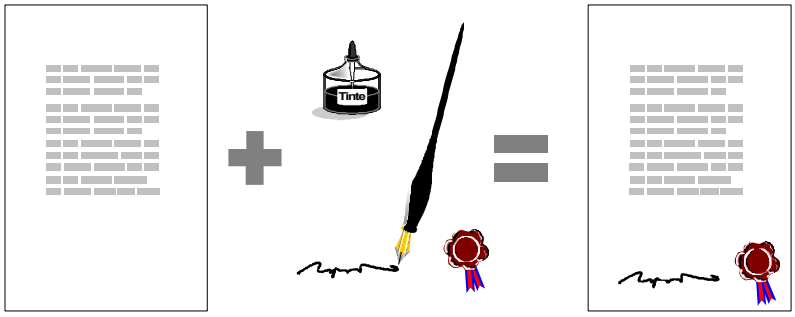
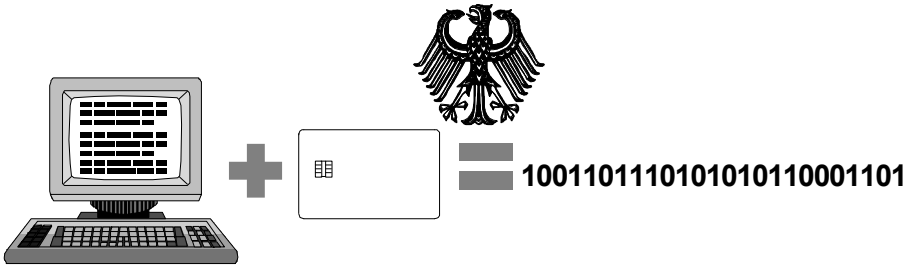
# DRAFT

# BSI Manual
# for Digital Signatures
## - on the basis of the Digital Signature Act (SigG)
## and the Digital Signature Ordinance (SigV) -

**Version 1.0**



# Introduction

Secure use of today's globally internetworked information technology requires the application of effective cryptographic mechanisms. This relates not only to the encoding of confidential data which initially springs to mind in this context. Modern asymmetric cryptography has also developed methods which are able to ensure the integrity and authenticity of digital data. Digital signatures are of special significance in this connection. Such signatures represent a functional digital equivalent to signing paper documents by hand.

The applications for digital signatures range from ordering goods, issuing means of identification, effecting bank transfers through to issuing medical certificates, for example. Digital signatures are a means of further digitalising information processing. In many instances, having to fall back on paper documentation for the purpose of signing is an extremely ineffective practice. The use of digital signatures enables digital information to be processed substantially more effectively, and is thus ultimately of major economic significance as well.

Around 20 years after their 'invention', concrete implementations of digital signatures are now widespread. In the USA, a specific algorithm has been mandatory for the area of administrative bodies and authorities since 1992, and numerous institutions are currently working on further standards for signature algorithms. The Federal German government initiated a Digital Signature Act [SigG] via a cabinet decision at the end of 1996, with the legislation subsequently coming into force on 1st August, 1997.

This Act is intended to prevent a proliferation of uncontrolled standards, to regulate the organisation of the required infrastructure, such as the certification authorities, and in this way to lay down the general conditions for practical introduction of the digital signature on a broad basis. In particular, this legislation establishes the essential basis for safeguarding the rights of individual participants in electronic legal transactions. In a further step, it will then be possible to draw up statutory regulations for legal issues relating to digital signatures.

The present safeguard catalogues for digital signatures have been drafted by the German Information Security Agency. They describe how the individual technical components and the organisational environment are to be configured and structured in order to achieve an overall system in which digital signatures can be created which possess the necessary degree of security to prevent forgery and manipulation.

## Literature

[SigG] Act on Digital Signature (Digital Signature Act - SiG) of 22nd July, 1997 (Federal German Law Gazette I, pp. 1870, 1872), promulgated as Article 3 of the 'Federal Act Establishing the General Conditions for Information and Communication Services (Information and Communication Services Act - IuKDG)'

# Contents

# 1. Outline

This volume contains the specifications of the German Information Security Agency (BSI) with regard to the safeguard catalogues laid down in the Ordinance to the Digital Signature Act [SigG]. § 12 of the Digital Signature Ordinance [SigV] requires the safeguard catalogue to be taken into account in the drafting and review of security concepts and in connection with confirmation of the results of security concept reviews. The safeguard catalogue in accordance with § 16 SigV is to be taken into account in the development and testing of technical components and in connection with confirmation of the results of testing on technical components.

Experts from the areas of industry and science were involved in drafting and coordinating the specifications contained in this volume. In the course of the coming years, the catalogues will require further development and adaptation to the duly acquired practical experience. To this end, the BSI is establishing a discussion forum, the results of which will be incorporated by means of a yet to be specified procedure into the next version of the safeguard catalogues to be maintained by the regulatory authority.

The introduction in Chapter 1 is followed in Chapter 2 by an overview of the services to be provided by certification authorities. An analysis of protection requirements is proposed for these services, and the manner of interaction between the services is presented.

Chapter 3 contains general recommendations on the design of certificates and on the contents of signatures. As in subsequent chapters, the recommendations are geared to international standards.

Chapter 4 presents the canonical procedures for all activities relating to digital signatures, from establishment of the required security structure through to the generation and testing of a digital signature. These procedures are oriented to the proposed solutions which are outlined in subsequent chapters. The detailed specifications for the procedural structures will be incorporated into the next version of the safeguard catalogues, after due consultation with users and experts from the areas of industry and science. The current state of progress is already accessible to interested members of the public as a basis for discussion on the BSI's webpage, http://www.bsi.bund.de.

In Chapters 5, 6, 7, the passages which are of relevance to security aspects are extracted from the Act and the Ordinance, and requirements and recommendations are then established on the basis of these passages. On the basis of model proposals, after listing the specific threats security safeguards which counteract the stated threats and fulfil the requirements and recommendations are proposed for the outlined proposals. A clear summary of these safeguards in tabular form is then provided. Chapters 5 and 6 form the core of the specifications for the safeguard catalogues.

