BILETA

14th BILETA Conference: "CYBERSPACE 1999: Crime, Criminal Justice and the Internet".

Monday, March 29th & Tuesday, March 30th, 1999.
College of Ripon & York St. John, York, England.

Securing Electronic Commerce with Digital Signatures - Do Digital Signatures Comply with the Legal Criteria for the Written Form and Supply Equal Proof?

Thomas Menzel and Erich Schweighofer
University of Vienna
Institute of Public International Law and International Relations
Research Center for Computers and Law

Abstract: *Due to the rapid growth of Electronic Commerce, the legal classification of digital signatures and certificates, which are fundamental tools for contracts via the Internet, is of vital interest. Security against fraud and misuse must at least be equal to traditionally signed written papers.*

*This paper will discuss the impact of the proposal of an EU-directive concerning Digital Signatures, granting in Article 5 qualified digital signatures the same legal effects as the hand-written signature, and Article 2 of UNCITRAL's Draft Uniform Rules on E*lectronic Signatures, which state*s independent presumptions on proof.*

The procedure of digital signing, using the framework of a strong Public Key Infrastructure, will be compared with hand-written signing, examining the classical function of a signature to verify the signer's identity, worked out by legal science. We will demonstrate that using current technologies, digital signatures fulfil the function of authentication. The second part will concentrate on the most crucial function of verification using biometric methods to assure identification of the communication partners on the same level as using hand-written signatures on paper.

The Limits of the traditional Method

Paper is a trusted medium for holding legal and audit evidence, People are familiar with this medium, and centuries of experience have tested the application of evidence to paper documents [Wright 1996]. Supreme courts have established detailed case law about the authenticity of signatures on paper documents and legal science has extracted basic functions, which are indeed applicable for every signature, from the case law centered around problems with hand-written signature.

Nevertheless, because of the different nature of written statements on paper and electronic documents, hand-written signatures and scanned images are not applicable for the use of electronic messaging systems. A paper document consists of the carrier (the sheet of paper), text or pictures, information about the issuer and a written signature. All of these parts are physically connected, and due to the nature of paper and ink, every modification leaves a mark. An electronic document is

imprinted on a magnetic support and can be deleted, modified or rewritten without traces of evidence. To ensure identification, authenticity, declaration, and proof, the process of signing should be substituted by new electronic methods.

Symmetric Cryptography

Applying symmetric cryptography on electronic documents, both persons – the sender and the addressee of the message - use the same secret key to encrypt and decrypt the message. The key has to be kept secret. The main problem is getting the sender and receiver to agree on a secret key without anyone else finding out. The key has to be transmitted using a different and secure channel from the communication line, which is used for the encrypted communication. Otherwise, anyone who overhears the transmission of the key, can later read and modify all messages encrypted with this secret key and is able to create new messages with the wrong identity [Pohl 1997, Stallings 1995].

The method works fine if the communication partners are physically present during their first meeting, where they can identify each other and exchange the key by traditional methods. Symmetric cryptography does not provide functionality to verify the identity of communication partners at their first contact. Further everyone has to share with each of his communication partners a unique secret key, forcing the users of symmetric cryptography to establish a large key database.

In Electronic Commerce, customers and dealers want to settle their one-shot deals only by electronic communication. An initial consultation to agree to a secret key prior to the electronic conclusion of the contract is not economically reasonable for one-shot deals. Therefore, a different technique, which can also handle verification of the identity and authenticity via electronic communication between strangers, is necessary to guarantee legally binding statements for transactions.

Asymmetric Cryptography, Digital Signatures and Certificates

The concept of asymmetric cryptography was introduced in 1976 by Diffie and Hellman in order to solve the key management problem. In their concept, each person gets a pair of different but related keys, one called the public key and the other called the private key. Each person's public key is published while the private key is kept secret. The need for the sender and receiver to share secret information is eliminated. All communications involve only public keys, and no private key is ever transmitted or shared. No longer is it necessary to trust some communication channels to be secure against eavesdropping or betrayal [Pohl 1997].

When someone wants to send a message, he only has to encrypt the text with his private key and transmits it to the addressee. The receiver seeks for the sender's public key and decrypts the text with this key. Encrypting the text with the addressee's public key produces a confidential message, which can only be decrypted with the addressee's private key. Applying both encryption processes one after another generates confidential and authentic messages. It is one of the system's definitions: that a message encrypted with one key of the key pair can only be decrypted with the corresponding other key. If the decryption process with the senders public key leads to a meaningful text, it is assured that only the sender's private key could be used to encrypt the message.

