GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials (Security 401)"
at http://www.giac.org/registration/gsec

Electronic signatures: How European Legislation meets the public

Introduction

Abstract

This paper introduces European and national legislation regarding electronic signatures and sheds light on the technical implications and current state of the art.

In 1997, the EU Directive on electronic signatures became effective. The Directive provides a common framework for all EU member states which was to be implemented in national law until 2001. It defines a terminology and contains rules for Certification Service Providers regarding market access, conditions of liability, and required security precautions. It stipulates the legal equivalence of electronic signatures. It requires security standards on the user's side and makes conditions on the content of the certificates which the electronic signatures are based on.

The German Signatures Act of 2001 and the accompanying Ordinance are discussed in detail. It is described why one must have an online connection to the CSP while signing, why signature creation has to take place on a specialized computer (such as a SmartCard), and how an attack against a legally valid electronic signature can be performed.

The tasks and publications of the competent authority are provided.

To link theory with practice, the current state of implementation is depicted in the application areas online banking, communication with authorities, and business relationships. Lacking standardization is identified as the main cause for the generally low acceptance.

The recently founded "Alliance for electronic signatures" is considered, and the author expresses his opinion why certification services should be a public task.

Author's note

I wrote this for technical people who want to understand the legal aspects of electronic signatures in the European Community. The reader should be familiar with the technical aspects of electronic signatures – terms like public and private key, signing and verifying an electronic signature should not make you sweat.[1]

I am a technical person and sometimes found it hard to understand the legal texts; I assume many of you make similar experiences digging into the legal stuff.

Since this paper deals mainly with legal texts and articles, language plays an elevated role. I have put some effort into trying to make the legal texts understandable for technical people while reflecting them as accurately as possible.

Where German texts formed the basis English translations were used where possible. However, the original German texts are available in the list of references.

Terminology

The EU Directive and the German Signatures Act will be discussed into detail. Working through the two legal texts it is remarkable that terms are defined right at the beginning of the texts. Terms are not chosen identically in the two documents, so let's put the terms abreast:

[1] For an introduction to electronic signat ures, see „Electronic Signatures" or comparable documentation.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Term according to EU Directive[2]	Term according to Signatures Act[3]	Term used in this paper
electronic signature	electronic signature	electronic signature
advanced electronic signature	advanced electronic signature	advanced electronic signature
(not available)	qualified electronic signature	qualified electronic signature
signatory	signature-code owner	signatory
signature-creation data	signature code	private key
signature-creation device	(not available)	signature-creation device
secure-signature-creation device	secure signature-creation device	secure signature-creation device
signature-verification data	signature test code	public key
signature-verification device	signature-application component	signature-verification device
(not available)	signature-application component	signature-application component
certificate	certificate	certificate
qualified certificate	qualified certificate	qualified certificate
certification-service-provider	certification-service-provider	Certification Service Provider (CSP)
electronic-signature-product	technical components for certification services	CSP components
(not available)	products for qualified electronic signatures	products for qualified electronic signatures
(not available)	qualified time stamps	qualified time stamps
voluntary accreditation	voluntary accreditation	voluntary accreditation

Table 1: Terminology

To avoid confusion, the terms in the third column of this table are used in the sequel of this paper.

Juxtaposition of the terminologies

Let's look at what the terms defined above mean; if not declared otherwise, the Directive and the Signatures Act mean the same thing by the same term.

- An "electronic signature" is a chunk of electronic data associated with other electronic data (i.e. the document to be signed) and which can be used for authentication. There is no statement on security or on the signatory.
- An "advanced electronic signature" is an electronic signature which
  - is uniquely assigned to the signatory,
  - identifies the signatory and the signed data uniquely,
  - is created using means under the signatory's sole control,

  AND
  - makes any subsequent change of the signed data evident.
- A "qualified electronic signature" only occurs in the Signatures Act. It is an advanced electronic signature which additionally

[2] „EU Directive", p. 13/14
[3] „Signatures Act", p. 3-4

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

➢ is based on a qualified certificate (of the signatory) which is valid at the time of signing[4]
AND
➢ has been created using a secure signature-creation device.

- In EU talk, a "signatory" is a person possessing a signature-creation device; however, in German law, a signatory is a person possessing a private key and whom an according public key has been assigned in a qualified certificate.
- A "private key" is data used to create an electronic signature.
- A "public key" is data used for verifying an electronic signature.
- A „signature-creation device" is mentioned in the EU Directive only as hardware and software that implements the private key.
- A „secure signature-creation device" is hardware and software that stores the private key and uses it for the creation of electronic signatures. Directive and Signatures Act agree that the device must assure that the private key is stored in a unique instance and cannot be downloaded or derived from the device.
- A „signature-verification device" is hardware and software used to verify an electronic signature.
- The German law defines a „signature-application component" as all hardware and software used for signature services at the signatory's side, i.e. a „signature-application component" is a signature-verification device or hardware and software that assigns data to the signature-creation device.
  For instance, this can be an application that creates a hash value from a document and sends it to the signature-creation device – possibly a SmartCard.
- A „certificate" is electronic data that links the public key to a person and confirms her identity.
- A „qualified certificate" is a certificate for a natural person that contain at least the set of attributes as stated further down in the Directive (annex 1) or the Signatures Act (section 7), respectively. These sets of attributes are identical except that the Signatures Act requires the cryptographic algorithms employed.
  Qualified certificates can only be issued by a CSP that fulfills with the requirements laid down in the Directive or the Signatures Act.
- A „CSP" (certification service provider) is a natural or legal person that issues certificates. Further requirements are laid down in the body of the legal texts.
- The term „qualified timestamp" only occurs in the Signatures Act as a piece of electronic data which confirms that other electronic data has been present at a given and specified time. However, qualified timestamps do not play a significant role.
- „CSP components" is software and hardware that is used by CSP's to deliver their services: Creating private keys and securely transferring them to the secure signature-creation device, server infrastructure to publish the public keys and qualified certificates, and generating qualified timestamps (the latter applies only to German law).
- „Products for qualified electronic signatures" occur only in the Signatures Act and are the union of secure signature-creation devices, signature-verification devices, and CSP components.
- „Voluntary accreditation" is a certification procedure for CSP's that set out specific rights and obligations.

[4] see also „Discussion of the German Signatures Act"

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

European legislation - The European Directive

The legal process for EU-wide electronic signatures made its first big step 16 April 1997 when the European Commission presented a „Communication on a European Initiative in Electronic Commerce“[5]. The Commission aimed primarily at facilitating and promoting electronic communication and commerce by the propagation of electronic signatures.

On 16 June 1998, the European “Commission submitted a proposal for a Directive on a common framework for electronic signatures to the European Council”[6]. The proposal was presented in the European Parliament in January 1999. After the presentation, the proposal was revised to improve readability and security and take greater account of technical developments and national interests. The resulting document was adopted by the Council as a „Common Position“ on 28 June 1999. It contains the text which was adopted by the European Parliament as the EU Directive.

In a leading section, the EU Directive states that an EU-wide legal harmonization of electronic signature is necessary to facilitate electronic communication and commerce. It aims to „strengthen confidence in, and general acceptance of, the new technologies“[7]. The EU Directive recommends open technical standards, but does not enforce a standardization process or organizations. The Directive does explicitly not harmonize the related services provided by Certification Service Providers or others, but refers to national service providers.

The EU wants to increase the market competitiveness of the European Certification Service Providers by creating a EU-wide internal market with common rules and without borders. Consumers and businesses shall be given means to communicate and trade electronically in a secure manner, „regardless of frontiers“[8]. As an incentive for Certification Service Providers-to-be, the start-up of a Certification Service Provider should not require prior authorization.