Chapter 5 contains the safeguards which should be taken into account by certification authorities when drafting security concepts.

Chapter 6 contains the safeguards which are to be taken into account in the development, testing and deployment of technical components in accordance with SigG and SigV. This covers such diverse areas as cryptographic algorithms, key generation, the drafting of certificates, the personalisation of signature components, the directory services, the time stamping service, the operational environment and the signature component.

According to the same procedure as in the previous chapters, Chapter 7 then develops safeguards which are required for the licensing of certification authorities and the approval of verification bodies for the results of evaluations and tests on security concepts and technical components.

Finally, Chapter 8 lists the rules and standards cited in the text; a summary of cited literature is provided at the end of each chapter.

## Literature

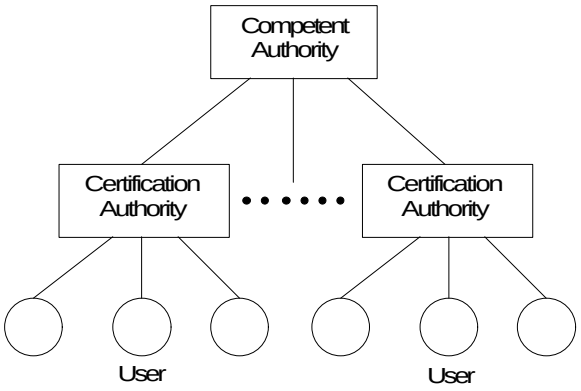
[SigG] Act on Digital Signature (Digital Signature Act - SiG) of 22nd July, 1997 (Federal German Law Gazette I, pp. 1870, 1872), promulgated as Article 3 of the 'Federal Act Establishing the General Conditions for Information and Communication Services (Information and Communication Services Act - IuKDG)'

[SigV] Ordinance on Digital Signature (Digital Signature Ordinance - SigV) of 22nd October, 1997 (Federal German Law Gazette I, p. 2498)

# 2 General Organisational Structure for Certification Authorities

This chapter provides an outline of the possible organisational structure for certification authorities (CA) in connection with the Act on Digital Signature [SigG].

In order to satisfy the requirements of the Act and the Ordinance, it is necessary in particular to establish a safety infrastructure (cf. also [RFC1422]) which enables authentic assignment of the public signature keys to natural persons (via a certificate). In this connection, the Act stipulates a safety infrastructure which establishes a two-level hierarchy of certification authorities:




The 'competent authority' in accordance with the Digital Signature Act functions here as the root authority and exclusively certifies specific public signature keys of approved certification authorities. In turn, these authorities exclusively certify the public signature keys of the connected users.

The following sections first of all present the services to be offered by a CA and then establish the typical scope of protection requirements.

## 2.1 Services to be rendered by a certification authority

### 2.1.1 Key generation for the certification authority

The certification authority is required to generate a key pair, consisting of a public and a private[1] key, corresponding to the selected method for producing digital signatures. This key pair is required in order to certify the public keys of the users using the method for digital signatures which is supported by the CA. The key pair must be generated in a suitable and secure environment within the CA. It must furthermore be ensured that unauthorised access to the private CA key is prevented.

This task is performed by the Key Generating Service.

[1] The secrecy of private keys should be maintained.

### 2.1.2 Establishment of the users' identities (incl. registration) (RA)

The users of a system for digital signatures must furnish proof of their identities to a trustworthy third party - in this case the certification authority. On positive identification being established, the user is assigned a suitable unambiguous name under which he is able to generate digital signatures. Should the user not wish to reveal his name to third parties, the name can be allocated in the form of a pseudonym, thus ensuring that the user's identity is not disclosed directly to third parties.

This task is performed by the Registration Authority (RA).

### 2.1.3 Certification of public user keys (CS)

For each user of the system, the CA is required to produce a certificate (cf. [X.509] or [X.509v3], for example), the contents of which include an identifying attribute for this user, the user's public key and a period of validity. These content items are combined in an authentic and non-manipulable manner by the digital signature, which is generated by the private key of the CA.

This task is performed by the Certification Service (CS).

### 2.1.4 Personalisation of the signing component when user keys are generated by the certification authority

When the user's private key is generated at the certification authority, it must be stored on a suitable signing component (e.g. a chipcard). Also, the user authentication process of the signing component must be activated (e.g. via a password or biometric attributes). The user data, the certificate for the public key and the public key of the CA can also be stored on this signing component.

This task is performed by the Personalisation Service.

### 2.1.5 Directory service (DIR)

All the key certificates of all users to this CA must be contained in authentic and non-corrupted form in a directory. Revoked certificates are entered in a revocation list which contains information on the time of revocation. The revocation information is to be kept available for retrieval by anyone at all times (verifiability of certificates). The certificates themselves and individual items of information from the certificates (e.g. user's name, public key) may be made accessible to third parties subject to the user's consent only.

### 2.1.6 Time stamping service (TSS)

In certain instances it is necessary to establish an authentic link between digital data and a specific time. For this purpose, such data are digitally combined with the reliable time to be provided by the CA's time stamping service and the result is subsequently digitally signed by the CA[2] . The duly signed data are then returned to the user.

[2] The time stamping service is therefore user of its own CA.

### 2.1.7 Generation of keys for users

When the user does not possess his own generated key pair, a key pair is to be generated for the user by the CA. This key pair consists of a private and a public key. The private key is used by the user to create digital signatures, while the public key is required to verify the signatures. It is essential that the private key be destroyed at the CA after being issued to the user, and that each key pair occur once only. To enable authentic allocation of the digital signatures generated by the user, allocation of the key pair to this user must also be effected in an authentic manner.

This task is performed by the Key Generating Service.

## 2.2 Analysis of Protection Requirements for a Certification Authority

Each of the above-stated services is subject to specific protection requirements with regard to confidentiality, integrity and availability. The protection requirements of the respective supporting IT applications, IT systems or communication systems can be derived directly from these specific protection requirements.

