Approaches of Digital Signature Legislation

Thomas F. Rebel, Olaf Darge, Wolfgang Koenig

Johann Wolfgang Goethe University of Frankfurt
Mertonstr. 17, 60054 Frankfurt a.M.
Germany
e-mail: {rebel, darge, koenig} @wiwi.uni-frankfurt.de

Abstract. This paper introduces three basic approaches of digital signature legislation. The overall aim of these approaches is to establish a framework for trust and security in open networks. As nowadays distributed working and distributed businesses widely depend upon open netwoks, such frameworks can be understand as an enabler for the development of electronic commerce. The framework for the use of digital signatures and the framework for the corresponding "trust infrastructure" according to the German Digital Signature Act is described in depth as an example for an accomplished legislative effort.

1. The Need for Trust and Security

Open networks such as the Internet are increasingly being used as a platform for communication in our society. Open and accessible, they allow rapid and efficient world-wide exchanges at a low cost. This will lead to new forms of business configurations (e.g. "virtual" enterprises, work collaboration across the globe), of private communication (e.g. e-mail) and of organisation of public services (e.g. electronic tax declaration) [1].

One of the major obstructions in this development is the lack of trust in open networks. However, in order to own a probative document one has to print it out and sign it by hand. This legally forced breach of media should be stopped as soon as possible. [2]

As long as the risks are as high as at present[1], suppliers and consumers will, in order to reduce the risk, restrict electronic transactions in open networks to low-value transactions. The Internet must be secure and reliable, otherwise users are unlikely to use the Internet on a regular basis for commerce.

Nowadays, integrity and authenticity can be guaranteed by digital signatures. However, public key systems (which are generally used for digital signatures) require a secure technical and organisational infrastructure to establish trust in the use of encryption for a reliable application of open networks used for the above mentioned purposes.

---

[1] As examples for the risks in open networks read [3] on "sniffing" and [4] on "spoofing".

Why is an infrastructure needed to make digital signatures useful? Henning introduces the "four pillars" of secure electronic commerce [5]: 1. authentication: the sender of a document must be identified precisely and without possibilities of falsification; 2. confidentiality: the contents of a message cannot be scanned by unauthorized parties; 3. integrity: changes made in messages without according remarks must not be possible; 4. non-repudiation: The sender of a message is directly connected to the contents of the message. We do not want to emphasise the confidentiality of communication in this paper. Instead, we concentrate on "pillar" 1, 3 and 4.

2. Cryptographic Applications

The following three measures comply to these four requirements. The use of cryptography for:

- encryption, the use of cryptography for
- digital signatures, and a
- trusted certification authority.

Basically, cryptographic applications can be subdivided into the following categories: hash algorithms, symmetric algorithms, and asymmetric algorithms.[2]

A digital signature is the encrypted hash value of a file, where a private key is used to encrypt it. The receiver of the file can decrypt this cipher text with the corresponding public key and verify the hash value. Verification is done by calculating the hash value and comparing it with the received and decrypted value in the signature. The document´s integrity is proved if both values are the same.

The public key of the sender can e.g. be looked up in an online directory. But this does not prove that the sender of the message is really the owner of the public key. There are some scenarios in which fraud is possible, e.g. the directories can be faked.

The problem of authenticity and the problem of non-repudiation can be solved by a certificate which connects the public key to the identity of a person. Such a certificate contains at least the public key of the holder, the holder´s identity (name or pseudonym), and the digital signature of the issuer of the certificate (the certification authority). One of the most known standards for these certificates is the X.509 standard [6]. Certificate standards determine what information is stored in a certificate.

There are three basic models of how certificates can be issued: a. by another user, b. by a certification authority of a private certification hierarchy, or c. by a certification authority of a public certification hierarchy. These models for certification of the affiliation of a public key with a person are referred to as "trust infrastructures" (also known as "public key infrastructures"), because the users trust in the issuer of a certificate.

Model a. is called the "web of trust". We will not dicuss this model, because it is not relevant for the digital signature legislation.

---

[2] [7] gives a very broad overview of cryptographic applications.