The only system requirement is that public keys are associated with their users in a trusted and authenticated manner, in a trusted directory, for instance. Anyone can send a confidential and authentic message by just using public information, but the message can only be decrypted with a private key, which is in the sole possession of the intended recipient.

At this stage everyone can choose freely the identity mentioned in the e-mail and the public key. It follows that another institution must support the infrastructure to ensure the correct binding of the entity to its named identity. Trusted third parties – also named certification authorities in some laws -

assure the user that the corresponding private key to the public key used to verify a signature is actually in the control of the named sender who has signed the transaction. Therefore, the user has to register locally in the trusted third party's office to check his identity and ensure his exclusive ownership of a key pair. These trusted third parties issue an electronic certificate for every public key, which contains the trustworthy assurance of the relationship between the identity of the keyholder and his public key. This certificate is also digitally signed with the trusted third party's private key, so it cannot be falsified. A directory of all certificates is maintained and provided on the Internet to allow online verification of validity and integrity of the received certificates. These services in a network of trusted third parties helps to erect a public key infrastructure providing trust in the Internet.

In summary the combination of digital signatures and certificates, which can be verified online with the use of the public key infrastructure, establishes analogue functionality of digital and hand-written signatures on the Internet to secure electronic commerce.

Most of the legislators realised the influence of the new technique and reacted by providing a legal framework to regulate the conditions for a strong and secure public key infrastructure [COM(98) 297]. The German Signature Act [SigG 1997] defines a digital signature as a seal affixed to digital data, which is generated by a private signature key, and establishes the owner of the signature key and the integrity of the data with the help of an associated public key, provided with a signature key certificate of a certification authority. A certification authority shall mean a natural or legal person who certifies the assignment of public signature keys to natural persons. A large set of mandatory security requirements for the operation of certification authorities shall help to improve the strength and security in the infrastructure.

Substitution of the Functions of Hand-written Signatures by Digital Signatures

The Current Legal Situation

The legal systems of most states give special preference for written documents. Some agreements, such as contracts of suretyship, last wills, or contracts approved by a notary are only valid, if they are written on paper. According to evidence law legally binding statements mentioned as proof before a court provide a better position if they are in written form. In Civil Law countries, paper documents with affixed hand-written signature statute full proof [Remotti 1997]. Clearly the statements in the document come from the signer until the opponent can prove the opposite. According to the current situation in most European countries this rule is only applicable for paper documents with a hand-written signature. Therefore, most parties agree for their business transactions which are not mandatory in the written form upon the use of papers, because their easier use of evidence. If the written form is not possible, for example in EDI communication, most parties constitute an arbitrating body for future dispute settlement, which is bound by contract to treat proof given in electronic form the same way as proof printed on paper.

Without this mutual agreed modification to evidence law, digital signed electronic documents, which might be offered at trial as evidence, are only subject to prima facie evidence [Rihaczek 1995]. To give full proof about its content at trial each electronic message must be individually authenticated and identified. The proponent must convince the court of the authenticity of the electronic document applying general rules of logic and experience of life. This rule of evidence for digitally signed electronic documents leads to a more hazardous situation for the proponent relating to electronic documents as a matter of proof in comparison to written papers.

New Proposals

During this century, most legal systems have reduced formal requirements, or at least have minimised the consequences of failure to satisfy formal requirements. Nevertheless, this process is

still in the beginning and various legal barriers still exist and prohibit seasonable legal recognition of modern communication and workflow models. Any case relating to electronic commerce is characterised by the absence of written documents and their substitution with electronic documents. To avoid difficult procedural requirements for daily used transactions which are only electronically recorded several proposals [UNCITRAL 1996, COM(98)586] demand a more or less equalisation of the legal effects between hand-written and digital signatures. The formal requirements for legal transactions, including the need for signatures, vary in the different proposals.

UNCITRAL

At an international level, the United Nations Commission on International Trade Law (UNCITRAL) has worked out Draft Uniform Rules on Electronic Signatures [UNCITRAL 1998]. With regard to the potential influence of electronic commerce on the changing of communication methods, and in recognising the difference of the methods, the Draft Rules try to harmonise the situation by stating presumptions about the legal recognition of digitally signed electronic documents:

It is rebuttably presumed for data messages authenticated by secure electronic signatures, that the data message has not been altered since the time the secure electronic signature was affixed to the data message, the secure electronic signature is the signature of the person to whom it relates, and that the secure electronic signature was affixed by that person with the attention of signing the message.