The table below specifies and explains the protection requirements which are to be typically expected for the respective services. The following protection levels are specified:

low/medium*: The potential harm is negligible, or limited and clearly foreseeable.

high: The potential harm may be considerable either for the user or for the CA.

very high: The potential harm may attain catastrophic proportions which threaten the existence of the user or the CA.

* Differentiation is not necessary, as IT baseline protection safeguards are required and adequate for both categories.

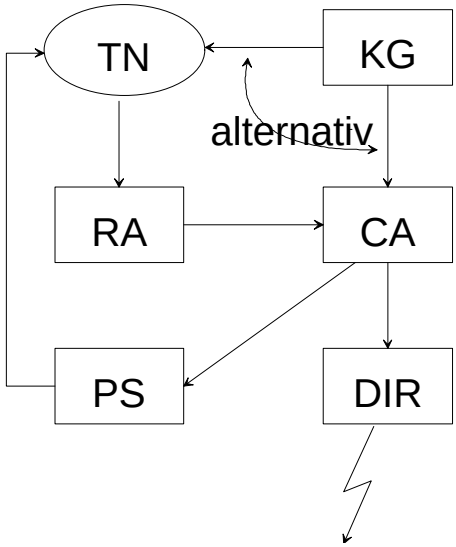
| **Protection requirements for the services of a certification authority** | | | | | | |
|---|---|---|---|---|---|---|
| **No.** | **Name** | **Aspect** | low/ medium | high | very high | **Explanation** |
| 1 | Key generation for the certification authority | Confiden -tiality | | | X | Certificates can be generated with the private key of the CA. |
| | | Integrity | | X | | When CA keys lack integrity, the certificates of all users will also lack integrity. The security structure will then be inoperable. The users do not incur any direct harm, however. |
| | | Avail- ability | X | | | Generation of the CA's key pair is non-time-critical. |

| **Protection requirements for the services of a certification authority** | | | | | | |
|---|---|---|---|---|---|---|
| **No.** | **Name** | **Aspect** | low/ medium | high | very high | **Explanation** |
| 2 | Establishment of identity (RA) | Confiden-tiality | X | (X) | | Although the information relates to individual persons, it is nevertheless open.<br>(In the case of pseudonyms the confidentiality requirement is high). |
| | | Integrity | | X | (X) | The identification parameters must enable unambiguous identification of the user.<br>(When key material generated by the user is submitted, the authentic linkage of identity and key pair must be completely guaranteed, so as to ensure that the identity of the person providing a signature can be established without any doubt (**N**on **R**epudiation of **O**rigin, NRO). |
| | | Avail-ability | X | | | The temporary inability to authorise a new user is acceptable. |
| 3 | Certification of the public key (CA) | Confiden-tiality | | | X | The private certification key of the CA is employed, which is absolutely confidential. |
| | | Integrity | | | X | The certificate must provide binding information on the validity and assignment of a user's public key (NRO). |
| | | Avail-ability | X | | | The temporary inability to issue a certificate to a new user is acceptable. |
| 4 | Personalisation of the signing component when user keys are generated by the certification authority | Confiden-tiality | | | X | When personalisation of the signing component is effected with a private user key generated at the CA, the confidentiality of this key and of the user authentication password is to be guaranteed absolutely, in order to prevent the unauthorised generation of digital signatures in the user's name. |
| | | Integrity | | | X | It must be ensured that the correct private signature key and the correct certificate are assigned to the signing component, as the possibility of digital signatures being generated under the wrong name cannot otherwise be excluded. |
| | | Avail-ability | X | | | The temporary inability to provide a new user with a signing component and thus with a certificate is acceptable. |

| **Protection requirements for the services of an certification authority** | | | | | | |
|---|---|---|---|---|---|---|
| **No.** | **Name** | **Aspect** | low/ medium | high | very high | **Explanation** |
| 5 | Directory service (DIR) | Confiden-tiality | X | (X) | | Although the information relates to individual persons, it is nevertheless open. (In the case of certificates which are not available for retrieval, the confidentiality requirement is high). |
| | | Integrity | | | X | The authentic linkage of identity and key pair and the current validity and correctness of the entries, in particular the revocation entries, must be ensured absolutely. |
| | | Avail-ability | | | X | The inability to access the directory services is not acceptable. |
| 6 | Time stamping service (TSS) | Confiden-tiality | | | X | The private key of the time stamping service is incorporated, and this key is absolutely confidential. |
| | | Integrity | | | X | The time stamp provides binding information on the linkage of a document to a specific time, and must be completely verifiable. |
| | | Avail-ability | | | X | The documents to be signed may be time-critical, e.g. when deadlines require to be observed. |
| 7 | Generation of keys for users | Confiden-tiality | | | X | With the generated keys, signatures of the user can be produced without authorisation; misuse must thus be prevented. |
| | | Integrity | | X | | The assignment of a key pair lacking integrity to a new user, as a result of which his signatures will be declared invalid, is to be avoided. The user does not incur any direct harm, however. |
| | | Avail-ability | X | | | The temporary inability to provide a new user with a key is acceptable. |

## 2.3 Interaction between the services of a certification authority

The above-specified services (with the exception of the time stamping service) do not operate independently of one another. The following basic procedure shows how these services interact with one another (cf. [ISO14516-2]):




A key pair is first of all generated (KG) by the user (TN) himself or at the certification authority. The user is registered and identified at the registration authority (RA) and applies for a certificate. This certificate is drafted by the certification authority (CA) and is transmitted both to the personalisation system and to the directory service (DIR). The personalisation system (PS) assigns the data which are relevant for the user and which are not yet on the signing component (i.e. this data may include the key pair) to the signing component, which can then be issued to the user.[3] The directory service can be reached via public communication facilities.

The time stamping service is a service which can be used by both the user and the RA or CA, in order to link any desired data or the certificate, for example, to a specific point in time. It is thus not explicitly incorporated into a specific procedure.