Trust infrastructures of type b. and c. are based on a concept of hierarchy. In this case, certificates are only issued by a certification authority. Certification authorities take the role of a trusted third party for a relationship between two parties who do not know each other. The certification authority issues certificates (each containing the identity and a public key) to both parties, so that each user can be sure about the identity of another user. The trust in the certification authority is determined by their policy of certification. This policy must be known to the users, i.e. the customers of the authority.

Basically, there are two ways to create a certification hierarchy. The hierarchy can be the responsibility of a company or some other non-public institution (we refer to this a private certification hierarchy), or the hierarchy is based on an act or some other kind of public regulation (we refer to this as a public certification hierarchy). This does not determine who issues certificates, but predicts who establishes the rules and techniques according to which a certification authority adduces its business (the certification policy). In a private hierarchy each authority works according to its own policy. In a public hierarchy the authorities have to match the requirements established by an act.

In this paper we introduce trust infrastructures according to model c.

3. Approaches of Digital Signature Legislation

Presently different national and international approaches of legislation on digital signatures exist. While some countries are just establishing task forces to study the use of digital or electronic signatures, others are providing guidelines or have already enacted regulations on the use of digital or electronic signatures.[3]

The main purposes of these laws (or the current draft versions) are almost similar:

- Facilitate commerce and economic development by means of reliable electronic messages,
- minimise the incidence of forged electronic signatures and fraud in electronic commerce, and consequently
- enhance the public's confidence in electronic commerce and electronic signatures.[4]

---

[3] For an overview of the worldwide activities in this area see [8].

[4] It should be noted, that there is not alaways a clear distinction between the terms "electronic signature" and "digital signature". Usually, "electronic signature" is a more general term. A definition can be found under the signature-enabling approach in this chapter. A "digital signature" therefore is a subset of an electronic signature, using public key cryptography. For a definition of a digital signature, please refer to chapter 5. Confusion is created by the improper use of the two terms. While laws following the prescriptive approach described later in this chapter use the term "digital signature", several statutes address digital signatures while meaning the more general term "electronic signature"[9]. Only five of the US federal states with a technology-neutral approach define both terms.

All laws are intended to remove existing barriers rather than create new obstacles. However, there is only little concensus on how to approach the subject. Following a survey of the Internet Law & Policy Forum [10], three major approaches can be identified: Prescriptive approach, Criteria-based approach, and Signature-enabling approach. The following sections will briefly introduce these approaches.

3.1 Prescriptive approach

The prescriptive approach consists of a detailed framework and regulations relating to the security infrastructure. Public key infrastructure serves as the technical baseline. The Utah Digital Signature Act has an outrider position among prescriptive approaches. Utah was the first legal system in the world to adopt a comprehensive statute enabling electronic commerce through digital signatures [11].

The Utah Digital Signature Act consists of five parts: Part I describes purposes and construction of the law and defines key terms. Part II deals with the licensing and regulation of certification authorities. Part III determines duties of the contracting parties, while Part IV is dedicated to the effect of a digital signature. Part V deals with repositories.

The following central issues can be identified to distinguish the prescriptive approach from other approaches:

- Public key infrastructure is the underlying technology with certification authorities playing a major role
- Processes for licensing, subscribing, ensuring a signature, revocation or expiration of a certificate can be deduced from the act
- Existence of requirements for the licensing of Certification Authorities
- Regulations on cross-border recognition of certificates

Utah adopted the Digital Signature Act on February 27, 1995. It went into effect on May 1, 1995. Further amendments to the Act became effective in 1996. On November 1, 1997, Administrative Rules became effective and by November 19, 1997, the Utah Departement of Commerce has commemorated the world's first license or accreditation of a certification authority by a state law.[5]

The prescriptive approach addresses public key infrastructure as the fundamental technology to put digital signature into practice. Many legal systems felt the danger of an over-regulation by establishing a too detailed framework. New technologies might be impaired and hindered in their development. Although the use of a public key infrastructure is voluntary, rules and regulations providing security and trustworthiness mainly apply only to digital signatures created by the use of asymmetric cryptography. To provide more flexibility and trust in future technologies, many states have decided to choose a technology-neutral approach by addressing electronic authentication more broadly, using the criteria-based or the signature-enabling approach.