The Directive does not interfere with national contract law or other formalities which define the legal effects of hand-written signatures.

The body of the Directive consists of 15 articles and 4 annexes which can be sketched as follows:[9]

1. “Scope” of the Directive is facilitating and legal recognition of electronic signatures. Interference with contract law is explicitly out of scope.
2. “Definitions” explain the terms listed in the previous section.
3. “Market access” sets rules for Certification Service Providers: Start-up shall not require prior authorization. In order to enable higher security standards, voluntary accreditation schemes can be implemented on a national level. A controlling system for CSP’s shall be implemented. The European Commission may define and publish standards for CSP components. Member states may pose extra requirements for publicly used electronic signatures as long as they do not hinder cross-border services.
4. “Internal market principles” force the member states to apply the national laws to the CSP’s in their respective countries. A free market for electronic-signature products and services is stipulated.

[5] „EU Directive“, p. 13/12
[6] „Common Position“, p. 243/44
[7] „EU Directive“, p. 13/12
[8] „EU Directive“, p. 13/12
[9] Note that the wording of legal texts such as the Directive and the Signatures Act is chosen very carefully; summarizing always implies loss of information and detail.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

5. “Legal effects” instruct the member states to equate an advanced electronic signature which was created using a secure signature-creation device (which is basically an qualified electronic signature according to the Signatures Act) with a hand-written signature. Furthermore, the legal validity of an electronic signature may not be denied before court solely because it does not comply with all of the before-mentioned criteria.[10]
6. The „Liability“ demands at the least that a CSP is liable for any damage someone experiences because she relies
   - on the accuracy and authenticity of attributes in certificates issued by the CSP,
   OR
   - that the signatory is the person mentioned on the qualified certificate at the time the certificate was issued,
   OR
   - on the fact that private and public key comply with each other,
   OR
   - on a certificate which has been revoked but the CSP has failed to register the revocation.

   The liability only applies if the CSP has acted negligently. Note that the Directive does not regulate liability of the CSP in case of
   - indiscretion of the private key,
   OR
   - ambiguity of private/public key pairs,
   OR
   - any possible forgery of an electronic signature even if the CSP has acted negligently.

   Furthermore, CSP's must be given the right to include limitations on validity or extent (e.g. an expiration date or the maximum value of a transaction) in the certificate. The CSP is exempt from liability caused by exceeding these limits.
7. „International aspects“ stipulate the conditions under which certificates issued by companies from outside the EU are to be considered legally equivalent. These conditions are:
   - The CSP fulfills the requirements of the Directive and has been accredited in a member state.
   - A recognized[11] CSP within the EU vouches for the foreign CSP.
   - An according agreement between the EU (or at least one member state) exists.
8. „Data protection“ ensures that CSP's conform to the EU rules of data protection regarding personal data and that CSP's collect personal data of a signatory applicant only directly from the applicant (or upon her explicit consent). The personal data may be collected for no other purpose than the certification service.
9. „Committee“ refers to a special committee which may consult the Commission.
10. „Tasks of the committee“ are mainly consultancy of the Commission regarding technical issues such as requirements, criteria, and standards.
11. The „Notification“ article demands that the member states notify the Commission on their national voluntary accreditation schemes, the national bodies carrying through accreditation and supervision, and all accredited CSP's.

[10] This is an interesting point: To deny an electronic signature as evidence before court, the party challenging the electronic signature must deliver evidence that the signature is not authentic.

[11] according to the Directive

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

12. -15. The closing sections „Review“, „Implementation“ „Entry into force“ and „Addressees“ essentially state that all member states shall implement the Directive in national laws until 19 July 2001.

The four annexes following the articles are:

13. Requirements for qualified certificates:
    Qualified certificates must contain
    - name and state of the CSP,
    - name of the signatory or his pseudonym which has to be identified as such,
    - the public key of the signatory,
    - beginning and end of validity,
    - a unique identifier,
    - information that this is a qualified certificate, and
    - the CSP's advanced signature of the certificate

    Beyond that, a qualified certificate may contain:
    - limitations on scope or value and
    - possible extra attributes.
14. Requirements for CSP's:
    CSP's must
    - run a highly available directory
    - not store private keys
    - provide accurate time services for issuing and revocation of certificates
    - employ competent staff
    - use reliable and trustworthy systems and products
    - prepare for forgery
    - have sufficient money to cover possible liability
    - inform applicants about the precise conditions of the business relationship
15. Requirements for secure signature-creation devices:
    A secure signature-creation device must ensure that the private key exists only on the device and cannot be derived from it. Furthermore, the private key must be protected against the use of others.
16. The last annex describes recommendations for signature verification. Note that these are not obligatory. They shall ensure the authenticity of both the signature and the signed data.

National legislation

The German Signatures Act

On 22 July 1997, the German government put its first Signatures Act into force. It was part of the “Law Governing the Framework Conditions for Information and Communication services”[12].

The primary intention of the 1997 Signatures Act was providing secure electronic signatures.[13] It consists of 16 sections on 8 pages and lacks the degree of detail which is provided by the 2001 Signatures Act. The 1997 Signatures Act is not discussed into detail because the 2001 Signatures Act took its place.

[12] „Informations- und Kommunikationsdienste -Gesetz“
[13] „Informations- und Kommunikationsdienste -Gesetz“, p. 9

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

The electronic signature according to the Signatures Act of 1997 was not accepted by the public. According to Peter Mankowski, "only three hundred signatures were registered in entire Germany until October 1999"[14].

The Signatures Act itself consists of 25 sections. An outline of them is:

1. „Purpose and Area of Application" of the law is providing a framework for electronic signatures. The use of electronic signatures is voluntary.
2. In „Definition of Terms", the middle column of the terminology table is described.
3. The „Competent Authority" is identified as the competent authority of section 66 of the Telecommunications Act[15] which is the „Regulatory Authority for Telecommunications and Posts", referred to as „Reg TP" in the sequel.
4. The „General Requirements" for CSP's state that they do not need approval (this eases market access). CSP's must prove reliability and employ experienced and skilled staff. A CSP-to-be must notify the competent authority before it starts business and prove its competence by handing in a security concept.[16]
5. The „Issue of Qualified Certificates" requires the CSP to identify the applicant for a qualified certificate. The applicant must explicitly agree with the publication of his certificate. (This apparently refers to the German Data Protection Act according to which no personal data may be published without consent of the person affected.) Extra attributes may be contained in the certificate; personal data may be included only with consent – Data Protection Act again.
   The CSP must ensure that the private key cannot be stored outside the secure signature-creation device, employ reliable staff and products, and prevent forgery without detection.
   The latter meets the point Bruce Schneier makes in „Secrets and Lies", p. 384:
   > „The digital security industry is in desperate need of perceptual shift. Countermeasures are sold as prophylactics [...]. Business is about taking risks [...]. The credit card industry doesn't need foolproof smart cards; they just need then strong enough to limit attacks so that the detection and response mechanisms can kick in."

   If forgery is detected reliably, the qualified certificates underlying the electronic signatures can be revoked immediately, and no more signatures can be created using this qualified certificate (see the below section „While signing, you must be online" for details on this).
6. The „Information Obligations" of the CSP are to inform the applicant about
   - proper use
   - the fact that re-signing may become necessary since the security of an electronic signature decreases over time
   - the equivalence of an qualified electronic signature with a handwritten signature
7. The „Contents of Qualified Certificates" are
   - name or pseudonym of the signatory,
   - public key,
   - cryptographic algorithms,
   - a unique number,
   - start and end of validity,
   - name and state of the CSP,

[14] „Wie problematisch ist die Identität des Erklärenden bei E -Mails wirklich?", p. 2826
[15] „Telekommunikationsgesetz", p. 29.
[16] The required content of the security concept is specified in the Ordinance.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

- possible limitations on scope or value,
- possible extra attributes,
- information that this is a qualified certificate, and
- the CSP's qualified electronic signature of the whole thing.