The following procedures:

- application by the user with registration,
- identification of the user,
- key generation and drafting of certificate,
- personalisation and issuing of the signing component to the user

thus require to be specified for the operations of a certification authority, together with

- accessing of the directory and time stamping service, and
- a revocation management system.

Note: By analogy with the Digital Signature Act, the terms stated in Chapter 2.1 are employed here exclusively in the meanings set out in this chapter. Different interpretations are to be found in the relevant literature.

## Literature

[ISO14516-2] Guidelines for the use and management of Trusted Third Parties - Part 2: Technical aspects, ISO/IEC Draft 1995

[RFC1422] Kent, S., 'Privacy Enhancement for Internet Electronic Mail: Part II: Certificate-Based Key Management', RFC 1422, BBN, February 1993.

[SigG] Act on Digital Signature (Digital Signature Act - SiG) of 22nd July, 1997 (Federal German Law Gazette I, pp. 1870, 1872), promulgated as Article 3 of the 'Federal Act Establishing the General Conditions for Information and Communication Services (Information and Communication Services Act - IuKDG)'

[X.509] ITU-T Recommendation X.509 (1993), Information technology - Open Systems Interconnection - The directory: authentication framework

[X.509v3] ITU-T Recommendation X.509, Information technology - Open Systems Interconnection - The directory: authentication framework, amendment 1: Certificate Extension, Final Draft 1996

# 3. General recommendations

## 3.1 The structure of certificates

§ 7 of the Digital Signature Act regulates the content of certificates:

> *(1) The signature key certificate shall contain the following information:*
>
> *1. name of the holder of the signature key to which additional information must be appended in the event of possible confusion, or a distinctive pseudonym assigned to the holder of the signature key, clearly marked as such,*
>
> *2. public signature key assigned,*
>
> *3. names of the algorithms with which the public key of the holder 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.*
>
> *(2) Information relating to the authority to represent a third party and to the professional admission to practice or other type of admission may be included both in the signature key certificate and in an attribute certificate.*
>
> *(3) Further information shall not be included in the signature key certificate unless the parties concerned give their consent.*

The provisions under § 7 enable the holder of a signature key to restrict the validity of the digital signatures generated with his signature key to specific legal transactions or to certain maximum monetary limits. In this context it is also possible to restrict the use of the signature key to authentication applications. It is also conceivable, for example, that some holders of signature keys may wish to use their chipcard, which serves as the signature key carrier, exclusively on technical components which are offered for use to third parties on a commercial basis. In technical terms, this could be achieved by means of a procedure whereby this chipcard requires authentication of the terminal, prior to generating a signature (see explanatory note on § 16 (3) SigV and S-CHIP 7.2).

The signature key certificate must expressly indicate whether a restriction in accordance with Article 7 applies. A more detailed description of these restrictions can then be provided in an attribute certificate.

The Digital Signature Act describes only minimum requirements for the contents of certificates. There is nothing to prevent the inclusion of further information in a certificate (e.g. the date of birth for minors, e-mail addresses) in accordance with contractual agreements between the holder of the signature key and the certification authority - that is, subject in particular to the consent of the signature key holder. § 5 SigV stipulates that a certification authority must verify that suitable technical components are employed for storage and application of the private signature key. This information could also be incorporated into the certificate, in the form of a manufacturer's or type code. On the basis of this code, the certificate would then clearly indicate, for example, whether

- the hashing algorithm stated in the certificate has been implemented on the technical component,
- the hashing computation process is carried out in part or entirely on the technical component,
- additional biometric authentication of the signature key holder is necessary,
- additional biometric authentication of the signature key holder is possible,
- specific data objects are appended to the data to be signed, and subsequently also signed independently of this technical component, and
- whether renewed entry of the signature key holder's identification data is required before each digital signature, after a preset number of digital signatures, or after a specific time has elapsed without the signing technology being used (explanatory note on § 16 (2) SigV).

The implementation of these requirements for the content of certificates in bit-accurate specifications is the responsibility of the competent standardisation bodies and the industrial sector. ITU-T X.509v3 [X.509v3] represents an international standard to specify the content of certificates. This sweep of this standard is very broad and flexible, however, as illustrated by the manner in which it grants every organisation the possibility of introducing and registering new extension fields. In principle, X.509v3 enables special information, such as the above-stated restrictions, to be encoded within a certificate, by defining so-called 'private extensions'. Other information, such as e-mail addresses, can be represented as 'standard extensions'. In stipulating and specifying certain contents of certificates, due account should generally be taken of international developments, such as the Internet Drafts on the Internet Public Key Infrastructure, or the 'Extended Certificates' in accordance with PKCS # 6, # 9 [PKIX] to specify the authority to represent a third party and the professional admission to practice or any other type of admission. The primary task here for the competent authority is, of course, to attain broad interoperability for those contents of certificates which have yet to be standardised via appropriate coordination of the appurtenant definitions.

In addition to the signature key holders, the certification authorities and the competent authority themselves, the following services assigned to the certification authorities also possess their own signature keys:

- Time stamping service

  This service will generally possess its own signature key. It is possible, however, that the signature key of the time stamping service may correspond to the signature key of the certification authority. In this case, the appropriate certificate or attribute certificate containing the 'time stamp' indicator must be incorporated into the data to be signed each time a time stamp operation is executed.

- Directory service

  The directory service signs revocation lists, information as to whether certain certificates are revoked or not, and lists of certificates and certificate indicators. As a supplementary function, it may sign notifications as to whether a signature submitted to it proved verifiable. The signature key of this service must not correspond to that of the certification authority.

- Internal documentation service

  § 13 SigV stipulates that a separate signature key is necessary to sign records which are maintained by the certification authority in digital form.

These services may possess a certificate of their certification authority and also dispose directly of a certificate of the competent authority.

In addition to the unambiguity of names, X509v3 also lays down provisions for specifying the use of the certified signature key by means of appropriate attributes (e.g. key usage for directory service and certification authorities).

