Legal Framework of Electronic Signatures in the European Union and Germany

Jens M. Nödler

February 20, 2006

Seminar in Network Security
Institute of Computer Science
Georg-August-Universität Göttingen

Contents

Chapter 1

Introduction

E-Commerce is booming. The business volume has risen dramatically in the past few years. The law has adapted itself to the circumstances of the Internet and nowadays it is possible to execute online declarations of intent and to conclude contracts. Nevertheless only electronic banking is used and acts of sale are concluded online.

More challenging transactions like public administration, tax assessments or notarial certificates are mostly done offline, because the infrastructure of the Internet cannot ensure the integrity and authenticity of data and the identity of users. A solution for these problems are electronic signatures which are legally recognized as handwritten signatures.

This thesis briefly introduces the technical background of electronic signatures like hash algorithms, asymmetrical cryptography and public key infrastructures. The main focus is set to the legal framework of electronic signatures in the European Union (directive 1999/93/EC) and Germany ("Signaturgesetz", SigG), requirements of electronic signatures, their legal recognition and use cases for electronic signatures related to computer science.

Chapter 2

Technical background of electronic signatures

This chapter briefly introduces the technical background of electronic signatures like hash algorithms, asymmetrical cryptography and public key infrastructures. To begin with, the basic principles of hash algorithms to ensure data integrity are outlined. Afterwards, asymmetrical cryptography as a subset of the cryptology is introduced. It can be used for encrypting, decrypting and signing data. Finally, two methods that allow to assert the authenticity and identity of users—public key infrastructure and Web of Trust—are presented.

2.1 Integrity: Hash algorithms

A hash algorithm maps an input (hash message) to a fixed output that is called the hash key, hash value or message digest. The hash key is generated by a mathematical algorithm so that it is extremely unlikely, that some other input will produce the same key. It should be almost unlikely or impossible to compute the input from the hash key [4, Chapter 6.4, Hashing].

An example for a weak hash algorithm is the cross total of a number, because the hash key is not of a fixed size and collisions are likely. E.g. the inputs 12345 and 555 would result in the same hash key 15.

The requirements for secure hash algorithms are:

1. Uniqueness: The same input must always lead to the same hash key.
2. Preimage resistant / One way character: If you know the hash key it should be hard to find the original message.

3. Second preimage resistant: Given a message m_1 it should be hard to find another message m_2 such that $\text{hash}(m_1) = \text{hash}(m_2)$.

4. Collision-resistant: It should be hard to find two different messages m_1, m_2 such that $\text{hash}(m_1) = \text{hash}(m_2)$.

5. Randomness: Even if two inputs differs only a little bit the resulting hash keys should differ clearly.

Well known and often used hash algorithms are the Message Digest Algorithm (MD2, MD4, MD5) and the Secure Hash Algorithm (SHA-0, SHA-1, SHA-224, SHA-256, SHA-384, SHA-512) families. The MD algorithms (128 bit hash keys) were developed by Ronald L. Rivest in 1989 (MD2) and advanced until 1991 (MD5), because MD2 and MD4 proved to be weak hash algorithms. Until 2004 MD5 was classified as secure, but then first attacks against MD5 were published and in 2005 researchers generated two different files with identical MD5 hash keys but entirely different but meaningful content.[1] Nowadays it is strongly recommended not to use the currently known variants of Message Digest Algorithms any longer.

The Secure Hash Algorithms (160 bit hash keys) were developed by the American National Institute of Standards and Technology (NIST) and the American National Security Agency (NSA) and published in 1994 (SHA-0) and in 1995 (SHA-1) respectively. In 2005 a series of attacks against SHA-0 and SHA-1 were published by Chinese cryptographers which made it possible to find collisions in 2^{39} (SHA-0) or 2^{63} (SHA-1) calculations instead of a brute force attack (2^{80} calculations).[2] As a result of these attacks SHA-0 and SHA-1 should not be used any longer[3] but be replaced by their successors (SHA-224, SHA-256, SHA-384, SHA-512) which were published in 2002 by the NIST and which are currently considered secure.[4]

There are a few other hash algorithms which are currently considered secure, like RIPEMD-160[5], Tiger[6] and Whirlpool[7].