A digital signature is regarded as a secure electronic signature, if the digital signature was created during the operational period of a valid certificate and is verified by reference to the public key listed in the certificate. This certificate is then considered as accurately binding a public key to a person's identity because the certificate was issued by a licensed certification authority or by a certification authority in accordance with issued standards.

Other digital signatures, which do not meet the requirements for secure electronic signatures, give only prima facies proof. The proponent has to provide sufficient evidence that indicates the certificate is accurately binding the public key to the holders identity.

European Union

Similar to UNCITRAL's regulation, a Proposal for a European Parliament and Council Directive on a common framework on electronic signatures [COM(98)297] plans to establish two levels of evidence provided by electronic signatures with regards to the quality of the signature, the certificate, and the certification authority. The higher level rules legal effects for secure electronic signatures with a qualified certificate. This certificate can only be issued by certification authorities which fulfils a set of security requirements. To contribute to the legal recognition of electronic signatures, Article 5 of the Draft regulates the relation to the written form and what degree of evidence this high graded electronic signature shall provide. In contrast to the UNCITRAL Draft Rules, the proposal of the European Commission does not give exact and detailed rules, excluding which facts have to be presumed under what circumstances. It does, however, state a general order to admit electronic signatures as evidence in legal proceedings:

Advanced electronic signatures, which are based on a qualified certificate and which are created by a secure signature creation device, satisfy the legal requirement of a signature in relation to data in electronic form in the same manner as a hand-written signature satisfies that requirement in relation to paper-based data, and are admissible as evidence in legal proceedings.

It is of interest to look at the modifications in the last sentence of this article. The newest version of the document from January 1999 is only in principle granting the admission of qualified digitally signed documents, however, the draft's previous version from May 1998 equated electronic

signatures and hand-written signatures concerning their admission in legal proceedings:

Electronic signatures, which are based on a qualified certificate issued by a certification service provider, which fulfils the requirements set out in Annex II, are admissible as evidence in legal proceedings in the same manner as hand-written signatures.

This revision in the newest version was a result of the reservations of some EU member states against the former formal equalisation, prompted by a different solution in their own national legislations to the different legal situation in some member states. They are now voting for a longer test-phase, so that people can adapt to the differences between hand-written and digital signature in daily use. In this test-phase digital signatures shall be admitted only for prima facies proof, thus, the courts are granted more freedom to examine the strength of each digitally signed document with the support of experts. The procedural facilitation in evidence law for papers - as a result of the high trust and knowledge people give to paper - should not be applied to electronic signatures until the usage of a public key infrastructure is far more popular used and the system is more closely tested and examined.

The second part of article 5 deals with the legal effects given to every electronic signature, independent of the combination with a qualified certificate. An electronic signature is not denied legal effectiveness and admissibility as evidence in legal proceedings solely on the grounds that the signature is in electronic form, or is not based upon a qualified certificate, or is not based upon a qualified certificate issued by accredited certification service provider, and or is not created by a secure signature creation device. In our opinion, this new formulation of the second part of this article has reduced the relevance of this general regulation about admission. In the old version, the general regulation allowed the basic recognition of electronic signatures for evidence, and the more specific first part expanded the legal recognition to grant the same procedural weight for qualified electronic signatures and hand-written signatures. In the actual state of the draft, both legal provisions - the general one and the rule applying only to qualified electronic signatures – establish the same effect: the admission of proof by electronic signatures cannot be denied by courts. Both kinds of electronic signatures provide the same features, and the incentive for qualified electronic signatures is, thereby, eliminated. As a result no one will use freely more qualified, and, therefore, more expensive electronic signatures issued from certification authorities with a higher security standard according to Annex II of the proposed directive. In combination with article 3, which prohibits the control of the quality of certification provider through a governmental controlled licensing system, this could lead to reduction of quality and security in the complete system of the public key infrastructure.