In addition to these certificates which are directly stipulated by legislation, additional certificates and appurtenant signature keys arise in the course of developing a functioning infrastructure for digital signatures, e.g. for the purposes of:

- the mutual authentication of signature key holder and technical components which are made available for use to third parties on a commercial basis, prior to the generation of a signature - see explanatory note § 16 (3) SigV and S-CHIP 7.2,

- the mutual authentication of signature key holder and the personalisation system of the certification authority when key generation is effected on the signature key carrier - see explanatory note § 5 (1) SigV and Chapter 4.3.2, and

- the mutual authentication of a security box and external processors, such as the time stamp and directory service, see S-SBOX 1.6.

In particular, those certificates which require autonomous interpretation by a chipcard, for example, in order to authenticate a terminal, will possess a substantially more simple structure and only a small number of data fields. These do not fall within the scope of the safeguard catalogue, but will be specified in connection with the chipcard specifications on digital signatures.

## 3.2 Content of signatures

§ 16 of the Digital Signature Ordinance requires in (3):

> *The technical components for verifying certificates must permit clear, reliable determination of whether verified certificates were present, without having been invalidated, in the register. The technical components must permit adequate determination, as necessary, of the contents of signed data or of data that is to be signed. If technical components pursuant to Sentences 1 to 4 are commercially provided to third parties for use, clear, reliable interpretation of the relevant data must be assured [...]*

This requirement can be satisfied by using only special formats and application programmes for certain applications. Otherwise, a data record must always be provided with an indicator specifying how it is to be interpreted. According to the law, the digital signature relates solely to the digital data themselves and is thus independent of the interpretation of these data. In this connection it is, however, incumbent on the business community to develop such unambiguous identification for its products.

§ 4 of the Digital Signature Ordinance requires the certification authority to inform the user of the following:

> *3. For generation and verification of digital signatures, and for display of data that must be signed or of signed data that must be verified, technical components shall be used that fulfil the requirements of the Digital Signature Act and of this Ordinance and whose security pursuant to the Digital Signature Act and this Ordinance has been confirmed. Such components shall be protected from unauthorised access.*
>
> *4. If a certificate contains restrictions pursuant to § 7 (1) No. 7 of the Digital Signature Act or information pursuant to § 7 (2) of the Digital Signature Act, and if this is significant with regard to the validity of signed data, the certificate shall be included with the data and in the digital signature.*
>
> *5. If a particular time can be of considerable significance with regard to use of signed data, a time stamp shall be appended.*
>
> *7. In verification of digital signatures, it shall be determined whether the signature key certificate and attribute certificates were valid at the time the signature was generated, whether the signature key certificate contains restrictions pursuant to $ 7 (1) No. 7 of the Digital Signature Act and whether Numbers 4 and 5 were complied with, if applicable.*

Number 7 expressly states that the appurtenant certificates and, where appropriate, even the certificates of the certification authority and of the competent authority itself are to be included in the verification of digital signatures (see also explanatory note on § 4 (7) SigV). This means that in the case of certificates/attribute certificates which are not available for retrieval in

particular, an unambiguous reference to the appurtenant certificate/attribute certificate must be affixed to the data which is to be signed.

The explanatory note on § 7 (2) expressly states that several certificates or attribute certificates, which under certain circumstances may even be from different certification authorities, may be issued for the same signature key. This appears perfectly realistic in the case of the following scenarios, for example:

- The holder of a signature key is issued a certificate containing his professional designation from one certification authority and a certificate without his professional designation from another certification authority. Both certificates are stored on his signature key carrier.
- Prior to expiry of the period of validity specified in the certificate, a user has a new certificate with a new period of validity issued for his unchanged signature key. On his signature key carrier, the old certificate is replaced by the new one. A chipcard which serves as a signature key carrier is unable to perform hashing computation itself, and requires input of an externally calculated hashing value. A certificate must, of course, contain all the necessary information to enable a signature to be verified without doubt, in particular the employed hashing algorithm. In order to support the various applications (e.g. home banking with a German bank, dispatch of a signed document abroad via e-mail) in which the created signature requires verification, the holder of a signature key could have one certificate issued for each of the most common hashing algorithms.
- A chipcard is able to perform the hashing computation itself, but various formats for integration of the hashing value into the signing algorithm can be supported (e.g. in accordance with PKCS # 1 and in accordance with ISO/IEC 9796-2 8ISO 9796-2], see chipcard specification on digital signature). A separate certificate is then provided for each format to be supported, so as to enable different applications to be supported as described above.

In view of these ambiguities as to which certificate belongs to a signature key, an unambiguous reference to the appurtenant certificate and any attribute certificates should be affixed to the data which is to be signed. In order to eliminate the possibility of manipulations, the digital signature must extend over this unambiguous reference. When there are neither restrictions in the certificate nor information in accordance with § 7 (2) SigG, and verification is required solely as to whether a certificate and any attribute certificates have been revoked, the cosigning of an unambiguous indicator for the certificate appears adequate, contrary to number 4 above.

The time stamp mentioned in number 5 generally covers the entire data record including the user's signature, particularly in the case in accordance with § 18 SigV, when signed data are required over a prolonged period. For special applications, however, it is necessary to affix a time stamp to the data which is to be signed, prior to signing the composite data record. This is the case, for example, when the directory service replies to an inquiry by the user as to whether a revocation entry applies to the certificate or not, as the time stamp eliminates the possibility of an old reply from the directory service having been read in again.

In accordance with number 3 above, each applicant must be instructed to use only duly verified components to generate and verify digital signatures and to display data which is to be signed and signed data which is to be verified. This does not preclude the possibility of users using their signature key carriers on non-secure systems, however. In order to provide the users with more effective protection, while at the same time also rendering it more difficult to dispute an actually affixed signature, instead of the signature key carrier merely signing the data record

with which it is supplied, the signature key carrier could also independently append certain data objects to this data record. The signature would then be effected via the composite data record. The following data objects should be taken into consideration:

- Total number of all affixed signatures (signature counter)

  This may prove problematic under certain circumstances, for reasons relating to data protection law. The signature counter does not have to be unambiguous, however, which means that it may be expedient to reset the signature to 0 automatically when a relatively low value, e.g. 50, is attained, according to the user's requirements. In certain circumstances, a user may also consider internal recording of the signature counter on his signature key carrier to be adequate, cf. S-CHIP 7.5.