[1] http://www.cits.rub.de/MD5Collisions/

[2] http://www.schneier.com/blog/archives/2005/02/cryptanalysis_o.html
http://www.schneier.com/blog/archives/2005/08/new_cryptanalyt.html
http://www.infosec.sdu.edu.cn/people/wangxiaoyun.htm

[3] Recommendation of the German BSI ("Bundesamt für Sicherheit in der Informationstechnik") http://www.bsi.de/esig/basics/techbas/krypto/

[4] http://csrc.nist.gov/publications/fips/fips180-2/fips180-2withchangenotice.pdf

[5] http://homes.esat.kuleuven.be/ bosselae/ripemd160.html

[6] http://www.cs.technion.ac.il/ biham/Reports/Tiger/

[7] http://paginas.terra.com.br/informatica/paulobarreto/WhirlpoolPage.html

2.2 Authenticity of data: asymmetrical cryptography

Asymmetrical cryptography—a synonym for public key cryptography—allows users or systems to communicate securely without having prior access to a shared secret key, by using a pair of cryptographic keys.

Each user or system owns a set of two keys (a private and a public key), where the public key is available to every other user or system and the private key is kept secret. Data is encrypted with the receivers public key and can only be decrypted with the corresponding private key.

Asymmetrical cryptography offer these possibilities:

- Encryption and decryption of data.
- Electronic signatures: The private key is used for signing data and the electronic signature can be verified using the corresponding public key.
- Key agreement: Negotiation of a shared secret key for symmetrical cryptography, because symmetrical cryptography is much faster than asymmetrical cryptography.

Asymmetrical cryptography is used for electronic signatures to ensure the authenticity of data: At the sender's side, a hash key is generated from the data, which is encrypted using the private key. This procedure ensures, that the signature is authentic, and—because of the fixed size of the hash key—small. At the receiver's side, the signed data of the electronic signature is decrypted with the sender's corresponding public key, and the hash key is compared with a self computed hash key of the data. If both hash keys are equal, the integrity and authenticity of the data is given, because the signature could have been created only by the corresponding private key (authenticity of data) and every change at the signed data would lead to a different hash key (integrity of data).

Most asymmetrical cryptography algorithms use the underlying mathematical problem of factorization a number into two very large prime numbers and the inverse task of multiplying the two prime numbers. The mathematical background is omitted, because it is not the core topic of this thesis. Well known and often used asymmetrical cryptography algorithms are RSA[8] and ElGamal [5, Chapter 8].

[8] http://www.di-mgt.com.au/rsa_alg.html

2.3 Authenticity of users: PKI and Web of Trust

Hash algorithms can ensure the integrity of data and asymmetrical cryptography can be used to verify the authenticity of data, but both cannot offer the authenticity of persons and their identities.

Two different approaches to verify the authenticity and identity of persons need to be distinguished:

1. Public key infrastructures (hierarchical structure) and
2. Webs of Trust (flat structure).

Public key infrastructures (PKI) are trusted third parties, that provide services which are capable of identifying persons. This is mostly done by issuing certificates, which associate the certificates (public and private keys) with the owner's identity. If somebody wants to identity a person, the corresponding public key (or it's hash key) is send to the PKI and the associated identity is provided, if the public key is known by this PKI. Every user needs to trust the PKI and cannot verify the authenticity of the provided informations, because the users authenticate themselves only once against the PKI.

The second approach is called Web of Trust and it uses a flat structure of trusted relationships between its users. If two persons (here X and Y) want to trust each other, they need to authenticate themselves by checking their identities. Then both sign the other person's public key and publish these keys to a server, so that everybody can see, that X and Y trust each other. If Y repeats this procedure with person Z, X and Z can also trust each other, because both trust Y—hence a Web of Trust originates.