---

[5] Governor Leavitt proclaims November 19, 1997 as Digital Signature Signing Day by a digitally signed declaration.[12]

3.2 Criteria-based approach

The predominant model for this approach is the California Government Code, § 16.5 [13]. Despite having a limited applicability (to communication with public entities), it has been followed by several states, including states creating laws with a general applicability. It was the first state to establish five requirements under which a digital signature shall have the same force and effect as the use of a manual signature[6]:

- It is unique to the person using it.
- It is capable of verification.
- It is under the sole control of the person using it.
- It is linked to data in such manner that if the data are changed, the digital signature is invalidated.
- It conforms to regulations adopted by the Secretary of State.

The Government Code addresses the Secretary of State to adopt regulations. These regulations are available in the final draft version [14]. They provide a "list of acceptable technologies":

- Public Key Infrastructure, and
- Signature Dynamics[7]

3.3 Signature-enabling approach

The third approach is the signature-enabling approach. According to this approach, any mark with the intent to authenticate is an electronic signature. In this context, the notion "electronic signature" is used, representing a genus of the term "digital signature".

The Massachusetts Electronic Records and Signatures Act [15] states that "a signature may not be denied legal effect, validity or enforceability solely because it is in the form of an electronic signature. If a rule of law requires a signature, or provides consequences in the absence of a signature, an electronic signature satisfies that rule of law."[15] In this case electronic signature means "any identifier or authentication technique attached or logically associated with an electronic record that is intended by the person using it to have the same force and effect as a manual signature." Regarding this, a digital signature based on public key infrastructure is included as one possible authentication technique.

The idea of this approach is to adjust existing law to the requirements of electronic commerce. Therefore the meaning of signature as well as other key terms like "writing", "original" or "record" are extended to include electronic records and signatures. The Model Law of the United Nations Commission on International Trade Law (UNCITRAL), designed to harmonise and unificate international law, takes the

---

[6] Under this act, the term "digital signature" has the meaning of an electronic signature as described above [9]

[7] Signature Dynamics means measuring the way a person writes his or her signature by hand on a flat surface and binding the measurements to a message through the use of cryptographic techniques. [14]

same approach, referring to it as a "functional-equivalent" approach. It is based on an analysis of the purposes and functions of the traditional paper-based requirement with a view to determining how those purposes or functions could be fulfilled through electronic-commerce techniques.

4. The German Digital Signature Act

4.1 The Process of Legislation

The following sections describe the the German Digital Signature Act as the first national legislation on digital signatures. This act conforms to the prescriptive approach described in the above section.

The German Bundestag passed the Information and Communication Services Act (IuKDG) in June 1997. The act came into effect in August 1997. The act governs such areas as the responsibility of providers, area-specific data protection and digital signatures. The law is limited to the statement of essential facts which require immediate regulation in order to define the legal framework necessary for the economic development of electronic commerce. Any existing legal uncertainty will thus be eliminated. In addition, public interests, for example concerning minors and consumer protection, will be safeguarded [16]. It does not govern any regulations on encryption.

Article 3 of the IuKDG is the Act on Digital Signatures. Its basic purpose "is to establish general conditions under which digital signatures are deemed secure and forgeries of digital signatures or manipulation of signed data can be reliably ascertained" [17].

The act describes the framework for the procedures of issuing and using digital signatures. Hence, it allows for other procedures of using digital signatures, which will not belong to the scope of validity of this act and therefore cannot be enforced on account of this act.

The act itself does not determine special technical and organisational procedures or components. It is specified by an Ordinance on Digital Signature [18] and a catalogue of measures.

The Ordinance on Digital Signature was enacted by the German government in October and came into effect on November 1st, 1997. The ordinance contains implementing statutes for the realisation of the act. It does not specify technical standards or operational procedures and thus leaves room for innovative solutions and competition between the private certification authorities.

The technical standards and operational processes of certification authorities are specified in the catalogue of measures [19]. The Bundesamt für Post und Telekommunikation[8] (BAPT) publishes this catalogue as a "useful assistance for the

---

[8] Federal Bureau of Postal Services and Telecomunication

realisation" of the act and the ordinance. This catalogue contains suggestions on how a certification authority can meet the requirements of the act regarding security and services. Therefore, the catalogue serves as a basis for the approval of certification authorities and the regular review process. The aim is to quicken the process of establishing and reviewing certification authorities according to the Digital Signature Act.

