message elements, their structures, contents and their sequences and was enhanced by the MD4 EDIFACT Security Group in the following way, that the exchange of EDIFACT messages is secured and observes security requirements [MD4 1991, 6]:

- Additional security elements were added to the actual EDIFACT message, which put services as confidentiality of content, data origin authentication, integrity of content, non-repudiation of origin and message sequence integrity into practice (see figure 1).
- In order to realize non-repudiation of delivery, an additional message is needed, which will be sent back to the sender of the original EDIFACT message.

Figure 1 depicts the extension of the conventional EDIFACT message structure. Basically, a Security Interchange Header (UNC), a Security Functional Group Header (UNK), a Security Message Header

(UNL) and the corresponding trailers (UNW, UND and UNV) were added. The new message structure has the same structure as the originally modified message. The header parts are used for relevant information for security services as the kind of security service or information on used methods of encryption. Trailers are used to store relevant information on results of security calculations such as hash-sums or digital signatures [Scheidegger/ Zbornik 1993, 36].



**Figure 2:** Security enhanced EDIFACT messages

This section shows, that the use of digital documents is very broad, not only in Electronic Commerce. It also shows, that digital documents and digital signatures should be used in conjunction, in order to observe security and legal requirements.

### 3 Competing Laws for Documents

The international usage of EDI raises the question, which national law is suitable to settle disputes. This situation is not new so that approximately four abstract possibilities exist to solve this problem:

- Most countries have an *international private law*. However, the term *international* is misleading. In fact, it is a *national* law regulating the jurisdiction and competence of different laws in international issues from a national point of view.
- *International contracts* regulate relations between states and their laws. In contrast to international private laws these *international contracts* have validity among signed countries and are subject to fulfillment.
- *International laws* are one kind of unification. These *international laws* are often created by international organizations as the European Community or the United Nations. Whether such a law is binding for the members (as most laws of the EC) or a ratification is voluntary (as most laws of the UN) depends on the structure of the organization. A very important international law is the *Vienna Sales Convention*. It regulates all questions among enterprises concerning contracts and is approved by most industrial countries such as the United States, Canada, Germany, France or the United Kingdom. Although this convention concerns contract law in general, it does not regulate problems of EDI.
- Another way of unification is the definition of so called *Model Laws* as references, which are supposed to be adapted to national laws. This is a very common way in the UN. For instance the

United Commission on International Trade Law (UNCITRAL) created a *Model Law on International Commercial Arbitration*. Among others countries such as Canada, Hong Kong, the Russian Federation, Scotland and some states of the United States created legislation based on this *Model Law*. UNCITRAL created recently the *Model Law on Electronic Commerce* concerning exactly the problems of EDI as recognition, the writing requirement, the signature itself or the term „original“. This *Model Law* is still a draft and not adapted yet [UNCITRAL, 1997].

## 4 Electronic Signatures and Digital Signatures

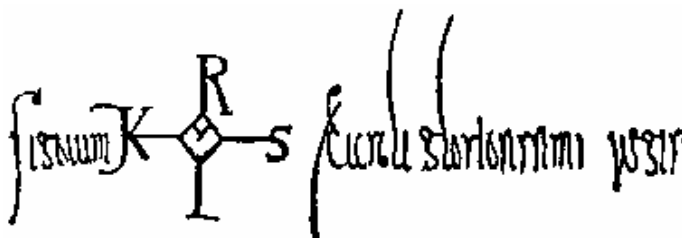
*„In the case of business transactions, authentication refers to the use of digital signatures, which play a function for digital documents similar to that played by handwritten signatures for printed documents: The signature is an unforgeable piece of data asserting that a named person wrote or otherwise agreed to the document to which the signature is attached.“* [Kalakota/Whinston 1996, 202].

A German legislation initiative for the acknowledgment of digital signatures unfortunately started a discussion concerning definitions of the electronic signature, resp. digital signature. The legislation bill, supposedly meaning the digital signature, uses only the term electronic signature, and describes the method of creating a digital signature. Even some well known researchers and authors do not differentiate between those two constructions, as we see for instance in [Herda 1995, 109].