8. „Invalidating Qualified Certificates“ describes the fourfold circumstances which lead to immediate, but not backdated, revocation of a qualified certificate:
   - the signatory (or representative) demands revocation,
   - the certificate was originally based on false data,
   - the CSP has ceased operation with no legal successor in place, or
   - the competent authority demands the revocation.

   The revocation time must be supplied.
9. If a CSP offers „Qualified Timestamps“, reliable staff and products must be employed for this purpose.
10. „Documentation“ ensures that the CSP documents its security concept and the issued qualified certificates. The signatory must be allowed access to the documentation concerning him.
11. „Liability“ means that the CSP must compensate damage if
    - the CSP does not meet the requirements of this act or the associated statutory ordinances,

    OR
    - its products for electronic signatures or other technical security fail.
    - Note that the latter does not only apply to the secure signature-creation device but also to the network security of the CSP. This means that the CSP is liable for damage caused by a hacker attack against the CSP's site.
12. The CSP must have sufficient „Cover“ to reimburse possible damage to its customers. Minimum cover is 250,000 EUR.
13. In case of „Cessation of Operation“, the CSP must
    - notify the competent authority immediately or in advance.
    - take care that all qualified certificates are taken over by another CSP or immediately revoked, respectively.
    - hand over its documentation to the successor or to the competent authority, respectively.
14. To ensure „Data Protection“, the CSP may ascertain and use data only for the sake of issuing the qualified certificate without explicit consent of the signatory.
    If the signatory is solely identified by a pseudonym, the CSP may disclose the real identity only to the competent authority and only if the disclosure serves prosecution of crime, avoidance of public risk or defense, intelligence or fiscal activities. Any disclosure must be documented. The signatory must be informed about the disclosure unless this hinders the above stated activities.
15. The section „Voluntary accreditation of Certification-Service Providers“ defines the rules under which a CSP is accredited. The requirements of accreditation are defined in section 24 of the Signatures Act. The accreditation proves the CSP to have a high level of security.
16. The section „Certificates from the Competent Authority“ define the role of the competent authority as the root CSP: The competent authority issues a qualified certificate for each accredited CSP. These qualified certificates must be publicly available at any time.
17. „Products for Electronic Signatures“ declare that qualified electronic signatures require the use of a secure signature-creation device. Such a device must guarantee that the private key

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

- is unique and secret,
- is stored on the device itself, and
- cannot be downloaded from the device.

Furthermore, the secure signature-creation device must be protected against the use of others. According to section 18, the competent authority confirms if a particular device meets these criteria.

The signature-application components on the computer of the signatory must display or clearly indicate the data to be signed before the signature is created.
The products used for signature verification both at the verifier's and the CSP's side must ensure that qualified certificates are secure against forgery and unauthorized download (see section 5 for the conditions of certificate publication).
Furthermore, the products used for creation of qualified timestamps must prevent forgery.
For the criteria for signature verification and timestamps, a declaration of the manufacturer is sufficient.

18. „Recognition of Testing and Confirmation Offices“ means that the competent authority may appoint someone for testing and confirmation, provided that this legal or natural person acts competently and dutifully.
    In practice, the legal person involved is the „Bundesamt für Sicherheit in der Informationstechnik“ (BSI), debis, and TÜVIT.
19. The provided „Supervision Measures“ declare supervision of the Signatures Act as task of the competent authority. To achieve this, the competent authority may
    - take measures against CSP's, in particular prohibition of operation.
    - order revocation of qualified certificates.

    The competent authority must publish any cessation or prohibition of operation.
20. As „Obligatory Cooperation“, a CSP must permit the competent authority[17] access to their premises and insight to any documentation, and provide required information and support.
21. „Fines“ are due if „... a person infringes regulations [...] deliberately or negligently“[18]. The precise conditions are listed in the law. Maximum fine is 50,000 EUR.
22. The section „Costs and Contributions“ regulates that the competent authority may charge the CSP's for the costs caused by its official duties.
23. The section „Foreign Electronic Signatures [...]“ regulates the validity of electronic signatures and related products from foreign countries.
    An electronic signature from another country is legally equivalent to a (German) qualified electronic signature if
    - it is based upon a qualified certificate from within the EU[19] and it complies with the EU Directive

    OR
    - it is based upon a qualified certificate from a third country, meets the requirements of the EU Directive

    AND
        - the CSP meets the requirements of the EU Directive and is accredited in a member state of the EU

        OR

[17] or anyone acting on her behalf
[18] „Signatures Act“, p. 12
[19] or a country which has signed the Treaty on the European Economic Area

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

- a European CSP complying with the EU Directive vouches for the certificate underlying the electronic signature
  OR
- the CSP is recognized under an agreement between the EU and the third country
  OR
- equivalent security can be proven. Responsibility for this proof is defined in the Ordinance.

A product for electronic signatures from a third country is equivalent to a secure signature-creation device if

- a member state states compliance with the EU Directive
  OR
- equivalent security can be proven. Again, the Signatures Act does not assign competence or responsibility.

24.-25. The closing sections „Legal Regulations“ and „Transitional Regulations“ deal with formal aspects.

Additional German regulations: Ordinance and Formanpassungsgesetz

In German legislation, the Signatures Act defines the framework for electronic signatures. The details for the implementation of this law are laid down in the „Ordinance on Electronic Signatures” („Verordnung zur elektronischen Signatur“).

The Ordinance (as it is called in the sequel of this paper) was decreed by the German government in November 2001. It consists of 19 sections and two annexes which describe aspects like notification by CSP's, identification of a signatory applicant, revocation of certificates, and costs for official acts – broken down to a level of detail of hourly rates for executives and secretaries and their use of vehicles.

The following issues of the Ordinance may be of elevated interest for the IT security professional:

- „Content of the security concept“ (section 3):
  The security concept of a CSP must contain (amongst others) a description of technical and organizational security measures, a process description of the certification services, business continuity planning, measures to assess and assure the reliability of the employees, and a risk analysis.
- „Individual security precautions“ of CSP's (section 5):
  Regarding the creation of the private key, the Ordinance stipulates that the creation has to take place either on the secure signature-creation device itself or at the CSP issuing the certificate or at a CSP which complies with the conditions of the Signatures Act regarding the technical security[20]. If the private key is generated on computers at the CSP, the uniqueness and secrecy of the key must be ensured; storage outside the secure signature-creation device must not be possible.
  If access to the secure signature-creation device is secured by passwords or biometric characteristics these data must be secret and must be stored solely on the secure signature-creation device itself.
  Handing over the secure signature-creation device may occur indirectly – i.e. in a parcel sent by mail – if there is an according written agreement between the CSP and the signatory applicant. If this occurs the creation of electronic signatures by a malicious third – i.e. by capturing the parcel, opening it and using the secure signature-creation device – must be prevented. To accomplish this, the CSP must publish the

[20] i.e. section 17 no. 1 of the Signatures Act

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

qualified certificate not before the signatory has confirmed[21] that she has received the secure signature-creation device.