The catalogue has been available since November 18, 1997 as a draft version. It is proposed to come into effect by the end of January 1998. The BAPT periodically updates the catalogue and adjusts it in accordance to the technical progress.

4.2 The Certification Hierarchy

Before we describe the procedures and organisational structure of the certifier according to the act, we illustrate the basic concept of the trust infrastructure.

The Digital Signature Act defines the following basic concepts:

A digital signature is 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 or the authority according to §3 (Competent Authority) of this Act."[17]

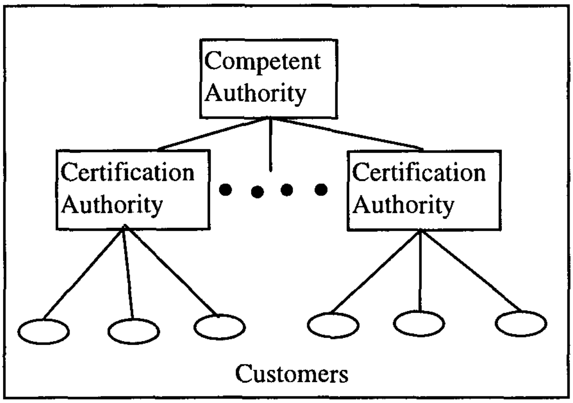
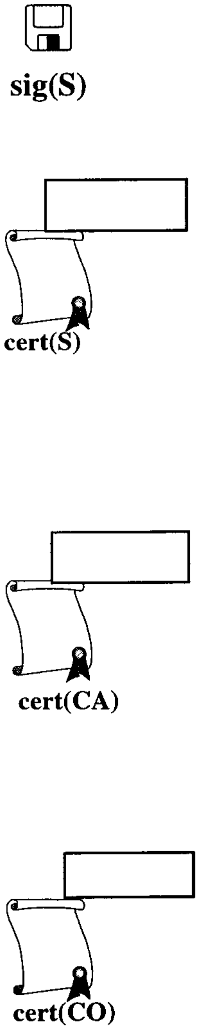


Fig. 1. A two layer certification hierarchy with a Competent Authority as the root certifier

A certification authority refers to "a natural or legal person who certifies the assignment of public signature keys to natural persons and to this end holds a licence pursuant to § 4 (Licencing of Certification Authorities) of this Act."[17]

These two definitions determine a *two layer certification hierarchy* (see figure 1) with a Competent Authority as the root certifier.



Document with the digital signature of the sender: sig(S)

First step: review sig(S)

1. Is sig(S) mathematically correct?
2. Is cert(S) valid?

Certificate of the sender: **cert(S)**
Contains: **validity period**, and digital signature of the certification
authority **sig(CA)**

Second step: review validation of cert(S)

1. Is sig(CA) mathematically correct?
2. Was the document signed before the end of the validity period of cert(S)
3. Is cert(CA) valid?

Certificate of the certification authority **cert(CA)**
Contains: **validity period**, and digital signature of the competent authority **sig(CO)**

Third step: review validation of cert(CA)

1. Is sig(CO) mathematically correct?
2. Was cert(s) signed before the end of the validity period of cert(CA)?
3. Is cert(CO) valid?

Certificate of the competent authority **cert(CO)**
Contains: **validity period**, and digital signature of the competent authority **sig(CO)**

Fourth step: review of validation of cert(CO)

1. Is sig(CO) on cert(CO) mathematically correct?
2. Was cert(ca) signed before the end of the vailidity period of cert(CO)?

Fig. 2. The review path in a certification hierarchy

The "competent authority" is a public authority, which is now the BAPT. Its purpose is to issue certificates used for signing certificates, to licence certification authorities, and to monitor those authorities for compliance with the act. The

Competent Authority is not allowed to issue certificates to customers and the certification authorities are not allowed to certify other certification authorities.