### 4.1 Electronic Signature

An electronic signature represents a digitalized image of the personal signature. These digitalized images are handwritings, which are saved as pictures (see figure 1). An electronic signature may originate from a scanned personal signature, which is put to disk in image formats such as gif, bmp, jpg or others. Because electronic signatures are bit and byte representatives of the personal signature they may be subject to manipulation. Unsecured open networks or infrastructures may cause or even simplify a potential manipulation of electronic signatures. An electronic signature is nothing else, than a simple photography of the personal signature, which can be found on any traditional legal statement [Rossnagel, 1996].

Signature of Charles the Great.  
Charles the great simply signed by drawing the rectangular in the middle of the four letters. The rest of the monogram was done by a writer (see [Löhmann, 1995]).



**Figure 3:** Personal signature of Charles the Great

In contrast to the digital signature, which is capable of offering certainty of integrity of sent messages, the electronic signature is not able to offer this surety of integrity. Furthermore, a clear identification of corresponding messaging-partners is not possible. Electronic signatures are unable to support an undeniable link to the original message content.

However, for researchers with a technical background, there is a difference between the *electronic signature* and the *digital signature*. The definition, as it is used in the German legislation bill, represents a „remarkable misconception“. According to [Rossnagel, 1995] and others we do have to draw a clear distinction between the *electronic signature* and *digital signature*.

### 4.2 Digital Signature

According to [Bizer, 1995], a digital signature is the „technical artifact“, which is generated by the use of asymmetric enciphering systems. No close relationship between a digital signature and

someone's personal signature can be pointed out. The fundamental principle of digital signatures is according [Diffie/ Hellmann, 1996] the principle of public-key enciphering systems. They identify the following requirements for digital signatures:

- The digital signature is dependent on the signing person and on the content, which is to be signed.
- Only the signer is able to create the digital signature for a specific message-content.
- Every one else is able to verify the digital signature.

Digital signatures give certainty of integrity in contrast to electronic signatures. Digital signatures may be manipulated during the transport likewise to electronic signatures, with a very decisive difference though: Once a digital signature was altered, it is useless for further third parties, who may claim to be the owner of some digital signature.

```
3081b4a04f310b300906035504061302444531183016060355040a130f49424d2044657574
7363686c616e64310c300a060355040b1303454e43311830160603550403130f416c657861
6e6465722052756e6765810d3936303131363130303731355aa20f300d06092a864886f70d
010104050083410048a66465bca9ef237a777298e91c73280b72fb265dbb816a8766197ea91
ef5d00448ba8f718f1ea0bc23522b5d5a347074a3444c160a94d10c05a2e71b2d344f
```

**Figure 4:** Example of a digital Signature

Further discussions of this paper focuses on digital signatures exclusively. Once signatures are used as substitutes for personal signatures, they have to respect certain legal functions as discussed in the next section.

## 5 Legal Functions of Signatures

The basic idea of each negotiated, agreed and settled contract is to express the will of each contracting partner to settle the negotiated contract with all its legal consequences. Normally, no specific way is required to express this will. Each party may express its will by a written or oral agreement or even by handsigns. However, certain circumstances request by law special forms of expression of will. This requirements of form are necessary for the contract to be reliable (e.g. part payment contracts). The most known form-requirement is the requirement of a written and signed document.

Parallel to the decision to require form specifications, such as the writing and signing requirement, from electronic contracts signatures itself need to observe certain required legal functions. The number of observed legal functions depend on the author and the applicable law. Functions of digital signatures according to [Rihaczek 1992, 4] partly match functions of digital signatures, which are identified by [Bizer/ Hammer, 1993]:

- **Settlement Function**

The signature is supposed to assure, that contract negotiating parties know and accept all the facts, which are written in the contract document. This function depends *not* on the signature itself, but on the *activity* of signing. The signature shows clearly, that the signer accepted the contract with the action of signing.

Every digital signature, that was not added to the document automatically, can fulfill the requirement of the Settlement Function. However, it is absolutely necessary, that the author of the document initiates the command to sign the document.