- Indicator to specify whether authentication has taken place for the technical component which has sent the data to be signed; when authentication has taken place, the identification code for this component or the indicator to specify the class to which this technical component belongs (e.g. manufacturer's indicator) is affixed.

- Total number of signatures affixed since the last authentication by the signature key holder (if variable within the meaning of the explanatory note on § 16 (2) SigV, cf. also above note on signature counter)

- Mode of authentication by the signature key holder (if variable, e.g. with or without biometric attributes)

- Incorporation of a random number into the signing algorithm for RSA signatures; see REQ-CHIP 1.2.

- Time of creation (if feasible)

- What is meant here is not a time stamp within the meaning of the Digital Signature Act, but a trustworthy system time of a security box, for example, cf. S-SBOX 1.24.

- The certificate (if it is installed on the signature key carrier, see also above) or at least an unambiguous indicator for the certificate.

In order to provide the verifying party with definite confirmation that these data objects have been affixed by the signature key carrier, it is necessary for the additional data objects to be appended to every data record which is to be signed. Such an arrangement will, of course, require the explicit consent of the signature key holder.

ISO/IEC 14888 'Digital signature with appendix' [ISO 14888] describes the basic procedure for incorporating data objects into a data record which is to be signed. When using RSA signatures in particular, the standard ISO/IEC 9796-2 'Digital signature schemes giving message recovery' permits the incorporation of data objects in such a manner that they do not have to be appended separately to the data which are to be signed, but are recovered automatically during verification of a signature.

## Literature

[ISO 9796-2] Digital signature schemes giving message recovery - Hash functions, ISO/IEC DIS

[ISO 14888] Digital signature with appendix, ISO/IEC CD

[PKIX] Internet Public Key Infrastructure, Internet drafts

- Web-based Certificate and CRL Repository
- Part 1: X.509 Certificate and CRL Profile
- Part 2: Operational Protocols
- Part 3: Certificate Management Protocols
- Part 4: Certificate Policy and Certification Practices Framework

[X.509v3] ITU-T Recommendation X.509, Information technology - Open Systems Interconnection - The directory: authentication framework, amendment 1: Certificate Extension, Final Draft 1996

# 4. Procedures

The aim of chapter 4 is to provide the reader of the safeguard catalogues with an initial insight into the organisational procedures which apply to the individual activities relating to the digital signature. To this end, all the procedures for the individual activities are presented from the point of view of both the provider and the user, on the one hand from the establishment of the required security infrastructure (certification authority) through the individual tasks performed at a certification authority to the functions of the directory service and the time stamping service, and on the other hand from registration of the user through to the generation and verification of a digital signature. The procedures are presented in canonical form, with flow diagrams also to be included in future. These procedures relate to the proposals for solutions which are specified in subsequent chapters and are thus not necessarily applicable to other approaches to solving the problems concerned.

A detailed specification of the procedural structures will be incorporated into the next version of the safeguard catalogues, after consulting users and experts from trade and industry and the science sector. The current state of progress is already accessible to interested members of the public as a basis for discussion on the BSI's webpage, http://www.bsi.bund.de.

# 5 Safeguard Catalogue in Accordance with § 12 (2) SigV

In accordance with § 12 of the Digital Signature Ordinance, every certification authority is required to draft a security concept containing all adopted security safeguards, an overview of deployed technical components and a presentation of all relevant procedures. This chapter presents the requirements which apply in this area and describes safeguards and procedures which are to be observed.

## 5.1 Requirements stipulated in the Act and the Ordinance

| Reference | Quotation | Interpretation |
|---|---|---|
| **§ 1 (1) SigG** | The purpose of this Act 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. | This is a general security clause to which the entire scope of security requirements can be traced back..<br>Derived requirements: REQ-SICO 4, REC-SICO 4, REC-SICO 5, REC-SICO 7 |
| **Explanatory note on § 2 (3) SigG** | Attribute certificates belong to the signature key certificate and are to be treated in the same manner as the latter. | Security requirements for signature key certificates are thus directly applicable to attribute certificates.<br>Derived requirement: REQ-SICO 5. |
| **§ 4 (3) sentence 2 SigG** | The required specialised knowledge shall be deemed available when the persons engaged in the operation of the certification authority have the necessary knowledge, experience and skills. | This is a criterion for personnel selection.<br>Derived requirements: REQ-SICO 44, REC-SICO 6. |
| **§ 4 (3) sentence 3 SigG** | The other requirements pertaining to operation of the certification authority shall be deemed met when the competent authority has been notified in a timely manner by means of a security concept of the safeguards ensuring compliance with the security requirements in this Act and the ordinance having force of law pursuant to § 16 and their implementation has been checked and confirmed by a body recognised by the competent authority. | This provision calls for a security concept and implementation of the safeguards specified therein.<br>Derived requirement: REQ-SICO 37. |