How can the validity of a digital signature be proved in this type of infrastructure? The digital signature of a document is valid, if it is mathematically correct and if the certificate of the sender was valid at the time of signing. But when is a certificate valid? The certificate of a sender is valid, if the signature was placed during the validation period of the certificate (usually 5 years), the certificate contains a mathematically correct digital signature of a certification authority, and this authority has attained a valid certificate from the root certification authority (the Competent Authority). In the next step, the validity of the certification authority´s certificate must be examined. The certificate of a certification authority is valid if the original document was signed during the validation period of the certification authority´s certificate, the digital signature of the Competent Authority at the certification authority´s certificate was mathematically correct, and the certificate of the Competent Authority was valid at the time of the issue of the certification authority´s certificate. Finally, the Competent Authoritiy´s certificate is valid if the digital signature on the certification authority´s certificate had been placed during the validation period of the Competent Authority´s certificate, and the digital signature of this authority on its own certificate is mathematically correct [20]. Figure 2 shows this process.

4.3 The Competent Authority

As we have seen above, the root of the certification hierarchy is the Competent Authority (the BAPT). The Competent Authority has two basic responsibilities: a. it signs the certificates of the certification authorities (so it is the certification authority of certification authorities); b. it has to take the fact into consideration that the certification infrastructure is secure and trustworthy (so the BAPT act for the public interest in a reliable certification policy, see chapt. 3). In this section, we describe the regulations that concern responsibility b. The activities for issuing certificates will be described in the subsequent section.

User´s trust in the use of digital signatures is largely determined by the quality and security of certification authorities [19]. The trustworthiness of these certification authorities depends on different factors, e.g. trust in the organisation of the authority, quality of techniques and processes, the usage of accepted standards, accordance with the laws, a valid contract between authority and user (customer) etc.

Therefore, the signature act determines that every certification authority must be licenced by the competent authority (§ 2 SigG (2); [17]).

The organisational security concept, the technical components, and the quality of the authority´s staff are the subjects of a scruting process foregoing the licencing.

According to the catalogue of measures, [19] the scruting process must be completed before the certification authority applies for the licence. The Competent Authority reviews the application of the certification authority based on the scruting result. If the security concept, the technical components, and the staff of the applying authority meet the requirements of the act and the catalogue of measures, the Competent Authority has to licence the applicant and issue him a digital certificate with the digital signature of the Competent Authority.

After the certification authority has started its business, the three subjects of the scruting process will be reviewed periodically, e.g. the organisational concept and the technical components will be reviewed every two years. In case of changes made to the relevant three subjects by the certification authority, the changes will be subject to a review and an approval.

4.4 The Certification Authority

Once a certification authority is licenced it has to offer five specific services: key creation services, registration services, certifcation servives, individualisation services, directory services, and time stamp services.

We explain these services according to the process of applying for a certificate. In the subsequent section we only discuss certificates for users. As we have seen above, certification authorities are only allowed to issue certificates to users and not to other certification authorities.

Assume a person, Mr. Jones, needs a certificate. A firm, Smith Inc., is a licenced certification authority according to the German Digital Signature Act. First Mr. Jones must use the registration service of Smith Inc. (see Figure 4). The *registration service* has to identify Mr. Jones with his passport unless Mr. Jones is already the owner of a certificate. In this case, he can be identified by his digital signature. We assume that Mr. Jones does not have a certificate or a pair of keys.[9] After Mr. Jones is identified, the registration service creates a unique name for Mr. Jones. The name can be his own name, e.g. "tjones", or a pseudonym, e.g. "MIB1997". The data of Mr. Jones is transferred to the certification service.

Subsequently the *key creation service* creates a pair of keys. One private key, which is handed out to Mr. Jones, and one public key which is stored in a directory. The private key is transferred in a high security channel to the individualisation service. The public key is transferred to the certification service and is deleted from the key creation service.

In the next step, the *certification service,* after having received Mr. Jones´s data and the public key, creates a certificate that contains the following information [17, article 3, § 7 (1)]:

1. **Name of the owner** of the signature key, to which additional information must be appended in the event of possible confusion, or a distinctive pseudonym assigned to the owner of the signature key, clearly marked as such,
2. **public signature key** assigned,

---

[9] According to the signature act it is possible to ask for a certificate using a self created pair of keys. Some people would prefer this, but the certification authority must inspect wether the keys have been generated by a secure system, i.e. that the keys meet the requirements of the catalogue of measures.