- **Disputability**

The Disputability Function is very much debated about, since it is very closely linked to law. In case of disputes between two or more communicating partners, electronic documents such as orders, order acknowledgments and others must be usable as evidence in front of court.

- **Perpetuation**

By law, some non electronic documents have to be filed over a period of one, two or even more years. The maximum term of prescription in German law is 30 years. Therefore, a document is not supposed to be changed afterwards in order to assure disputability.

As a conclusion of terms of prescription, the digital signature must be used in such a way, that a manipulation of digital signatures or the contents itself is not possible afterwards. The digital signature must be used in such a way, that older digital signatures are still verifiable. Of course, digital signatures must be stored for the same terms of prescription as the documents and contents itself.

- **Identity Function**

In comparison to personal signatures, which state the identity of signing persons, digital signatures do have to declare the identity of the signing person. However, natural persons may have several digital signatures to sign with. This possession of several private keys, which are used to generate digital signatures, depends on the role, a person assumes at a specific moment. Thus, an absent owner of a company, who is supposed to digitally sign an agreement, may be substituted by a partner, if this partner has access to the secret key of the former. The substitute then acts on behalf and in the role of the company owner.

- **Transparency**

Transparency states the function of the signer. Although this function is not demanded by most laws [Gauch/ Schlupe 1991, 86], a lot of enterprises have rules, that reserve certain legal actions to certain positions in the company. Law defines and matches specific competencies to certain positions. For example, the Swiss law knows a signature *per Prokura* and a signature *per Handelsvollmacht*. However, not every position in the company is allowed to perform a signature per Prokura or a signature per Handelsvollmacht.

The use of special and distinct secret encryption keys displays and reveals the impersonated role of the signing person. The function and role of the signer is identified by means of digital signatures, and therefore the digital way of signing declares the function and role of the signer much safer than a personal signature.

- **Unforgeability**

A verifier does not only want to be sure, that a digital signature is closely linked to the signed content and thus covers the content, he also wants to be sure, that the verified digital signature is not subject to manipulation during the transport across open, partly unsecure communication infrastructures.

Contracts are only reliable, if they represent the exact will of the participating contract partners. Thus, unforgeability is naturally a requirement of each contract.

A digital signature, which is certified by a third party, will assure unforgeability much better than a hand-written signature. Of course, this unforgeability depends on the correct work of signature applications and the confidentiality, which is put into certification authorities.

- **Visibility**

Due to the syntax and outer appearance of digital signatures, human beings are not able to read or even verify digital signatures. Thus, identity, role and reason of digital signatures must be verified by IT-systems. This implies, that confidence in digital signatures is shifted to confidence in verifying IT-systems. A content of some electronic document, which is to be signed and displayed on the computer screen does not necessarily need to be the same content which is being signed within the memory of the computer.

- **Warning Function**

The action of signing must raise the awareness of contract negotiating parties, that they are about to accept legal consequences, which are eventually linked closely to electronic contracts. The warning function makes the signer confirm, that he recognizes, that a defined electronic document will *imply legal consequences*. The Settlement Function differs from this warning-function, it makes the signer confirm, that he is about to *settle* a contract.

## 6 Technical Mechanisms for Realization of Legal Functions in Digital Signatures

*„A combination of access controls, encryption technologies, and digital signatures can be used by copyright owners to protect, license, and authenticate information.“*  
[Kalakota/ Whinston 1996, 592].

Technical means, which are used to realize the above mentioned above-mentioned (section 5) legal requirements on signatures include encryption systems, certification authorities in co-ordinance with trust centers, electronic notary services, hash functions and additional means of applications as described next.

- **Encryption**

With the technique of encryption, a normal, normally readable text is transformed into an enciphered text by using some secret formula. In asymmetric encryption, this secret formula is a pair of keys, where one key (the secret key) is used for the generation of a digital signature, the corresponding other key (the public key) is used for the verification of such a digital signature.