The Functions of a Signature

It is a common opinion that many attributes of paper–based communication - writing and signing used in a traditional way - contribute to satisfying the legal requirements for signatures. A company’s name and logo appearing on a purchase order, the letterhead at the top of a correspondence, or the hand-written signature at the end of the document are examples to support authenticity, verification of identity, non- repudiation and other functions of the written form. These attributes are lost or weakened in the move to electronic messages [Smedinghoff 1996]. With electronic communications, however, there can be no traditional writing and hand-written signing, due to the basic difference of the analogue form of writing and signing and the digital nature of electronic communication in cyberspace. In opposition to handwriting and printing, there is nothing inherently distinctive about the bits that built an authentic electronic message that distinguish them from the bits that are resembled to a copy or forgery of that electronic message. Referring to the verification of the identity is the problem, that the Internet is a place, where spoofing and faking an false identity can be realised very easily. Lastly the paper – based medium and the message on it are inherently bound together; that is, they are transmitted together in one physical object. In networks, electronic information flows absent a physical medium until it is displayed on the screen or printed

out. Therefore, evidence law constitutes reasonable differences in the quality of proof provided by traditional paper-based messages and simple electronic messages not secured with digital signatures.

It is a logical consequence that a system, like a public key infrastructure, follows totally different underlying principles, technical methods and uses different attributes to provide for the users in the end the same functionality. To evaluate compatibility and usability for the legal application, we have to measure the new system by the functions of signatures lined out in case law and extracted by legal science.

Verification of Identity

It is most important that a signature should indicate the person who signed a document, message or record, and it should be difficult for another person to produce it without authorisation [ABA 1996].

The most crucial point to satisfy this requirement by the use of digital signatures is the possibility to access a private key. According to the nature of the underlying technique of asymmetric encryption anyone who has access to the private key can digital sign messages indistinguishable to the certified holder of the responding keypair. The recipient of the message only can verify the content of the certificate, which tells him trustworthy to whom the certificate and the keypair belongs. He cannot be sure, who is really using the private key to encrypt that message he has received. To restrict access to the private key only for the authorised user is the most critical task in the complete system. This is done by the process of authentication, which is executed to check the authorisation of a user before granting access to a private key for encrypting the hash code of a message. Authentication means the service designed to verify the user's identity. Identification and authentication can be made by knowledge (for example: password protection), by possession (for example a smart card), or by checking the user's human characteristics (biometrics) [Polemi 1997]. Recommendable and often realised in computer programmes is a combination of authentication by possession and knowledge or human characteristics.

At a low security level the private key is stored on the harddisk of a computer, which is often connected to the network. Knowledge of a password is the only authentication to get access. In combination with common user praxis handling their passwords and security breaches of personal computers this method provides definitely not enough safety for a secure key storage. The next step to secure private keys is to store them on a medium, which is physically in the exclusive possession of the certified keypair holder. Smart cards comply with this condition. The complete encryption process is taking place on the card, because the card contains a RSA microprocessor and can handle hashing of the message and encrypting the hash code with the local private key. Finally only the results of the encryption process will be transmitted to the network, so the private key never leaves the smart card to be stored temporary on insecure systems. The hardware of the card is designed to prevent the extraction of the data of the private key [Rhein 1997].

These techniques satisfy the requirement of authentication as long as the smart card is in the possession of the corresponding certificate holder. However, field studies [Pordesch 1993] examining the use of smart cards have shown, that authorised holders give them together with the password necessary to encrypt on the card freely away to secretaries and self nominated service technicians. To prevent this misuse users must know about the legal difference between granting authority someone to sign in their own name an obligation for the user and give away their private key. The importance to treat private keys according to their name and leave them only in the private possession of the certified holder of the keypair, should be told by the certification authorities to every new subscriber. Further more the contract between certification authority and certified user should imply a clause to legally bind the user to this behaviour.

Another possibility to prevent this voluntary undermining of authentication is to force the restriction of use only to the certified person with technical methods. Instead of authorising the access

privileges with a password check, the system could also verify the matching of biometric attributes of the user who request access and a reference data set of the certified holder's biometric attributes The verification is accurate only for identical data sets, and access to the private key will be allowed.

Science and research developed methods using different biometric attributes for authentication. They are divided in two basic categories. The physiological based techniques, which measure the physiological characteristics of a person, like fingerprint verification, facial analysis, iris analysis, or handgeometry-vein patterns. The behavioural approach includes all techniques, which are based upon the measurement of the behaviour of a person. Examples for this category are speech analysis, hand-written signature verification, or keystroke analysis. Generally the physiological based technologies have a better ratio between false accept rate and false reject rate meaning that the cognition of the attributes and the allocation to the reference data sets is more accurate than using behavioural approach techniques. However, the social acceptance for behaviour related approaches is higher, because people feel unwell giving away fingerprint data or data about retina to computer systems [Polemi 1997].