3. names of the **algorithms** with which the public key of the owner of the signature key and the public key of the certification authority can be used,
4. **serial number** of the certificate,
5. beginning and end of the **validity period** of the certificate,
6. name of the **certification authority**, and
7. an indication as to whether use of the signature key is **restricted** in type or scope to specific applications.

If Mr. Jones wishes to, other parameters can be included in the certificate as well, e.g. rights of disposal. The certificate is sent to the individualisation service.

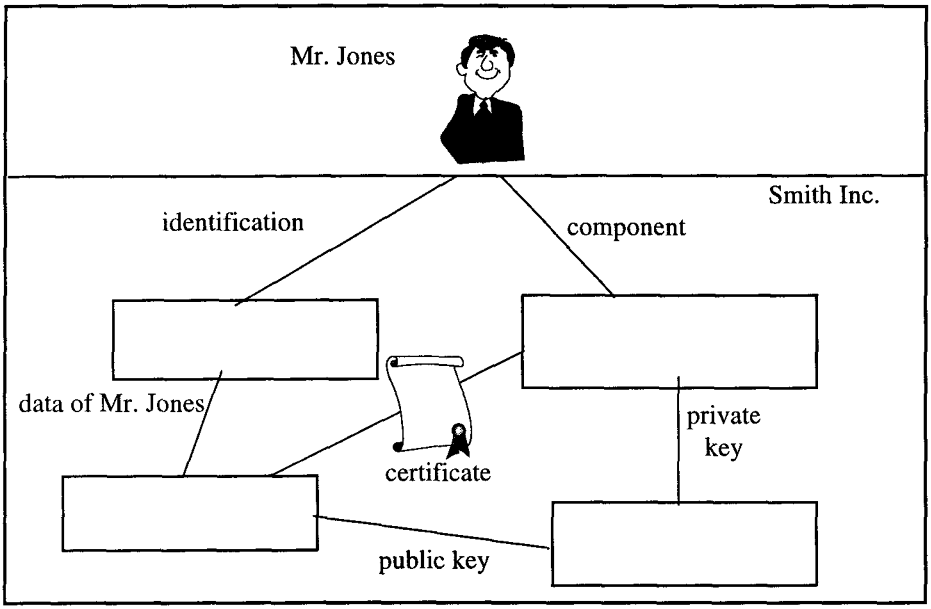


Fig. 3. The services of a certification authority: application for a certificate

The *individualisation service* recieves the private key of Mr. Jones from the key generation service. The private key must be stored on a "signature component", e.g. a smart card, and deleted from all the certification authority's databases. After the private key is stored on the signature component, the component is "locked" with an authentification technique, e.g. a PIN number or a biometric technique, such as a fingerprint. This authentification technique protects the private key of unauthorised use. The individualisation service signs the component with the private key of the certification authority.

The signature component is then transferred to the registration service, where Mr. Jones is waiting for it. The component contains Mr. Jones's certificate, Mr. Jones's public key, Smith Inc.'s public key, and the public key of the competent authority.

Mr. Jones is now able to use his component to sign all kinds of data by putting it in a reader in his computer, identify himself by PIN or a fingerprint, and activating the "sign"-function of his signature tool. The "sign"-function will perform the process we described in chapter 3.

The *directory service* stores all certificates of a certification authority and allows online access for reviewing the validity of a certificate. The process of evaluating the validity of a signature was described above. Therefore, the corresponding certificates in the directory service must be reviewed. How many of the steps of reviewing one wants to take depends upon one´s security needs. At least the first step, reviewing of the correctness of a business partner´s certificate, must be applied. The most important part of the directory service is the revocation list. This list stores all invalid certificates. Reasons of invalidity could be expiry of validity, disclosure of the key, loss of the signature component.

Time is an important factor in business and in certification. As we have seen in the chapter on the review of the validity of certificates, the date of signing is significant. The date on a contract is important in business, or the date on which a user acts, e.g. transfers time-critical data. Therefore, certification authorities offer a *time stamp service*. In order to use this service, a user must "hash" a file and transfer the hash value to the time stamp service. The service adds the time he recieved the hash value to this hash value and signs this pair of information with his own key. He therefore proves having seen this hash value (which stands for a certain unique file) at this time.