With the use of encryption mechanisms, requirements such as disputability, the identification function and unforgeability are satisfied (see table 2). Once digital signatures will be legally acknowledged, disputability is fulfilled in co-operation with hash functions. The source or the originator (Identification-Function) is checked by verifying the secret key itself which was used to generate the digital signature and the composition and coherence between the content and the digital signature is verified by hash functions (see below). Thus, it is possible to clearly identify the author of an electronic document, accept the signed content as his will (because it was covered with the digital signature) and use it as evidence in front of court (once these mechanisms are accepted).

Encryption mechanisms ensure unforgeability of digital signatures only in conjunction with Certification Authorities. If secret keys are issued only once and are securely saved on Personal Security Environments (PSE) or chip cards (Personal Trust Centers: PTC), no one is able to forge someone's digital signature.

- **Trust Centers and Electronic Notary Services**

Certification Authorities and Trust Centers do not only issue and verify key-pairs, but store and file additional information on associated users of key-pairs. A request to verify a public key of someone may include a request to give additional information on that specific user. Organizational roles, authorizations and authentications are thus to be found out, in order to fulfill transparency, *why* that specific user signed that document.

Trust Centers, in the sense of electronic notary services, will eventually store all kinds of information. They may even file electronic contracts itself. Because electronic contracts do have special terms of prescription, these contracts have to be stored over a longer period of time, of course legally acknowledged, including the digital signature. These stored digital signatures must not be subject of, manipulation; they have to be protected. Once electronic notary services will emerge, they will ensure perpetuation of files and digital signatures in the same way Certification Authorities ensure security of key-pairs.

- **Hash Functions**

Hash functions are mathematical one-way functions, where some input byte stream, is transformed into a decimal sum. Because it is not possible to draw a conclusion from the resulting hash sum to the initial input stream, hash sums are used to realize a close coherence between the contents (the initial input stream) and the final digital signature. This coherence is due to the way of creating digital signatures. Digital signatures are created by applying the owners secret key onto the resulting output stream of the hash-sum.

By applying hash sums to electronic documents, immediacy between the content itself and the digital signature is realized. If just one letter of the original content is altered, the hash function generates a hash sum, which is different from the original calculated and signed hash sum. Once mechanisms such as hash-functions and encryption are acknowledged, electronic documents and thus electronic contracts observe disputability.

Mechanism / Requirement	Settlement-function	Disputability	Perpetuation	Identityfunction	Transparency	Unforgeability	Visability	Warnfunction
Encryption / Trust Center		X		X		X		
Trust Center / Electronic Notary Services			X		X			
Hashfunction		X						
Additional means of applications	X						X	X

**Table 2:** Realization of requirements on digital signatures

- **Additional Means of Applications**

The settlement and warning functions are satisfied by additional means of signature applications. Additional means of applications are extra confirmation calls from applications to verify actions, which were requested by the user. A certificate of correct work for signature applications accomplishes this, especially clarity.

Users, who want to sign an electronic document, start that signature process by figurative pushing a button on the monitor. If the application, which is actually signing the electronic document, asks the user again, if he is really sure to sign the document, the settlement function is realized. If the application prompts the user once again and tells him, that he is about to make a declaration of will and that this commitment will eventually have legal implications, the warning function is satisfied.

Of course, users want to be ensured, that documents, which were displayed on the monitor, are exactly the same documents, which were actually signed by the computer. They also want to get a certificate on the correct enforcement of the signing process. The only way to realize this requirement, is by certifying signature applications, of course carried out by an accepted and acknowledged public institution like a technical control board or an association for technical inspection.

Modern information society has enough means of satisfying identified requirements on digital signatures. Digital signatures are well suited and will have a wide range of usage in Electronic Commerce environments, e.g. for electronic contract negotiations, ordering products and services and of course doing secure electronic payment transactions. One way to realize digital signatures is by saving secret keys on chip-cards, which may have enough memory space for additional services as described in the next chapter.

## 7 Digital Signatures in the German Homebanking Computer Interface

The discussion about smartcards and their utilization as multi-functional tokens have been known since more than a century. A lot of smartcards are in use, e.g. as phone or bank cards, but the very most of them are mono-functional. The real potential of smartcard technology has not been realized yet.