- „Revocation“ (section 8):
  The Ordinance requires a telephone number under which a signatory can revoke his qualified certificate „without delay“ - this is why it must be available 7 x 24 hours. It also stipulates that the identity of the calling person must be ensured. However, the Ordinance does not regulate how this can be achieved – after all the identity of the signatory is in question!
- „Cessation“ (section 10):
  If a CSP gives up his business, the competent authority and all signatories should be informed at least two months in advance. The information must include if there is a successor.
- Validity (section 14):
  A qualified certificate must not be valid longer than five years.
- „Requirements [...] for qualified electronic signatures“ (section 15):
  Remember that qualified electronic signatures can only be created using a secure signature-creation device. The Ordinance stipulates that the use of the secure signature-creation device must be secured by passwords or biometric characteristics. When verifying a signature, it must be possible to determine if the qualified certificate was present and not revoked „at the given time“. The author's interpretation for „the given time“[22] is the time of signing. However, neither the Signatures Act nor the Ordinance clearly state that the electronic signature must contain the time of signing. Thus, it is unclear if the time of signing must be included in the signed document or by a qualified timestamp to provide two-factor authentication.
- „Long-term data security“ (section 17):
  The competent authority publishes an expiration period after which qualified certificates and electronic signatures become insufficiently secure due to the employed cryptographic algorithms or related parameters. In order to keep its legal relevance, electronic data must be re-signed before the expiration date. The new signature shall include any earlier signatures and a qualified timestamp.
- „Assessment of [...] foreign electronic signatures and products“ (section 18):
  Let's assume that a CSP from a country outside the EU wants to start its business with legally equivalent electronic signatures (see also section 24 of the Signatures Act for the precise conditions of this process).
  If there is a European CSP which vouches for the foreign CSP, the European CSP must notify the competent authority before the foreign CSP starts his business. The European CSP must ensure that the services of the foreign CSP comply with the EU Directive. The competent authority publishes the name of the foreign CSP including the vouching European CSP.
  Otherwise, the competent authority has to ascertain that the security of the foreign CSP is equivalent to the rules set out in the Signatures Act.
  The competent authority publishes the qualified certificates of the recognized CSP's.

All the texts in German legislation discussed so far told us the „Hows“ of electronic signatures – they did not make a statement on the legal equivalence of electronic signatures with regard to written signatures. Here we go:

[21] by means of a written or electronic signature
[22] “Ordinance on Electronic Signatures”, p. 13

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

The Civil Code (Bürgerliches Gesetzbuch), section 126 deals with the written form. It defines that „a document must be signed by the maker by his own hand“[23]; contracts require the written signature of both parties on the same document. The Civil Code was adapted by the Formanpassungsgesetz (Form Adaption Act) which was adopted in July 2001. In its first section, the Formanpassungsgesetz extends section 126 of the Civil Code so that „the written form can be replaced by the electronic form if not ensued otherwise from another law.“[24]. So electronic documents can be used as documents and contracts.

And how about authentication? The Formanpassungsgesetz introduces section 126a to the Civil Code. Section 126a[25] stipulates that electronic documents and contracts have to be signed using a qualified signature according to the Signatures Act. In case of a contract, the parties do not have to sign the same document but two identical documents.

This constitutes the legal equivalence of a qualified electronic signature to a written signature.

Discussion of the German legislation regarding electronic signatures

Summary of German legislation

Only a qualified electronic signature is legally equivalent to a written signature. Electronic signatures from other European countries are legally equivalent if they comply with the EU Directive. Electronic signatures of other kind or from other countries can be legally equivalent if it can be proven that the technical security is equivalent to a qualified signature.

A signature of this kind must be created using a secure signature-creation device. The competent authority publishes a list of technical products certified as secure signature-creation devices. Such a device must have the private key stored exclusively on it, and the private key cannot be derived from the device. The secure signature-creation device must be secured by passwords or biometric characteristics.

The CSP publishes the qualified certificates of all signatories containing the public key and the identity of the respective signatory. Publication may not occur before the signatory has confirmed reception of the secure signature-creation device.

At the time of signing, the validity of the qualified certificate must be checked at the CSP.

A secure signature-creation device must be a specialized computer

A secure signature-creation device cannot be a multi-purpose computer such as a PC or a Unix workstation because the operating systems currently available do not prevent the copying of the private key.

Bruce Schneier expresses this in „Secrets and Lies“ on page 265 where he writes about various attacks against a signature-creation device:

> „If Alice [the signatory] is working on a general-purpose computer, I do not believe it can ever be trusted enough to avoid this problem. If Alice is using a small, single-purpose, digital signature computer, then there is hope.“

Taken the insufficient security of general-purpose computers into account, a secure signature-creation device must be a piece of specialized hardware with a well-defined, limited user and programming interface.

It may not be possible to derive the private key from the secure signature-creation device. If the device were merely a storage medium, the key would have to be transferred to the

[23] „BGB § 126 Schriftform“, translatio n by author
[24] „Formanpassungsgesetz“, p. 1542,translati on by author
[25] „BGB § 126a Elektronische Form“

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

computer for signature creation. Thus, the secure signature-creation device must be a computer, and the signature must be created on the device.

This does not mean that the document to be signed must reside on the device; it is sufficient to transfer the hash code of the document to the device, compute the signature on the device and transfer the signature back to the computer.

A possible attack against qualified electronic signatures

The inference that it is sufficient to transmit the hash code to the secure signature-creation device unveils a security weakness in the legal definitions.

The weakness becomes apparent if you think of an attacks against electronic signatures as described in literature:

> „There's an easy implementation in Windows: A malicious macro could simply watch for PGP's „open file" dialog, see what file Alice is about to sign, and copy its own file to that filename, the restore the old file afterward." (Secrets and Lies, p. 264)

In a slightly modified scenario, a possible attack against a qualified signature is:

The attacker – let her be called Eve – has a document she wants to have signed by Alice. Knowing the hash algorithm used by Alice's secure signature-creation device (that's an easy one – the algorithm is published on the web site of the Competent Authority), Eve computes the hash code. The Competent Authority helps Eve even further by publishing the signature-application components used by Alice to compute the hash code on Alice's computer[26]. Note that the legal regulations neither require the hash code to be created on the secure signature-creation device nor impose an elevated security level to the signature-application components. So Eve manipulates the signature-application component on Alice's PC in a way that Eve's faulty hash code is sent to the secure signature-creation device. By encrypting Eve's hash code, Alice actually signs Eve's document. If Eve has done a good job, the malicious code sends the signature – an inconspicuous little chunk of data – to Eve, and restores the original signature-software component to cover over its tracks.

Alice does not even necessarily notice she has been fooled because section 17 of the Signatures Act requires the signature-application component – i.e. the hacked software on Alice's computer – to display the document to be signed. Things would be harder for Eve if legislation would require the document to be displayed or indicated on the secure signature-creation device.

While signing, you must be online

The qualified certificate must be valid at the time of signing. If a qualified certificate is revoked, this must immediately be published by the CSP in his directory. If a secure signature-creation device is stolen, time may be crucial because the thief is likely to misuse the stolen device shortly after the deed. Thus, the validity of a certificate can only be ensured if the CSP's directory server is contacted at the time of signing. This implies that the computer the secure signature-creation device is connected to must be online[27]. Moreover, the CSP must authenticate itself reliably to avoid a fake CSP server.

---

[26] See the section „The Comptetent Authority as an interface between law and technology" on where and how the Authority publishes these information.

[27] By April 2003, all certified products for qualified signatures are based on SmartCards and require a computer running signature-application components. In the future, specialized hand-held devices are imaginable that maintain the online connection to the CSP themselves. Such secure signature-creation devices could do without a computer attached.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

At the time of signing, it must also be ensured that the qualified certificate has not expired. The system clock of the computer the secure signature-creation device is attached to cannot be trusted. So, the device can either ask the CSP's server (whose answer must be reliable, so this communication must be secured by encryption[28]) or must have a tamper-proof clock built in.

Security devices such as SecurID cards[29] have built-in clocks, so this is technically feasible. Without investigating into depth, the author strongly believes that manipulating the built-in clock by exploiting relativistic effects on time by using high-speed aircrafts is technically not feasible.