The output of the described process is a public key certificate. According to the act a user can also own an attribute certificate. These certificates may contain information on his affiliation to a certain group, or a specific professional qualification. The process of receiving such a certificate is the same as for key certificates, except, that the user does not have to prove his identity but an attribute, e.g. by a testimonial.

4.5 Certificates Issued by Other Countries

The Digital Signature Act, the Ordinance, and the catalogue of measures contain only very few statements on the point of acceptance of certificates issued in other countries. The act determines that all certificates "shall be deemed equivalent to digital signatures under this Act, insofar as they show the same level of security" [17]. Which certificates will meet the requirement will probably be subject to bilateral negotiations between governments.

5. Conclusion

We have introduced different basic approaches for digital signature legislation. The German Sigital Digital Signature Act was introduced in depth as a example of the presvriptive approach, because it is the first national law on this subject. One of the most important goals for future research to establish trust and security in electronic commerce is to review the applications and services running according to this act and create solutions for the problems arising in the markets, the courtrooms and the laboratories.

The overall aim of academic and business activities in this field has to be the reduction of the problems, especially the unsecurity, of distributed working in open networks. Efficient and easy to use tools that match the requirements of the the legislation have to be developed to serve as an enabler for the development of electronic commerce.

References

1. Wigand, Rolf/Picot, Arnold/Reichwald, Ralf: Information, Organization and Management : expanding markets and corporate boundaries, 1997.
2. Rieß, Joachim: Digitale Signaturen, in: Datenschutz und Datensicherheit 21 (1997) 5.
3. Bellovin, R.: Security problems in the TCP/IP protocol suite, in: Computer Communications Review, 19(2):32-48, April 1989.
4. Bellovin, R./Cheswick, W.: Firewalls and Internet Security, 1994.
5. Henning, Peter: Wie sicher ist "Sicher"?, in: bank und markt, December 1997.
6. CCITT: Recommendations X.509: The Directory - Authentification Framework, 1988.
7. Schneier, Bruce: Angewandte Kryptographie, 1996.
8. Summary of Electronic Commerce and Digital Signature Legislation, http://www.mbc.com/ds_sum.html.
9. Smedinghoff, Thomas J.: Analyzing State Digital Signature Legislation (1997), http:www.mbc.com/ds_rev.html.
10. Didari, Albert/Morgan, John/Coie, Perkins: Survey of Electronic and Digital Signature Legislative Initiatives in the United States, prepared for the Internet Law and Policy Forum, September 199, (http://www.ilpf.org/digsig/digrep.htm).
11. Wims, Michael D.: History and Current Status of the Utah Act, http://www.commerce.state.ut.us/web/ commerce/digsig/dsintro.htm
12. http://www.governor.state.ut.us/html/digital_signatures.htm
13. California Government Code ° 16.5, 1997, http://www.ss.ca.gov/digsig/code165.htm.
14. California Secretary of State: Final Draft of California Digital Signature Regulations, November 18, 1997 (http:// www.ss.ca.gov/digsig/finalregs.htm).
15. Commonwealth of Massachusetts: Massachusetts Electronic Records and Signatures Act, Draft, November 4, 1997 (http://www.magnet.state.ma.us/ itd/legal/mersa.htm).
16. n.a.: Das Informations- und Kommunikationsdienste-Gesetz (IuKDG) - Kurz-darstellung, June 1997, http://http://www.bmbf.de/archive/magazin/mag97/kw25/informat.htm.
17. Digital Signature Act, Article 3 of the Information and Communication Services Act, Bonn 1997, http://www.iid.de/rahmen/iukdgebt.html
18. Verordnung zur digitalen Signatur, in der Fassung des Beschlusses der Bundesregierung, October 1997.
19. BAPT ed.: Massnahmenkatalog fuer digitale Signaturen (Entwurf), 1997.
20. Kent, S.: Privacy Enhancement for Internet Electronic Mail: Part II: Certificate-Based Key Management, RFC 1422, BBN, February 1993.