| | | |
|---|---|---|
| **Explanatory note on § 4 (5) SigG** | The certification authority may issue the 'root certificate' to the signature key holder concerned in authentic manner, together with his own certificate (storage on the data carrier with the signature key). | Issue of the root certificate is recommended, signifying an additional function for the personalisation service / the RA.<br>Authentic verification of chains of certificate can be performed with the aid of the root certificate.<br>If the root certificate is handed over, authenticity is to be ensured.<br>Derived requirements: REC-SICO 2, REQ-SICO 22. |
| **Explanatory note on § 4 (5) SigG** | The signature keys certified by the competent authority are intended exclusively for signing certificates and, where necessary, for signing time stamps. | The scope of application of the CA signature keys is restricted.<br>Derived requirements: REQ-SICO 1, REQ-SICO 35. |
| **Explanatory note on § 4 (5) SigG** | [...] any number of customer service centres (at which the applications for certificates are accepted, the applicants are identified and informed in accordance with $ 6 and the certificates are, where appropriate, handed over); they may also be affiliated by means of cooperation agreements. | Provision is allowed for the operation of decentralised security structures with branch RAs.<br>Derived requirement: REC-SICO 1. |
| **§ 5 (1) sentence 1 SigG** | The certification authority shall reliably establish the identity of persons applying for a certificate. | This provision requires the RA and a reliable identification mechanism.<br>Derived requirements: REQ-SICO 6, REQ-SICO 16. |
| **§ 5 (1) sentence 2 SigG** | It *(the certification authority)* shall confirm the assignment of a public signature key to an identified person by a signature key certificate which, together with any attribute certificates, shall be kept available for verification and, with the consent of the holder of the signature key, for retrieval at all times and for everyone over publicly available telecommunication links. | This calls for the CA, the directory service, and a certificate-based security infrastructure.<br>The directory service is obliged to accept contracts.<br>Certificates which are not available for retrieval are to be treated confidentially.<br>Derived requirements: REQ-SICO 6, REQ-SICO 14, REQ-SICO 41. |
| **Explanatory note on $ 5 (1) sentence 2 SigG** | The certificate shall, however, be disclosed only with the express consent of the holder of the signature key. | On request from the user, the confidentiality of a certificate must be safeguarded by explicit safeguards.<br>Derived requirement: REQ-SICO 41. |

| | | |
|---|---|---|
| **§ 5 (2) SigG** | At an applicant's request the certification authority shall include in the signature key certificate or an attribute certificate information relating to his authority to represent a third party and to his professional admission to practice or other type of admission insofar as reliable proof is furnished of the consent by the third party to the inclusion of the authority of representation or of the admission. | This function is obligatory and signifies additional functions in the area of the RA.<br>Derived requirement: REQ-SICO 8. |
| **§ 5 (3) SigG** | At an applicant's request the certification authority shall indicate a pseudonym instead of the applicant's name in the certificate. | This function is obligatory and signifies additional functions in the area of the RA.<br>Derived requirement: REQ-SICO 9. |
| **Explanatory note on § 5 (3) SigG** | In accordance with § 7 subsection 1 no. 1, pseudonyms are to be identified as such [...] | Pseudonyms must be identifiable via special entries in the certificate.<br>Derived requirement: REQ-SICO 9. |
| **§ 5 (4) SigG** | The certification authority shall take safeguards to prevent undetected forgery or manipulation of the data intended for certificates.<br>It shall also take safeguards to ensure confidentiality of private signature keys. Storage of private signature keys by the certification authority shall not be permitted. | The integrity of the certificates, the confidentiality and uniqueness of the private signature keys are to be ensured via personnel, organisational and technical safeguards.<br>Derived requirements: REQ-SICO 40, REQ-SICO 45, REQ-SICO 49. |
| **Explanatory note on $ 5 (4) SigG** | Above all, this requires repeated internal controls (e.g. comparison of certificates and certification applications via random sampling). | The form of documentation in accordance with § 10 SigG must enable such reviews.<br>The post of 'Revisor' must be installed within a certification authority.<br>Derived requirements: REQ-SICO 10, REQ-SICO 49. |
| **Explanatory note on § 5 (4) SigG** | As the possibility of corruptions of data due to technical reasons in particular cannot be excluded, such corruptions must be noted automatically at least. | The automatic detection of such corruptions requires special technical safeguards.<br>Derived requirement: REQ-SICO 50. |
| **Explanatory note on § 5 (4) SigG** | When the holder of the signature key generates the key himself, it *(the certification authority)* is to verify that he uses a suitable method which provides adequate safeguards against disclosure of the key. | In principle, the employed method is suitable when a tested and confirmed component is used. The RA can thus check for use of such a component (cf. chapter 6.3).<br>Derived requirement: REQ-SICO 13. |

| | | |
|---|---|---|
| **§ 5 (5) sentence 1 SigG** | The certification authority shall engage reliable staff for the exercise of certification activities. | This is a criterion for the selection of personnel. The aspect of reliability relates equally to technical competence and to repute, police records, debts, etc.<br>Derived requirements: REQ-SICO 44, REC-SICO 6. |
| **§ 5 (5) sentence 2 and 3 SigG** | For the provision of signature keys and the issue of certificates it shall use technical components as set out in § 14. This shall also apply to technical components enabling verification of certificates according to § 5 (1) sentence 2 above. | No other technical components may be used.<br>Derived requirement: REQ-SICO 48. |
| **§ 6 SigG** | The certification authority shall notify applicants according to § 5(1) of the safeguards necessary to support secure digital signatures and their reliable verification. It shall notify applicants of the technical components meeting the requirements of § 14(1) and (2) and of the assignment of digital signatures generated by a private signature key. It shall advise applicants that data bearing a digital signature may need to be signed again before the security of the existing signature decreases with time. | Notification of the applicants is required.<br>Special requirements are imposed with regard to the quality of information by the codicil 'to support secure digital signatures and their reliable verification'.<br>Derived requirement: REQ-SICO 23. |