Effects on key generation

Since the secure signature-creation device is a computer by itself, key generation can take place on it – if the computing resources suffice. In this case, secrecy of the private key can be provided.

What does it mean that it may not be possible to store the private key if key generation takes place on computers of the CSP – as it is stipulated in the Ordinance? If the private key would exist in the memory of the computer, it could be swapped to disk by the memory management of its operating system[30]. Thus, if the Ordinance is construed tightly, the private key may not exist in the memory of the generating computer. The private key would have to be created in parts independently, and the parts would have to be transferred to the secure signature-creation device independently. Finally, the secure signature-creation device assembles the private key from the parts.[31]

Confidentiality of the signatory's real identity

Imagine the case where someone wants to sign documents but does not want to have his real identity revealed. This could be the case for VIPs – the VIP reveals his pseudonym to some confidants and publishes signed documents under his pseudonym. This could also be a criminal who wants to be sure to use up-to-date encryption technology for signing (and also encrypting) information.

If pseudonyms are used instead of the real identity of a signatory, the certificate must indicate that this is a pseudonym. In any case, the CSP must ensure the real identity of the signatory before she issues the secure signature-creation device – and the CSP must ensure the confidentiality of the pseudonym.

The CSP must disclose the real identity of a pseudonym only for the sake of criminal prosecution, securing the public, intelligence or fiscal activities. Disclosure may only occur to the Competent Authority.

The competent authority is the interface between law and technology

Section three of the Signatures Act identifies the “Regulatory Authority for Telecommunications and Posts” (Reg TP, http://www.regtp.de) as the competent authority. As such, it plays the role of the interface between the legal regulations and the technical and procedural implementations. It is the official institution which takes care that real life at the CSP's and the signatories meet the legal regulations.

[28] which includes signed data or the use of qualified timestamps

[29] From RSA Security, see http://www.rsasecurity.com/products/securid/ . Note that SecurID cards are not certified by the Competent Authority.

[30] ... unless the CSP has disabled virtua l memory on the key-generatio n server.

[31] In the scope of this paper, it has not been researched if appropriate key generation mechanisms exist and if CSP's employ suchlike mechanisms.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Technical operation of the Root CSP and publication[32]

Germany's national Root CSP for electronic signatures is operated by the Reg TP and is available under http://www.nrca-ds.de/ . Using this service, certificates can be validated, and public key directories and certificate revocation lists can be downloaded.

The public key of the Reg TP which is also the root key for all certificates issued by all accredited CSP's is available under http://www.regtp.de/en/tech_reg_tele/in_06-02-02-00-00_m/01/index.html.

When testing the services, I was surprised to experience that they all use the HTTP protocol. I would have expected them to use SLL authentication to ensure the integrity of the data transmitted.

Accreditation authority

The Reg TP performs and coordinates the formal process of accreditation of CSP's and publishes the results.

Since the Reg TP is not entitled to have the technical competence to evaluate the applicants itself, it recognizes evaluation bodies for this purpose. The recognized evaluation and certification bodies are published on the Net under http://www.regtp.de/en/tech_reg_tele/in_06-02-02-00-00_m/04/index.html and in the Federal Gazette. These are the Bundesamt für Sicherheit in der Informationstechnik (BSI), debis and TÜV.

For accreditation, the certification body checks the security concept of the CSP which has been handed in according to section 4 of the Signatures Act and section 3 of the Ordinance.

When the accreditation process is successful, the accredited CSP is published in the Internet under http://www.regtp.de/en/tech_reg_tele/start/in_06-02-04-00-00_m/index.html and in the Federal Gazette. Currently[33], there are 15 accredited CSP's (most of them bar associations). The same document contains the list of CSP's which have commenced their operation. Note that only one of the 15 accredited CSP's (namely D-Trust) has officially started business.

The Reg TP also decides whether a CSP loses her accreditation and publishes this using the same means.

Certification of technical products

The Reg TP publishes the technical products which have been certified by the recognized certification body in the Net under http://www.regtp.de/en/tech_reg_tele/start/in_06-02-05-00-00_m/index.html.

On the signatory's side, there are 11 certified secure signature-creation devices (all of them SmartCard based systems), 9 certified card reader systems, and 10 certified signature application components of which 7 are specifically designed for email clients (Microsoft Outlook or Lotus Notes).

On the CSP's side, there are two key generators (in six versions). Both are designed to create the key pairs on the computers of the CSP and to transfer them securely onto the card system. There are 18 certified products for CSP components, namely hardware and software systems for directory and timestamp services.

[32] Reg TP describes its tasks in “RegTP's Tasks“. Note that all statements in this section are valid as of 28 March 2003.

[33] 28 March 2003

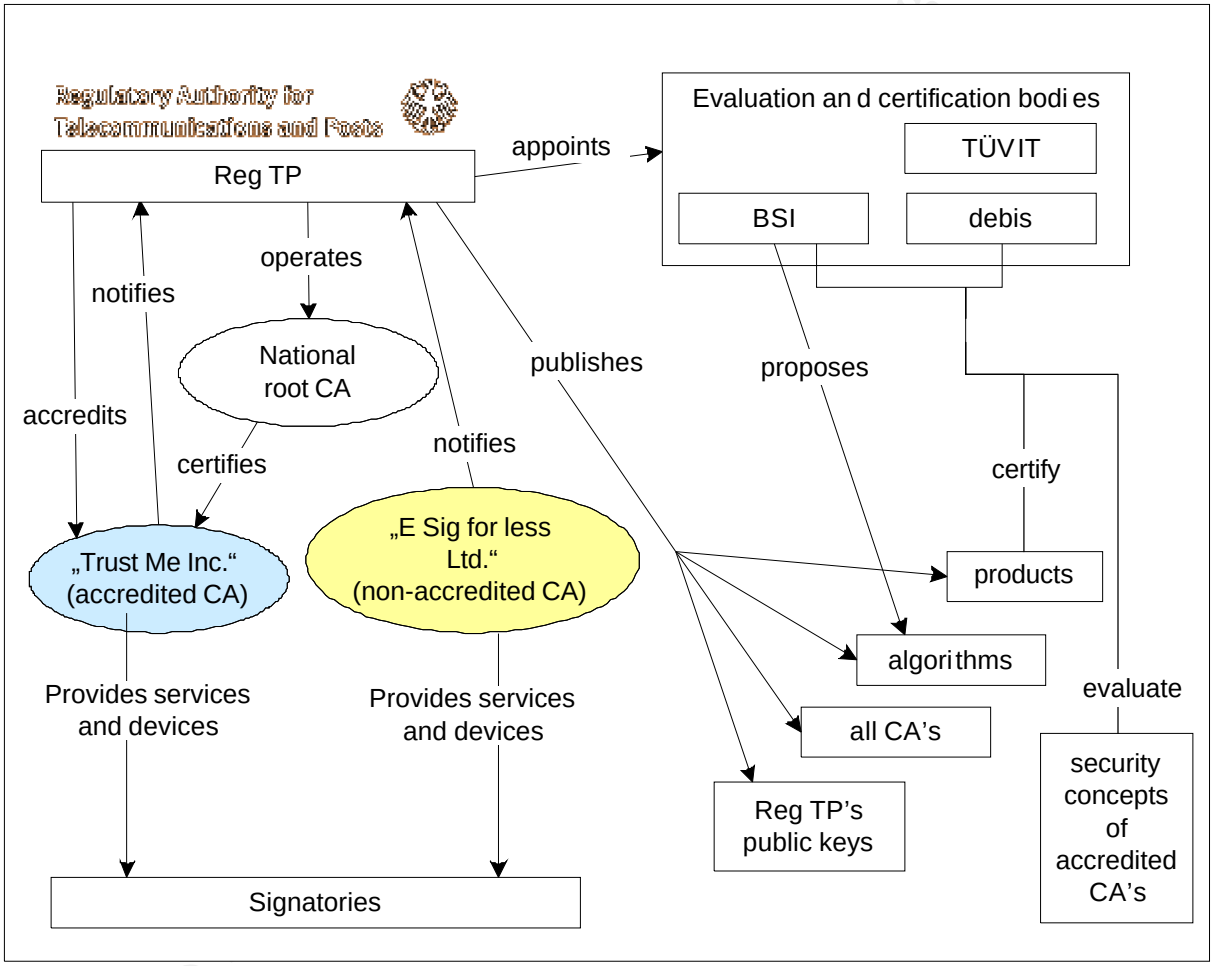
© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Competent Authority - Summary

The competent authority operates the national root CSP, recognizes evaluation and certification bodies, accredits CSP's and publishes the relevant information (its own public keys and issued certificates, name of the evaluation and certification bodies, accredited CSP's, suitable cryptographic algorithms, and certified products).