Since a few years we have an intensive discussion and growth in the field of Electronic Commerce via the Internet. But there are some very fundamental obstacles which will inhibit the success and growth of EC. These are, among others mentioned above, the lack of real comfortable and secure payment systems as well as a trustworthy environment for business transactions in a mass market.

For the success of telematic applications the acceptance by users is essential. Instruments to achieve the acceptance especially in a mass market are the use of well known and established tokens. One of these potential tokens are the 'eurocheque-cards' (ec-cards) that are well established in most of the European countries. For example, in Germany 55 million ec-cards are issued. These cards are standardized on an European level and they are issued by banks. They serve in their original meaning as a security token for the eurocheques. Nowadays, ec-cards have a magnetic stripe and are mainly used as ATM- and debit-cards. Security is established by using a PIN (Personal Identification Number)-code. To summarize it, ec-cards are well known to the most European consumers and are well accepted as a payment instrument.

With the beginning of 1997 ec-cards in Germany, as well as in other countries like Austria and Switzerland, are equipped with an additional chip. The new ec-cards are hybrid cards because they still have the magnetic stripe. On the one hand they will have the same functions as traditional ec-cards. But with the introduction of the chip these cards can be considered as smartcards. These new, smart ec-cards will be used (1) as electronic wallets and (2) as a security token for telebanking applications [Krebs, 1996], [Sperlich, 1996].

First of all the smartcard serves as an electronic wallet and thus aims at a substitution of the electronic cash, as it is used today, especially in the segment of small amounts between 3 to 17 US\$. The cards may be loaded by using the existing, but upgraded ATMs. The owner then may pay small amounts by using this new functionality of the ec-card. Therefore the merchant has to apply special off-line terminals. The electronic wallet has no security functions and the same attributes like real cash; it is anonymous. Losing the card means losing the money stored on the electronic wallet.

The chip on the German cash card, called 'Geldkarte', will not use all the capacity for the wallet functionality. While the electronic wallet functions are standardized by all issuing banks in Germany, the usage of the free memory space on the chip can be applied for individual purposes. Typical applications are, e.g., bus-/ train-/ theater-tickets or marketing applications of department stores like customer tracking.

The 'classical' telebanking solutions, offered by the German banks through media like the videotex successor T-Online or even the Internet, use a security system consisting of (a) an user-ID and (b) a PIN (Personal Identification Numbers) to log on to the system and (c) a TAN (transaction number) for each (payment-) transaction as a substitute for the signature. The handling of this system is not very comfortable, e.g. you have to manage the use of TANs, and, furthermore, it is not the most secure.

To overcome this old fashioned way of authentication and authorization, the German banking industry developed a new telebanking standard, the 'Homebanking-Computer-Interface' (HBCI) [SIZ, 1996]. The homebanking specification HBCI creates an automated and multibanking capable interface. HBCI is platform and device independent and describes the interface between the customers client software and the bank system. HBCI deploys RSA for message verification and encryption, e.g., utilizing the above mentioned smart ec-card.

In a typical HBCI transaction a password authorizes a user to access the banking system. Each user has a unique digital signature based on the RSA algorithm. The HBCI architecture also includes a

mechanism to check for message integrity by placing a signed hash code over a message [Amdur, 1997].

To be compatible to already existing telebanking security solutions there are also specifications for these solutions described. Until the necessary infrastructure is established, e.g. a chipcard reader for each PC, a hybrid, software based DES-based solutions will be applied in the first step.

The first implementation of HBCI as a RSA-based software solution was realized for the Internet-Banking system of the Raiffeisen-Volksbank Mainz (Germany). After the opening of the account the bank generates a pair of keys for the new customer. The public key remains at the bank, the secret key for the customer is encrypted and stored on a diskette. The HBCI-based communication between the bank and the customer uses its own channel, but not the http protocol. The customer's authentication will be verified utilizing a digital signature that is generated using the secret RSA-key. The bank will verify the signature applying its public key. A transaction number (TAN) is no longer needed [Luckhardt, 1997].