2.4 Security concerns of electronic signatures

Beside the technical (hash algorithms and asymmetrical cryptography) and organizational (authentication of persons, administration of a PKI) background, other important security concerns of electronic signatures should shortly be mentioned.

1. The used hash algorithms, asymmetrical cryptography algorithms and protocols might become compromised someday. The infrastructure must be designed for reissuing certificates and the use of new algorithms and protocols to provide seamless services.
2. The user's private key must be protected from unauthorized access. It should not be stored as a regular file, but on a external media like

a Smartcard and should also be protected by a special token (like a password or biometric identification).

3. The process of signing data must ensure that no foreign or hidden data is signed. This affects the coding standards of data (like ASCII or Unicode) and their textual representation (some characters might not be displayed correctly) and also the use of binary files, which could include meta data and invisible data [2].

4. Due to the proliferation of viruses, backdoors and rootkits the fulfillment of the last two requirements is a challenging task.

Chapter 3

Legal framework of electronic signatures

The first law dealing with electronic signatures came into force in Germany in 1997 ("Signaturgesetz", SigG 1997) as part of a series of information and communication laws ("Informations- und Kommunikationsdienste-Gesetz", IuKDG). The SigG 1997 was the precursor for a directive of the European Community (EC) to consort the laws of electronic signatures in the Member States of the European Union (EU)[1].

3.1 Directive of the EC on electronic signatures

Directives are templates that must be implemented in the local laws of the Member States of the EU whilst keeping within a given deadline. A directive shall be binding, as to the result, that is to be achieved, upon each Member State to which it is addressed, but shall leave the choice of form and methods to the national authorities.[2] The contents of the directive 1999/93/EC of the European Parliament and of the Council of 13th December 1999 on a Community framework for electronic signatures were orientated at the German SigG 1997. The primary intentions of the directive are:

- Increase of the use of electronic signatures by establishing an equivalence in the legal recognition of electronic signatures and handwritten signatures,

[1] Where the European Union is the superstructure of the European Community.

[2] Article 249, Consolidated Version of the Treaty Establishing the European Community

- Removal of barriers to the use of electronic communications and electronic commerce through convergent laws for data authentication with electronic signatures,

- Promotion of the interoperability of electronic-signature products,

- Enhance competitiveness of the transborder certification-service-providers,

- Setting of the requirements for secure signature-creation devices to ensure the functionality of advanced electronic signatures,

- Allowing the use of electronic signatures as evidences in legal proceedings,

- Establish a legal framework not only for the issuing and management of certificates, but also businesses, such as registration services, timestamping services, directory services, computing services or consultancy services related to electronic signatures.

The directive consists of 28 paragraphs describing their intentions ("Erwägungsgründe"), 19 articles with definitions and directives and an annex, that lists special requirements for qualified certificates, certification-service-providers and secure signature-creation devices. Article 2 defines basic terms:

1. "electronic signature" means data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication;

2. "advanced electronic signature" means an electronic signature which meets the following requirements:

   (a) it is uniquely linked to the signatory;
   (b) it is capable of identifying the signatory;
   (c) it is created using means that the signatory can maintain under his sole control; and
   (d) it is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable;

3. "certificate" means an electronic attestation which links signature-verification data to a person and confirms the identity of that person;

4. "qualified certificate" means a certificate which is provided by a certification-service-provider and meets these requirements as listed in annex I:

   (a) an indication that the certificate is issued as a qualified certificate;
   (b) the identification of the certification-service-provider and the State in which it is established;
   (c) the name of the signatory or a pseudonym, which shall be identified as such;
   (d) provision for a specific attribute of the signatory to be included if relevant, depending on the purpose for which the certificate is intended;
   (e) signature-verification data which correspond to signature-creation data under the control of the signatory;
   (f) an indication of the beginning and end of the period of validity of the certificate;
   (g) the identity code of the certificate;
   (h) the advanced electronic signature of the certification-service-provider issuing it;
   (i) limitations on the scope of use of the certificate, if applicable; and
   (j) limits on the value of transactions for which the certificate can be used, if applicable.