The qualified certificates issued by accredited CSP's are certified by the national root CSP. They exclusively use equipment which has been certified by the certification bodies mentioned above.

The relationships between the competent authority are illustrated in the following figure which is based on slide 3 of the Reg TP publication „Legal Status of Qualified Electronic Signatures“:



The BSI as the technical consultant

The “Bundesamt für Sicherheit in der Informationstechnik” (BSI[34], http://www.bsi.bund.de) has been founded in 1991 as a federal authority with high technical competence with responsibilities in IT security. The BSI acts as a consultant for the Reg TP.

The BSI determines the suitable cryptographic algorithms annually and sends them to Reg TP where they are published under http://www.regtp.de/en/tech_reg_tele/in_06-02-02-00-00_m/03/index.html.

[34] do not mix up the German BSI with the British Standards Institution

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Legal implementation in other EU member states

Simone van der Hof maintains a website which reflects the current state of legal implementations of electronic signatures in countries all over the world[35].

France[36]

Contrary to the German Government's policy of valuing the individual's data protection, France traditionally preferred a policy which gives more control to the government. Thus, the use of strong encryption was not liberalized before 1996 obstructing the development and propagation of electronic signatures in the mid-nineties.

On 1 April 2001, act nr. 2000-230 which implements the EU directive entered into force. The act was followed by a decree[37] which clarifies details. Further decrees will follow to regulate more details since the level of detail of the act and the first decree is relatively shallow (compared to German legislation).

UK[38]

In 1997, a working group appointed by the Department of Trade and Industry found that the then legislation does not know of an electronic equivalent of a signature. This resulted in a legislative process which produced the "Electronic Communications Act 2000". The act became effective on 25 May 2000. The Electronic Communications Act consists of three parts: "Cryptographic Service Providers", "Facilitation of Electronic Commerce, Data Storage, etc.", and "Miscellaneous and Supplemental".

Electronic signatures are addressed in section 7. The EU Directive from 1999 was implemented by the Electronic Communications Act partially. The full implementation – which has due to 19 June 2001 – occurred on 8 March 2002 by entry into force of the "Electronic Signatures Regulations 2002".

Ordinances which describe the procedures and responsibilities into greater detail are still owing.

Spain[39]

> "In 1999, the Spanish government has passed Royal Decree No. 14 of 17 September 1999 on Digital Signatures, which provides legal effect for digital signatures. [...] In 2000, the order of 21 February 2000 was issued, which complements Royal Decree No. 14 of 17 September 1999 on Digital Signatures by establishing specific rules for the operation of CA's."[40]

Similarly to UK, the Royal Decree and the order implement the EU directive partially. For a full implementation, on 11 July 2002 an according act was adopted.

There are no ordinances which regulate further procedural details and responsibilities.

---

[35] "Digital Signature Law Survey – What's New"

[36] The content of this section is based on Simone van der Hof: "France".

[37] "Décret no 2001-272 du 30 mars 2001 pris pour l'application de l'article 1316 -4 du code civil et relatif à la signature électronique"

[38] The content of this section is based on Simone van der Hof: "UK" and "Electronic Communications Act 2000", and "The Electronic Signatures Regulations 2002".

[39] The content of this section is based on Simone van der Hof: "Spain" and "LEY 34/2002, de 11 de julio, de servicios de la sociedad de la información y de come rcio electrónico."

[40] Simone van der Hof: "Spain".

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Austria[41]

Austria was the first country to fully implement the EU Directive by the Austrian electronic signature act which entered into force on 1 January 2001. An accompanying ordinance was published in 2000. The level of detail is comparable to German legislation: Responsibilities (such as the supervision body) are defined, fees of supervision activities, concretion of security requirements of the CSP.

However, Austrian legislation does not provide a certification process for secure signature-creation devices in the manner the Reg TP certifies and publishes secure hardware and software.

Summary of the EU-wide comparison

In EU, Germany and Austria play a leading role regarding the legal implementation of electronic signatures. Other countries such as UK, France, and Spain, still lack detailed regulations regarding responsibilities (such as certification bodies) and procedures (which would be laid down in ordinances).

Exemplary implementations of legally valid electronic signatures

In Germany – and I assume other European countries do not differ considerably in this respect – electronic signatures currently play a role not worth mentioning in public life. This is 2003, six years after the first and two years after the second Signatures Act was adopted.

Why so? Isn't there a need for reliable authentication in the electronic world? Let's look how the authentication problem is tackled in various application areas in Germany:

Online Banking and Trading

Every major German bank has started online banking and trading services in recent years. These services are new, they did not have to overcome the legacy of existing structures and client relationships, they target at a broad audience and there is a vital need for reliable authentication. A perfect playground for electronic signatures, one might think. How do they do?

All the major „pure“ online banks and brokers (Advance Bank – http://www.advance-bank.de, comdirect – http://www.comdirect.de, DAB Bank – http://www.dab.com, Consors – http://consors.de, and Deutsche Bank/Deutsche Bank 24 – http://www.deutsche-bank.de) rely on PIN/TAN authentication (PINs for one-time and TANs for per-transaction authentication).

To enhance security, the banks have developed a standard for online banking called HBCI[42]. As of January 2003, more than 1900 credit institutions offer the HBCI standard.[43]

To ensure security in online banking on the user's side, the Federal Association of German Banks publishes their opinion on how to do secure online banking[44]: Secure your PC (by using an anti-virus scanner, performing a security check, using secure browser settings, backing up data), check SSL certificates of your communication partners, choose secure passwords, and deal carefully with sensitive data.

PIN/TAN authentication, a specialized standard for online banking technology, PC security on the user's side - this is the state of the art how major German banks ensure security on the user's side in a multi-billion EURO business six years after the first Signatures Act became effective!

---

[41] The content of this section is based on Simone van der Hof: “Austria”, “Summary of the Austrian Law on Electronic Signatures”, and “Federal Electronic Signature Law”.

[42] see the official documentation „Welcome to HBCI“ by Zentraler Kreditausschuss

[43] „Banks offering HBCI“

[44] „Online-Banking-Sicherheit“

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Communication with public authorities

Communication between citizens and public authorities requires a lot of authentication. Office hours of the public authorities are limited. Handicapped people or people living in remote areas have difficulties visiting the offices. And the state is meant to be a role model – so why not use electronic signatures?

I can think of many areas of application: applications for official documents (such as driving licenses, passports, ID cards), income tax return, insight into confidential documents or information not free of charge, or simply elections.

On a national level, there has been no attempt to employ electronic signatures for authentication between citizens and public authorities for day-to-day tasks.