As the first group in the German banking industry, the saving banks will apply the chipcard-based security solution. The smart ec-card will be used to create off-line a digital signature as a means for securing electronic payment transactions as stated in the previous sections. This will foster the use of telebanking and thus electronic payment and abolish the use of PINs and TANs. Thus it will improve user comfort and security.

It is very obvious how the utilization of the theoretical and technical aspects of the digital signature, as described in the previous sections using a smartcard like the German 'Geldkarte' will have an enormous impact on Electronic Commerce due to the emerging potentials of a trustworthy environment for EC. Especially the existence of a really secure telebanking/payment system will push the diffusion of EC in the retail sector.

## 8 Conclusion

The use of digital documents will expand according to quantity and quality not only in the scope of Electronic Commerce. However, the legally-acknowledged use of digital documents and digital signatures, especially in fields such as Electronic Commerce, will be very decisive for the further dissemination of Electronic Commerce in general or tools of various phases especially.

Of course, if digital documents are used for orders, order acknowledgments or electronic contracts, they must obey legal requirements such as form restrictions. Form specifications as they are defined by law today can not *exactly* be fulfilled by technical means. However, existing technical means and their combined use for creating digital signatures in digital documents do offer a better security and (not yet) legal background, although these technical mechanisms are not explicitly defined by law. This paper shows, how technical means may be combined and thus fulfill the *meaning* of legal requirements. It is possible to put legal requirements into practice current technical means need only to be accepted by law.

To generate a legally accepted background for the transmission of digitally signed documents law needs to accept already developed and used technical means such as encryption technologies or Trust Centers. This adaptation of law must happen in a homogenous global effort. The Model Law on Electronic Commerce of the UNCITRAL is a very usable draft for that.

The creation and use of digital signatures is therefore no longer a problem, despite the fact, that digital signatures are not yet accepted by law. However, the adaptation of law will take a long time. Today, it is desirable for organizations to evolve and take over trustbuilding services such as Trust Centers, Certification Authorities or digital electronic notaries. The fact, that digital signatures are not yet accepted legally will not hinder these services very long, since digital signature legislation bills are in discussion in some countries already. Therefore new service providers should be established in order to gain experience and knowledge in the provision of these new services. These service providers will then be perfectly suited to provide *legally* accepted trustbuilding services with the adoption of digital signature bills.