This leads to another possibility to categorise the different techniques distinguishing between the method used to store the templates, which content the biometric reference data of the authorised users. It can be stored in the device performing the biometric verification or in a database on a server to which the device is connected. The first group is divided in devices, which are permanent connected to the network and small devices like personal digital assistants or smart cards, which perform the verification procedure internally and transmit only the result of the process to the network. This last group is in the perspective of data protection the safest product for verification.

Conclusion

Taking into account the different methods to authenticate users under the perspective of the most significant protection of the private key all the aspects mentioned above lead to the conclusion, that the best protection for the system-crucial access to private keys is to store them on a smart card with internal biometric authentication features. The key is always in the immediate possession of the certified owner, who is the only person authorised to use it. Further he cannot give away his key voluntarily, because the smart card verifies his identity before access is granted. Finally his biometric data is well protected against misuse by third parties , because it is stored only on the smart card, which is absolutely in his own sphere of control.

If the compliance of the elements building a public key infrastructure with this criteria for verification of the identity is assured and the certification authorities also comply with other satisfactory security standards, the security provided by the public key infrastructure reaches the same grade as security provided by hand-written signatures set under paper-based messages. Provided that the users get familiarised with the use of digital signatures and electronic messages, the legal solutions to the new technologies described in this paper by the presumptions granted by UNCITRAL's Draft Rules and the rules given in the Proposal of a European Signature Directive are reasonable, adequate and promoting for the usage of digital signed electronic documents with legally binding statements.

References

[ABA 1996] Michael Baum (Editorial Committee Chair); Digital Signature Guidelines; American Bar Association 1996

[COM(98)297] COM/98/0297; Proposal for a European Parliament and Council Directive on a common framework for electronic signatures; 1998 – in the release of Working Document No 3, 25 January 1999; text established by the secretariat of the European Council after the meeting of the working group on 21. January 1999

[COM(98)586] COM/98/0586; Proposal for a European Parliament and Council Directive on certain legal aspects of Electronic Commerce; 1998

[Pohl 1997] Hartmut Pohl; Guidelines for the Use of Names and Keys in a Global TTP Infrastructure, Report for the European Commission, DG XIII, Essen Germany 1997

[Polemi 1997] Despina Polemi; Biometric Techniques: Review and Evaluation of Biometric Techniques for Identification and Authentication, Including an Appraisal of the Areas where they are most Applicable; Report for the European Commission, DG XIII; 1997

[Pordesch 1993] Ulrich Pordesch, Alexander Roßnagel, Michael J. Schneider; Erprobung sicherheits- und datenschutzrelevanter Informationstechniken mit Simulationsstudien (Testing Information Techniques relating to Data Security and Data Protection with Simulations); in: Datenschutz und Datensicherheit; Braunschweig, Germany; Vieweg; September 1993

[Remotti 1997] Luca Remotti; Legal and Regulatory Issues for the European Trusted Services Infrastructure – ETS; Report for the European Commission; DG XIII; Rome 1997

[Rhein 1997] Paul Rhein; Digitale Signatur mittels Smart Cards (Digital Signatures using Smart Cards); Master Thesis, Technical University of Vienna; 1997

[Rihaczek 1995] Karl Rihaczek; Schriftform – Elektronische Form (Written Form – Electronic Form); in: Datenschutz und Datensicherheit Fachbeiträge: Digitale Signaturen und sicherheitssensitive Anwendungen; Braunschweig, Germany; Vieweg 1995

[SigG 1997] German Digital Signature Act; BGBl. I p. 1870; 1997

[Smeddinghof 1996] Thomas J. Smedinghoff (Editor); Online Law, The SPA's Legal Guide to Doing Business on the Internet; Addison-Wesley Developer Press; Reading Massachusetts 1996

[Stallings 1995] William Stallings; Security on the Data Highways; Prentice Hall 1995

[UNCITRAL 1996] United Nations Commission on International Trade Law, Working Group on Electronic Commerce; Model Law on Electronic Commerce with Guide to Enactment; General Assembly Resolution 51/162 of 16. December 1996; New York 1997

[UNCITRAL 1998] United Nations Commission on International Trade Law, Working Group on Electronic Commerce; Draft Uniform Rules on Electronic Signatures; A/CN.9/WG.IV/WP.73

[Wright 1996] Benjamin Wright; The Law of Electronic Commerce – EDI, E-Mail, and Internet: Technology, Proof, and Liability; Little, Brown and Company 1996