5. ”signatory” means a person who holds a signature-creation device and acts either on his own behalf or on behalf of the natural or legal person or entity he represents;

6. ”signature-creation data” means unique data, such as codes or private cryptographic keys, which are used by the signatory to create an electronic signature;

7. ”certification-service-provider” means an entity or a legal or natural person who issues certificates or provides other services related to electronic signatures. To act as a provider for qualified certificates the following requirements according to annex II must be fulfilled (incomplete list):

   (a) demonstrate the reliability necessary for providing certification services;
   (b) ensure the operation of a prompt and secure directory and a secure and immediate revocation service;
   (c) ensure that the date and time when a certificate is issued or revoked can be determined precisely;
   (d) verify, by appropriate means in accordance with national law, the identity and, if applicable, any specific attributes of the person to which a qualified certificate is issued;

(e) employ personnel who possess the expert knowledge, experience, and qualifications necessary for the services provided, in particular competence at managerial level, expertise in electronic signature technology and familiarity with proper security procedures; they must also apply administrative and management procedures which are adequate and correspond to recognized standards;

(f) use trustworthy systems and products which are protected against modification and ensure the technical and cryptographic security of the process supported by them;

(g) take measures against forgery of certificates, and, in cases where the certification-service-provider generates signature-creation data, guarantee confidentiality during the process of generating such data;

(h) maintain sufficient financial resources to operate in conformity with the requirements laid down in the Directive, in particular to bear the risk of liability for damages, for example, by obtaining appropriate insurance;

(i) not store or copy signature-creation data of the person to whom the certification-service-provider provided key management services; and

(j) use trustworthy systems to store certificates in a verifiable form so that only authorized persons can make entries and changes, information can be checked for authenticity, certificates are publicly available for retrieval in only those cases for which the certificate-holder's consent has been obtained, and any technical changes compromising these security requirements are apparent to the operator.

In contrast to the SigG 1997—where the accreditation of certification-service-providers through a governmental organization was mandatory—it is now voluntary according to article 3 para. 2 directive 1999/93/EC and only *may* be introduced or maintained by the Members States. Instead, a new service provider placed into service only needs to inform the appropriate authority.

Article 5 deals with the legal consequences of electronic signatures. Member States shall ensure, that advanced electronic signatures which are based on a qualified certificate and which are created by a secure-signature-creation device:

1. satisfy the legal requirements of a signature in relation to data in electronic form in the same manner as a handwritten signature satisfies those requirements in relation to paper-based data; and

2. are admissible as evidence in legal proceedings.

The following articles adjust the liability of certification-service-providers, international aspects like the validity of a qualified certificate in all other Members States, considerations of data protection and the time limit (19 July 2001) to bring the law into force.

3.2 German laws and electronic signatures

From 1997 to 2001 electronic signatures were officially called "digital signatures" ("digitale Signatur", SigG 1997) in Germany. This was changed to "electronic signatures" in 2001 by the SigG 2001 which was an implementation of the directive 1999/93/EC as discussed above. Since the directive adopted many ideas of the SigG 1997 one of the most noticeable changes was the abolishment of the duty of accreditation of certification-service-providers.