## References

- [Amdur, 1997] Amdur, Dan: „European Banks Play Their (Smart) Cards“; in: BYTE April 1997, pp. 40IS7-12, 1997.
- [Baum/ Perrit, 1991] Baum, M.S./ Perrit, H.H. jr.; „Electronic Contracting, Publishing and EDI law“; Jon Wiley & Sons, New York; 1991.
- [Bizer, 1995] Bizer, J.; „Voraussetzungen und Bedingungen für die rechtliche Anerkennung digital signierter Dokumente“; in: Horster, P. (Hrsg.): „Trust Center“; DuD; 1995.
- [Bizer/ Hammer, 1993] Bizer, J./ Hammer, V.; „Im Namen des Volkes: ... Sie haben signiert! Beweiswert elektronisch signierter Dokumente“; in: GMD-Spiegel, Nr. 2/93; June 1<sup>st</sup>, 1993.
- [Bons/ Lee/ Wagenaar, 1994] Bons, R. W.H./ Lee, R.M./ Wagenaar, R.W.; „Implementing International Electronic Trade Using Open-EDI“; Working Report No. 94.12.01; Euridis Institute of the Erasmus University Rotterdam; December 1994.
- [Gauch/ Schlupe, 1991] Gauch, P./ Schlupe, W.R.; „Schweizerisches Obligationenrecht, Allgemeiner Teil“; Schulthess Polygraphischer Verlag; Zürich; 1991.
- [Herda, 1995] Herda, S.; „Zurechenbarkeit – Verbindlichkeit – Nichtabstreitbarkeit“; in: Struif, B.; „Digitale Signatur und Sicherheitssensitive Anwendungen“; DuD-Fachbeiträge; 1995.
- [Igbaria/ Sprague, 1996] Igbaria, M./ Sprague, R. H. jr.; „Introduction to the Minitrack on Digital Documents on Organizations and the Workplace“; Proceedings of the 29th Annual Hawaii International Conference on System Sciences; Volume V; 1996.
- [Kalakota/ Whinston, 1996] Kalakota, R./ Whinston, A.B.; „Frontiers of Electronic Commerce“; Addison-Wesley Publishing Company; Reading, Massachusetts; 1996.
- [Koller, 1996] Koller, A.; „Schweizerisches Obligationenrecht, Allgemeiner Teil: Grundriss des allgemeinen Schuldrechts ohne Deliktsrecht“; Stämpfli & Cie. AG, Bern; 1996.
- [Krebs, 1996] Krebs, T.; „Elektronische Geldbörse - Grundlagen, Erfahrungen, Perspektiven.“; in: Informatikzentrum der Sparkassenorganisation GmbH (SIZ-Special); 1996.
- [Löhmann, 1995] Löhmann, B.; „Anwendungen der digitalen Signatur in der Kunde-Bank-Kommunikation und im Interbankenverkehr“; in: Struif, B.; „Digitale Signaturen & Sicherheitssensitive Anwendungen“; DuD-Fachbeiträge; 1995.
- [Luckhardt, 1997] Luckhardt, Norbert: „Auf dem Weg zum Standard?“; in: c't Report Geld Online, pp. 25-26, 1997.
- [MD 4, 1991] MD4 EDIFACT Security Group; „Security framework for EDIFACT“; document 1.19 v.1.6; 1991.
- [Meier/ Sprague, 1996] Meier, J./ Sprague, R.; „Towards a Better Understanding of Electronic Document Management“; in: Proceedings of the 29th Annual Hawaii International Conference on System Sciences; Volume V; 1996.
- [Palmer, 1997] Palmer, J.W.; „Supporting Diverse Activities with Digital Documents: A Pilot Study of The Peter F. Drucker Manuscript and Archives Project“; in: Proceedings of the 30th Annual Hawaii International Conference on System Sciences; Volume V; 1997.
- [Rihaczek, 1992] Rihaczek, K.; „Das elektronische Unterschriftssurrogat“; DuD, Nr. 1/ 92.
- [Scheidegger/ Zbornik, 1993] Scheidegger, P./ Zbornik, S.; „Sicherheitskonzepte für offene elektronische Märkte auf der Basis von EDI“; working report No. IM2000/ CCEM/ 18; Institute for Information Management, University St. Gallen; March 12th, 1993.
- [Schmid 1995] Schmid, B.; „Electronic Mall: Banking und Shopping in globalen Netzen“; B.G. Teubner, Stuttgart; 1995.

- [**Schmidlin 1985**] Berner Kommentar, Art. 1 - 18 OR, Bern 1985.
- [**SIZ 1996**] SIZ (eds.); HBCI - Homebanking-Computer-Interface Schnittstellenspezifikation, Vers. 1, August 1996, Bonn.
- [**Smedinghoff, 1996**] Smedinghoff, T.; „Online Law - The SPA’s legal guide to doing business in the Internet“; Addison-Wesley Developers Press; Reading, Massachusetts; April 1996.
- [**Spar/Bussang, 1996**] Spar, D./ Bussang, J.; Ruling the Net; in: Harvard Business Review, May-June 1996, pp. 125-133.
- [**Sperlich, 1996**] Sperlich, T.; „Bündel, Scheine und Münzen: Mit der Smartcard auf dem Weg zur bargeldlosen Gesellschaft.“; in: c’t Magazin No. 7; 1996; pp. 98-101.
- [**Tan/ Bui, 1996**] Tan, M./ Bui T.; „Exploring the Impacts of Electronic Imaging on Organizational Process, Structure, and Strategy“; in: Proceedings of the 29th Annual Hawaii International Conference on System Sciences; Volume V; 1996.
- [**UNCITRAL 1996**] United Nations Commission on International Trade Law: UNCITRAL Model Law on Electronic Commerce. <http://www.un.or.at/uncitral/texts/electcom/english/ml-ec.htm>; February, 3<sup>rd</sup> 1997.