There is a point solution for income tax return (and several other taxes) called ELSTER[45]. The electronic tax return does not use electronic signatures and still requires a hand-written signature for authentication against the tax authorities. However, employment of electronic signatures is intended for future releases.

Many communes engage in eGovernment projects; the state of these eGovernment projects as of June 2002 is described in detail in „E-Government in Deutschland – Profile des virtuellen Rathauses". Three of projects – Nuremberg, Bremen, and Esslingen – are supported by the Federal Ministry of Economics and Labour (see „MEDIA@Komm" for details on these supported reference projects). Implementation of qualified electronic signatures was a prerequisite for the funding. The three supported communes have implemented qualified electronic signatures and belong to the international top level regarding the extent of technical and legal realization[46]. Nuremberg offers 30 areas of application and has issued 1,000 secure signature-creation devices by May 2002. The near-term goal is to double this number until end of 2003. Bremen supports 35 application areas and has issued 2,250 secure signature-creation devices. Until end of 2003, 180 application areas shall be supported electronically, and 10,000 secure signature-creation devices shall be distributed to the public. In Esslingen, up to May 2002 not a single application area was realized, however, they are going to realize 30 application area by the end of 2003; 1,500 secure signature-creation devices shall be distributed by then.

Amongst the communes which were not supported, 12 communes have implemented or are going to implement electronic signatures. Meanwhile, one of them (Mannheim) has given up electronic signatures due to lack of demand.[47]

The unsupported communes suffer from the lack of technical standards and compatibility of the various products for electronic signatures.

> „Some communal representatives think that some initiatives of the respective government of a Land little helpful. For example, the card issued by the Land Baden-Württemberg was considered a competition of communal projects."[48]

The town of Büchen has implemented 15 different areas of application using advanced electronic signatures. The implementation of advanced electronic signatures is less costly than implementing qualified electronic signatures, but does not provide legal equivalence with a written signature. Thus, the authenticity of the chosen areas of application is less critical than the ones I described in the beginning of this section: Büchen supports insight

[45] „Informations about ELSTER - the electronic tax return"
[46] „E-Government in Deutschland – Profile des virtuellen Rathauses", p. 9 and 64
[47] „E-Government in Deutschland – Profile des virtuellen Rathauses", p. 65 and following
[48] „E-Government in Deutschland – Profile des virtuellen Rathauses", p. 34, translation by author

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

into official documents, cancellation of registration, ordering an income tax card, and announcement of address change, for example.

Apart from the technical complexity and the financial effort, the activities on the communal level suffer from lacking networking effects:

> "Especially the communes are working intensely on implementation concepts, technical solutions and procedures. E-Government projects are developed in many places. However, the activities are networked insufficiently. The experiences that could be helpful for other communes are frequently not passed on at all or only to small circles, and therefore they are not used efficiently. In this situation, many good examples threaten to remain unappreciated, although they could serve as blueprints for appropriate developments to other communes."[49]

Business relationships

In business life, contracts are signed, a lot of information whose integrity (and confidentiality!) is important is transmitted (think of tenders, deadline commitments), and financial transactions are carried out in large numbers so that electronic signatures could improve efficiency considerably.

What do enterprises think about electronic signatures? Stephan Maruschke works in the legal department of Dachser GmbH & Co KG, a major German transport and logistics company, and has examined electronic signatures for his company. According to personal communication with Mr. Maruschke, his findings are:

- The legal recognition of electronic signatures is adequate.
- Electronic signatures have not established themselves in business life sufficiently.
- The IT costs are expected to be significant – higher than the efficiency gain (in financial transactions, for example).
- There are no significant client requirements to support electronic signatures.
- There is a risk to bet on the wrong horse by choosing a particular technology.

The company has decided to await – until dominant products have emerged, until general acceptance has increased, until business requirements arise.

Relevance in real life – summary

Electronic signatures have not been accepted as a means for authentication in private, business, and civil life.

Where authentication is necessary in the online world, point solutions have emerged that serve the respective need. The security and level of sophistication varies from simple user/password authentication (ebay Germany works this way, and they do not even encrypt the transmission of user names and passwords!) up to card systems with strong encryption and authentication of the user on the card (e.g. HBCI for home banking).

The efforts on a communal level are remarkable, but they suffer from insufficient networking.

Companies and private people avoid a product decision – everyone in the game waits for the other players to go ahead.

Above all, there is a lack of standardization – there are many different technical products and CSP's on the market. The various products and services do not interoperate sufficiently: Creation and verification of signatures cannot be performed using one set of products if signatory and verifier have different products and CSP's.

[49] „kikos-Newsletter vom 08. Oktober 2002", p. 1 -2, translation by author

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

What's ahead?

Foundation of the "Alliance for Electronic Signatures"

In April 2003, the "Alliance for electronic signatures" was founded by public institutions and enterprises to promote electronic signatures in Germany.[50]

The founding public institutions are the Federal Ministries of Interior, Economics, and Finance, the IT Central of the Land Niedersachsen, the three communes Nuremberg, Bremen, and Esslingen[51], and the Federal Insurance Institution For Employees (Bundesversicherungsanstalt). The founding enterprises are Siemens, HypoVereinsbank, Deutscher Sparkassenverlag, the IT Central of the savings banks, the Deutsche Sparkassen- und Giroverband, and the Deutsche Bank.

According to the Federal Ministry of Interior,

> "Germany was one of the first countries in the world which equated electronic signatures to written signatures. Therewith we were pioneers in law, but unfortunately not in practice."[52]

The alliance aims mainly at sharing existing infrastructure to reduce the number of different products and applications. It shall become possible to use several applications with one SmartCard. However, the alliance does not aim to consolidate the certification services. The number of CSP's will remain.

What should be ahead?

The EU Directive aims to increase the competitiveness of the European CSP's. Thus, competition of various CSP's is desired by the European Commission.

The author believes[53] that the resulting heterogeneity of products and services is a crucial point.

Authentication is a very basic and fundamental service, and electronic signatures accomplish this purpose in the digital world. Decades ago, the state has accepted authentication as a public task. Passports and identity cards have always been issued by national institutions.

So why should this be different in the digital world? Electronic signatures are not about features; the whole business consists of the question if particular data is to be associated with a particular natural person. What advantage does the public have from competing enterprises?

The broad public will not be willing to pay considerably for electronic signatures. Signing has been free for centuries, so why should I pay for it just because I use a computer instead of a pencil? This is the reason why I believe that certification services are not a business with multi-million Euro returns – unless signing is "enriched" with additional services or a strong monopoly has emerged.

Both alternatives are not desirable.

So, if electronic signatures are left at the market, either one more monopoly is going to rule its part of the world, or electronic signatures will not take off.

List of References

The list of references is sorted in order of appearance:

---

[50] This section is based on "Bündnis für elektronische Signaturen gegründet".
[51] See section "Communication with public authorities"
[52] "Bündnis für elektronische Signaturen gegründet", translation by author
[53] A similar opinion is expressed by Heinrich C. Mayr in "Bündnis für elektronische Signaturen gegründet".

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Reg TP. „Electronic Signatures“. URL: http://www.regtp.de/imperia/md/content/tech_reg_t/digisign/102.pps (28 March 2003).

European Parliament. „EU Directive“. Directive 1999/93/EC of the European Parliament and of the Council on a Community framework for electronic signatures. 13 December 1999. URL: http://www.sicherheit-im-internet.de/download/eu-signatur-e.pdf (21 January 2003). Published in Official Journal of the European Communities, 19 January 2000.

European Commission. „EU-Richtlinie“. Richtlinie 1999/93/EG des Europäischen Parlaments und des Rates über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen. 19 January 2000. http://www.sicherheit-im-internet.de/download/eu-signatur-d.pdf (21 January 2003). Published in Official Journal of the European Communities, 19 January 2000.