The current revision of the SigG dates from the year 2005 and is unofficially called SigG 2005.[3] It experienced only little changes compared to the SigG 2001.[4] The SigG contains the common and abstract rules for electronic signatures and is completed by the signature regulation ("Signaturverordnung", SigV) which deals with technical details. The algorithms to use for hashing and asymmetrical cryptography are part of neither the SigG nor the SigV. They are regularly published by the responsible agency ("Bundesnetzagentur", formerly known as "Regulierungsbehörde für Telekommunikation und Post") in their Official Journal and these algorithms should be secure for the next six years. The last publication originates from 2005 and refers to the SHA-family of hash algorithms and to the RSA and DSA algorithms for asymmetrical cryptography.[5] The latest draft for the year 2006 stills refers to SHA-1 (among others) as a secure hash algorithm, even though it should not be longer used.[6]

The SigG is structured like the directive 1999/93/EC and consists of 25 paragraphs, the most important of which are: § 1 SigG defines the aim and coverage, § 2 contains the definitions of article 2 of the directive as seen

[3] Gesetz über Rahmenbedingungen für elektronische Signaturen, 16. Mai 2001, Zuletzt geändert durch Art. 3 Abs. 9 G v. 7.7.2005 I 1970

[4] Erstes Gesetz zur Änderung des Signaturgesetzes, (1. SigÄndG)

[5] Bekanntmachung zur elektronischen Signatur nach dem Signaturgesetz und der Signaturverordnung, Vom 2. Januar 2005, Geeignete Algorithmen zur Erfüllung der Anforderungen nach §17 Abs. 1 bis 3 SigG vom 22. Mai 2001 in Verbindung mit Anlage 1 Abschnitt I Nr. 2 SigV vom 22. November 2001, veröffentlicht unter: http://www.bundesnetzagentur.de/media/archive/1507.pdf

[6] http://www.bsi.de/esig/basics/techbas/krypto/algo_entw1_06.pdf

above, § 4 sets the requirements for certification-service-providers, § 5 adjusts the release of certificates, § 7 lists requirements for qualified certificates, § 8 regulates the barring of certificates, § 9 regulates qualified time-stamps, § 11 adjusts the liability of certification-service-providers, § 15 deals with the voluntary accreditation of certification-service-provider, § 17 lists requirements for products for qualified electronic signatures and § 23 adjusts the status of foreign electronic signatures.

The SigG introduces and regulates qualified time-stamps (§ 9 SigG) which are not covered by the directive. A qualified time-stamp allows to validate the point in time when a document was signed. With the combination of qualified time-stamps and qualified electronic signatures it is possible to answer the three main questions of digital documents: Who signed it? (authenticity); Is the data valid? (integrity); When was it signed? (time-stamp).

The SigG and SigV define the organizational and technical framework of electronic signatures but not their legal recognition. The recognitions are regulated in distributed specific laws like the private law (”Bürgerliches Gesetzbuch”, BGB), civil code of law (”Zivilprozessordnung”, ZPO) and cadaster order (”Grundbuchordnung”). These and other laws were changed to provide the legal recognition of the electronic format and electronic signatures by the *formality adaptation law.*[7]

The most important changes are located in the BGB and ZPO. Paragraph 3 was added to § 126 BGB to permit the substitution of the written form by the electronic form if nothing else is defined. § 126a para. 1 BGB was added and defines, that the electronic form as a substitute for the written form needs to be signed with a qualified electronic signature according to the SigG, and that the signing person needs to add his name. § 126a para. 2 BGB defines, that a contract in electronic form must be signed by both parties. § 126b BGB introduced the text form, which is an analog or digital declaration, that must be permanently reproducible and the signing person must be named. The text form does not need to be signed with a qualified signature in contrast to the electronic form.

§ 292a ZPO was added and defines the prima facie evidence (”Anscheinsbeweis”, ”Beweis des ersten Anscheins”) for qualified electronic signatures. A prima facie evidence is an alleviation of evidence in cases of common events. The prima facie evidence of a document in the electronic form—that is signed according to the SigG—means that it is seen as authentic until a fact upsets this prima facie evidence. If—for example—person Y gets a signed document from person X the document is treated as authentic because of the prima facie evidence. If person X denies this, then he is the party with

[7] Gesetz zur Anpassung der Formvorschriften des Privatrechts und anderer Vorschriften an den modernen Rechtsgeschäftsverkehr, Stand 18.7.2001, BGBl 2001 I, S. 1542

the burden of proof and needs to prove that he did not sign the document (e.g. because the underlying qualified certificate was stolen). This regulation empowers qualified electronic signatures for the use in court for evidence.