German Government. „Signatures Act“. Law Governing Framework Conditions for Electronic Signatures and Amending Other Regulations - inofficial version for industry consultation. 16 May 2001. URL: http://www.sicherheit-im-internet.de/download/026-Signaturges_englisch.html (21 January 2003). Published in Official Journal (Bundesgesetzblatt) 21 May 2001.

German Government. „Signaturgesetz“. Gesetz über Rahmenbedingungen für elektronische Signaturen und zur Änderung weiterer Vorschriften. 21 May 2001. URL: http://www.sicherheit-im-internet.de/download/signaturgesetz.pdf (21 January 2003). Published in Official Journal (Bundesgesetzblatt), 21 May 2001.

European Parliament. „Common Position (EC) No 28/1999“. on a Community framework for electronic signatures. 28 June 1999. URL: http://www.accurata.se/QC/documents/direng990827.pdf . Published in Official Journal of the European Communities, 27 August 1999.

Mankowski, Peter. „Wie problematisch ist die Identität des Erklärenden bei E-Mails wirklich?“. NJW. 39 (2002): 2822 – 2828.

German Government. “Telekommunikationsgesetz”. 25 July 1996. URL: http://www.bmwi.de/Homepage/download/telekommunikation_post/tkg.pdf (28 March 2003).

Schneier, Bruce. Secrets and Lies. Chichester: John Wiley, 2000.

German Government. „Ordinance on Electronic Signatures“. Unofficial working translation. 16 November 2001. URL: http://www.sicherheit-im-internet.de/download/sigvo-final.pdf (21 January 2003). Published in Official Journal (Bundesgesetzblatt), 21 November 2001.

German Government. „Verordnung zur elektronischen Signatur“. Signaturverordnung – SigV. 16 November 2001. URL: http://www.dud.de/dud/documents/sigv-011116.pdf (21 January 2003). Published in Official Journal (Bundesgesetzblatt), 21 November 2001.

German Government. „Formanpassungsgesetz“. Gesetz zur Anpassung der Formvorschriften des Privatrechts und anderer Vorschriften an den modernen Rechtsgeschäftsverkehr. 13 July 2001. URL: http://www.bsi.de/esig/basics/legalbas/formanpg.pdf . Published in Official Journal (Bundesgesetzblatt), 18 July 2001.

German Government. “BGB § 126 Schriftform”. 2 January 2002. URL: http://bundesrecht.juris.de/bundesrecht/bgb/__126.html (19 April 2003).

German Government. “BGB § 126a Elektronische Form”. 2 January 2002. URL: http://bundesrecht.juris.de/bundesrecht/bgb/__126a.html (19 April 2003).

Reg TP. “RegTP's Tasks”. URL: http://www.regtp.de/imperia/md/content/tech_reg_t/digisign/100.pps (28 March 2003).

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Reg TP. “Verzeichnisdienst der Regulierungsbehörde für Telekommunikation und Post”. URL: http://www.nrca-ds.de (19 April 2003).

Reg TP. „Certificates issued by the competent authority“. URL: http://www.regtp.de/en/tech_reg_tele/in_06-02-02-00-00_m/01/index.html (28 March 2003).

Reg TP. „Recognised attestation bodies for technical components“. URL: http://www.regtp.de/en/tech_reg_tele/in_06-02-02-00-00_m/04/index.html (28 March 2003).

Reg TP. „Certification Service Providers“. URL: http://www.regtp.de/en/tech_reg_tele/start/in_06-02-04-00-00_m/index.html (28 March 2003).

Reg TP. „Electronic Signature Products“. URL: http://www.regtp.de/en/tech_reg_tele/start/in_06-02-05-00-00_m/index.html (28 March 2003).

Reg TP. „Legal Status of Qualified Electronic Signatures“. URL: http://www.regtp.de/imperia/md/content/tech_reg_t/digisign/101.pps (28 March 2003).

Reg TP. „Suitable Cryptographic Algorithms“. URL: http://www.regtp.de/en/tech_reg_tele/in_06-02-02-00-00_m/03/index.html (28 March 2003).

Simone van der Hof. “Digital Signature Law Survey – What's New”. 12 February 2003. URL: http://rechten.uvt.nl/simone/ds-new.htm (20 April 2003).

Simone van der Hof. “France”. May 2001. URL: http://rechten.uvt.nl/simone/tekst.asp?Land=France&Verzendknop=Submit (20 April 2003).

French Government. “Décret no 2001-272 du 30 mars 2001 pris pour l'application de l'article 1316-4 du code civil et relatif à la signature électronique”. 31 March 2001. URL: http://www.admi.net/jo/20010331/JUSC0120141D.html (20 April 2003).

Simone van der Hof. “UK”. 24 April 2002. URL: http://rechten.uvt.nl/simone/tekst.asp?Land=United+Kingdom (20 April 2003).

British Government. “Electronic Communications Act 2000”. 25 May 2000. URL: http://www.legislation.hmso.gov.uk/acts/acts2000/20000007.htm (20 April 2003).

British Government. “The Electronic Signatures Regulations 2002”. 8 March 2002. URL: http://www.legislation.hmso.gov.uk/si/si2002/20020318.htm (20 April 2003).

Simone van der Hof. “Spain”. 12 March 2003. URL: http://rechten.uvt.nl/simone/tekst.asp?Land=Spain&Verzendknop=Submit (20 April 2003).

Spanish Government. “LEY 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.”. 11 July 2002. http://www.setsi.mcyt.es/legisla/internet/ley34_02/sumario.htm (20 April 2003).

Simone van der Hof. “Austria”. October 2000. URL: http://rechten.uvt.nl/simone/tekst.asp?Land=Austria&Verzendknop=Submit (20 April 2003).

Dr Brenn, Christoph. “Summary of the Austrian Law on Electronic Signatures”. URL: http://rechten.kub.nl/simone/brenn.htm (20 April 2003).

Austrian Government. “Federal Electronic Signature Law” (Signature Law – SigG). 1 January 2001. URL: http://www.bmck.com/ecommerce/austrianesig.pdf (20 April 2003).

Zentraler Kreditausschuss. “Welcome to HBCI”. URL: http://www.hbci.de/siz_hbci.nsf/PageNames/english?OpenDocument (19 April 2003).

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Zentraler Kreditausschuss. „Banks offering HBCI“. 10 January 2003. URL: http://www.hbci.de/siz_hbci.nsf/Images/HBCIInstitute/$File/HBCI-Institute.xls?OpenElement (6 April 2003).

Bundesverband deutscher Banken. „Online-Banking-Sicherheit“. URL: http://www.advance-bank.de/pdf/info/sicherheit_onlinebanking.pdf (6 April 2003).

Oberfinanzdirektion Muenchen. „Informations about ELSTER - the electronic tax return“. URL: https://www.elster.de/ssl/main-pro-info-english-01.htm“ (6 April 2003).

Dr. Helmut Drüke. “E-Government in Deutschland – Profile des virtuellen Rathauses”. URL: http://www.mediakomm.net/documents/arbeitspapier.8.2003.pdf (12 April 2003).

Deutsches Institut für Urbanistik. “MEDIA@Komm”. URL: http://www.mediakomm.net/index.phtml (12 April 2003).

KGSt. “kikos-Newsletter vom 08. Oktober 2002”. 8 October 2002. URL: http://www.kgst.de/menu_links/produkte/kikos_wissensdatenbank/aktuelles/kikos_newsletter_vom_08_oktober_2002/newsletter_okt02.pdf (6 April 2003).

Golem. “Bündnis für elektronische Signaturen gegründet”. 3 Apr 2003. URL: http://www.golem.de/0304/24858.html (20 April 2003).

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.