3.3 Advanced electronic signatures

An advanced electronic signature according to § 2 number 2 SigG is an electronic signature which meets the following requirements:

1. It is uniquely linked to the signatory;
2. it is capable of identifying the signatory;
3. it is created using means that the signatory can maintain under his sole control; and
4. it is linked to the data to which it relates in such a manner, that any subsequent change of the data is detectable.

Roßnagel investigated in an article the legal framework and possible use cases for advanced electronic signature [8]. The main objection is the lack of legal recognition of advanced electronic signatures, because advanced electronic signatures are only defined by the directive and the SigG to define more ambitious ways of signing. Even if a method of signing would fulfill the above requirements, the use would not lead to special legal consequences. Hence the application of advanced electronic signatures is not further described, even though common standards like PGP would be classified as advanced electronic signatures [2].

3.4 Qualified electronic signatures (QES)

The directive is in part not very logically structured: It defines the terms ”electronic signature” and ”advanced electronic signature” in article 2. But only advanced electronic signatures

1. which are based on a qualified certificate and
2. which are created by a secure-signature-creation device

satisfy the legal requirements of a signature in the same manner as a handwritten signature and are admissible as evidence in legal proceedings (article 5). The SigG clarifies this by naming signatures that fulfill these requirements ”qualified electronic signatures” (QES). They are defined in § 2 number 3 SigG on top of the definitions of ”electronic signatures” and ”advanced electronic signatures”.

To sign a document with a QES the signatory must own a qualified certificate, a secure-signature-creation device and a special token (like a password or biometric identification) which unlocks the certificate (§ 15 para. 1 SigV). The signatory itself must be natural person or must act on behalf of the natural or legal person or entity he represents. A secure-signature-creation device must protect the qualified certificate from unauthorized access (§§ 2 number 10, 17 para. 1 SigG), must display the data which will be signed and must give some kind of alert before finally signing the data (§ 17 para. 2 SigG). These strict rules should prevent abuse like the signing of foreign data.

3.5 QES in automated processes

The term of automated processes describe processes which are carried out automatically by a system. This, for example could be the shipment of digital bills via e-mail or a website where customers can get juridical relevant documents. Electronic signatures can be used to sign these documents automatically, so that the receiver and third persons may verify the origin and authenticity of those documents.

But neither the directive nor the SigG mentioned something related to the use of electronic signatures in automated processes. The use of electronic signatures is only interesting from an economic point of view, if the process of signing can be automated—instead of hand signatures. The facility to use QES in automated processes was raised by Roßnagel [8] and the main questions are:

1. Are QES only a substitute for handwritten signatures?
   To give the answer directly: No, because the directive itself ”should not be limited to issuing and management of certificates”[8] and the fact that electronic signatures are regarded as legally equivalent to handwritten signatures does not mean that electronic signatures are a substitute for handwritten signatures. Electronic signatures might be used for tasks where no handwritten signature is necessary at all.

2. Must the process of signing be initiated separately for each document?
   For signing a document with a QES, one needs to enter the token (password) to unlock the certificate. Must this be done separately for each document? No, it's up to the signatory, how many documents he

[8] Directive 1999/93/EC, intention 9

is going to sign. But the signatory must assign the statements of the signed data to itself, because he initiated the process of signing, and a third person must be able to trust the signature and in those who signed the data.

3. Is the process of automated signing equivalent to the requirements of the SigG?
   This question must be posed, because the signatory must be a natural person according to the SigG. But already the reasoning of the SigG 1997 proposed that this must be the case, because the process of signing must be initiated by a natural person at some given point in time.

Finally it is possible to use QES in automated processes. It is important to know, that the owner of the qualified certificate that is used for the signing must assign all statements to itself. It must be ensured in the automated process that no foreign data is signed because the signatory would be responsible therefor.

3.6 QES for software agents and web services

Electronic signatures are regarded as legally equivalent to handwritten signatures of natural or legal persons. They are not *designed* for communication between electronic systems like software agents or web services. It is possible—as seen above—to use QES in automated processes nevertheless. Might electronic signatures also be used between software agents and web services under some circumstances?

For automated processes Roßnagel pointed out that statements made by a computer system are assigned to the system's operator, if the use of the system is the operator's will and if the operator is willing to assign the statements to itself [8]. This should also be possible for operators of software agents and web services. They must ensure with juristic, technical and organizational precaution that no foreign data is signed, because foreign statements would also be assigned to the operator and it might be impossible to prove, that the data was signed by fault due to the regulations of § 292a ZPO (prima facie evidence).

In concluding, it should be possible to use QES for software agents and web services as long as the operator is willing to assign the system's statements to itself. The conditions equal those for the use of QES in automated processes, but the operator needs to pay attention to the consequences of signing documents, especially if they contain declarations of intent ("Willenserklärung"). The risk of abuse might be reduced by adding limitations of the scope to the qualified certificate according to § 7 para. 1 no. 7 SigG.

Chapter 4

Conclusion and outlook

The legal framework permits the use of qualified electronic signatures coequal to handwritten signatures for many use cases by establishing an equivalence in the legal recognition of both kinds of signatures. Due to the complexity of the use and administration of qualified electronic signatures, they are still not widely used. Many potential users don't see any advantages for themselves and are not willing to pay for the qualified certificate and secure-signature-creation device.

On the other hand this complexity is the price to pay for legally recognized electronic signatures. There is also no choice for the users, because the qualified electronic signature is the only standard, that is legally coequal to handwritten signatures.

The future of the electronic signature depends on indirect developments like a possible integration in the electronic card of the health care system[1] ("elektronische Gesundheitskarte") or extended legally obligated formality of the use of qualified electronic signatures.

[1] http://www.dimdi.de/static/de/ehealth/karte/basisinformation/gesetzrahmen/

Bibliography

[1] aus der Fünten, Jörg: *Die Haftung der Zertifizierungsstellen nach dem Signaturgesetz,* Münster 2000

[2] Gassen, Dominik: *Digitale Signaturen in der Praxis,* Köln 2003

[3] Jungermann, Sebastian: *Der Beweiswert elektronischer Signaturen: eine Studie zur Verläßlichkeit elektronischer Signaturen und zu den Voraussetzungen und Rechtsfolgen des § 292a ZPO,* Frankfurt am Main 2002

[4] Knuth, Donald E.: *The Art of Computer Programming: Volume 3, Sorting and Searching* Second Edition, Addison-Wesley 1998

[5] Menezes, Alfred J., van Oorschot, Paul C. and Vanstone, Scott A.: *Handbook of Applied Cryptography,* CRC Press, Fifth Printing, 2001, http://www.cacr.math.uwaterloo.ca/hac/

[6] Palandt, Otto: *Bürgerliches Gesetzbuch,* München 2005

[7] Roßnagel, Alexander: *Die fortgeschrittene elektronische Signatur,* MMR 2003, 164 - 170

[8] Roßnagel, Alexander und Fischer-Dieskau, Stefanie: *Automatisiert erzeugte elektronische Signaturen,* MMR 2004, 133 - 139

[9] Spindler, Gerald und Schmitz, Peter und Geis, Ivo: *Teledienstegesetz, Teledienstedatenschutzgesetz, Signaturgesetz: Kommentar,* München 2004

All URLs used in this thesis were downloaded last at 2006-01-23. If a URL is no longer available a copy of the document can be requested via email to *jens@noedler.de.*