| | | |
|---|---|---|
| **§ 7 (1) and (3) SigG** | (1) The signature key certificate shall contain the following information:<br>1. name of the holder of the signature key to which additional information must be appended in the event of possible confusion, or a distinctive pseudonym assigned to the holder of the signature key, clearly marked as such,<br>2. public signature key assigned,<br>3. names of the algorithms with which the public key of the holder of the signature key and the public key of the certification authority can be used,<br>4. serial number of the certificate,<br>5. beginning and end of the validity period of the certificate,<br>6. name of the certification authority, and<br>7. an indication as to whether use of the signature key is restricted in type or scope to specific applications.<br>(3) Further information shall not be included in the signature key certificate unless the parties concerned give their consent. | The contents of signature key certificates are stipulated in explicit terms. Any parameters beyond those stated in subsection 1 (including control parameters) shall require the consent of the party concerned.<br>Derived requirements: REQ-SICO 11, REQ-SICO 19, REC-SICO 2. |
| **Explanatory note on § 7 (1) SigG** | The provision in (1) is intended to ensure that each signature key holder bears a unique name in the directory of a certification authority. | Each user name at a certification authority is unique. Distinction on the basis of the serial number of the user's certificate alone is not sufficient.<br>Derived requirement: REQ-SICO 11. |
| **Explanatory note on § 7 (2) SigG** | It is also possible for several signature key certificates and attribute certificates to be issued for the same signature key by different certification authorities. | Unambiguous assignment is achieved only via combination with the unique name of the CA and a serial number for the certificate.<br>If the certificate or an unambiguous reference to the certificate is not incorporated when creating a signature, the 'double certification' of signature keys will lead to misunderstandings, however.<br>Derived requirement: REQ-SICO 15. |

| | | |
|---|---|---|
| **§ 8 (1) sentence 1 SigG** | The certification authority shall revoke a certificate when the holder of a signature key or his representative so requests, when the certificate was obtained through false statements in respect of § 7, when the certification authority ceases operation and its activity is not continued by another certification authority or when revocation is ordered by the competent authority pursuant to § 13(5) sentence 2. | Revocation management is required here.<br>The conditions under which revocation may be effected are stipulated in explicit terms.<br>Derived requirement: REQ-SICO 27. |
| **§ 8 (1) sentence 2 SigG** | The revocation shall indicate the time at which it enters into effect. | This is a requirement relating to the contents of the revocation entry.<br>Derived requirement: REQ-SICO 29. |
| **§ 8 (1) sentence 3 SigG** | Retrospective revocation shall not be permitted. | This requirement relates to revocation management procedures.<br>Derived requirement: REQ-SICO 29. |
| **§ 8 (2) SigG** | Where a certificate contains third party information, this party may also request revocation of the certificate. | This is a further condition under which revocation may be imposed.<br>Derived requirement: REQ-SICO 27. |
| **Explanatory note on § 8 SigG** | When a signature key certificate is revoked, all appurtenant attribute certificates are revoked accordingly. Attribute certificates can be revoked separately. See also explanatory note on § 5 subsection 2.<br>The validity of the digital signatures generated prior to the time of revocation is not affected by the revocation. In cases of doubt, a time stamp provides definite confirmation as to whether a signature was generated before or after the revocation (cf. § 9). | These are requirements which relate to revocation management procedures.<br>When the time of creation of a signature cannot be ascertained subsequently without doubt, a time stamp is obligatory, when the validity of the signatures is to be maintained after a possible revocation.<br>This applies in the same manner for the signature of a certification authority under a user's certificate, should the signature key certificate of the certification authority be revoked by the competent authority.<br>Derived requirements: REQ-SICO 30, REQ-SICO 31. |

| | | |
|---|---|---|
| **Explanatory note on § 8 (1) SigG** | The subsequent generation of digital signatures for backdated data cannot be prevented by revocation. This is prevented by a time stamp. The Ordinance provides for the holders of signature keys to be notified as to when a time stamp is necessary. The signed signature key certificates themselves contain information on the beginning and end of their validity periods (cf. § 7 subsection 1 no. 5). The supplementary Ordinance further provides for the time of drafting and issue of the certificates to be documented by the certification authority. | In order to confirm beyond doubt that an affixed digital signature was generated prior to a possible future revocation a time stamp is required, if the time of generation of the signature cannot be proven beyond doubt in another manner. In particular, it must be possible in the course of signature verification to ascertain directly whether the time of issuing the corresponding certificates is prior to or after the time of revocation. When the time of generation of a signature is not confirmed beyond doubt, digital signatures lose their validity after revocation of the corresponding key certificate. This is, however, acceptable in the case of digital signatures, the relevance of which is of only short duration. The relevance of digital signatures under key certificates is never of short duration.<br><br>This is a requirement concerning documentation and relates to the contents of the documentation.<br><br>Derived requirements: REQ-SICO 20, REQ-SICO 31. |
| **§ 9 SigG** | Upon request the certification authority shall affix a time stamp to digital data. § 5 (5) sentences 1 and 2 shall apply mutatis mutandis. | This provision calls for action by the time stamping service.<br><br>Derived requirement: REQ-SICO 6. |
| **Explanatory note on § 9 SigG** | The allocation of time stamps (cf. § 2 subsection 4) is to be stipulated as an obligatory service for certification authorities, as time stamps are essential when using digital signatures whenever it is possible that the question as to whether data existed at a certain point in time may acquire evidentiary importance. | The attachment of a time stamp is compulsory at least in cases in which data may acquire evidentiary importance.<br><br>Derived requirement: REQ-SICO 6. |
| **Explanatory note on § 9 SigG** | A time stamp may be requested by anyone who generates data or is in possession of data from third parties and who has an interest in a time stamp for reasons of evidence in connection with such data. | The time stamping service is obliged to accept contracts.<br><br>Derived requirement: REQ-SICO 7. |

| | | |
|---|---|---|
| **Explanatory note on § 9 SigG** | The provision in sentence 2 is intended to establish the same personnel-related and technical security for the generation of time stamps as applies to the generation of certificates. | The attachment of time stamps requires the same security safeguards as apply to the generation of key certificates.<br>Derived requirements: REQ-SICO 45, REQ-SICO 5. |
| **§ 10 SigG** | The certification authority shall document the security safeguards for compliance with this Act and the ordinance having the force of law pursuant to § 16 and the certificates issued in a manner such that the data and their integrity can be verified at all times. | This is a stipulation for the area of documentation and concerns reprocessing of the contents of documents.<br>Derived requirement: REQ-SICO 33. |
| **§ 12 (2) SigG** | Where the holder of a signature key uses a pseudonym, the certification authority shall be obliged to communicate, upon request, to the competent bodies any data pertaining to his identity which is required for the prosecution of criminal or administrative offences, for averting danger to public safety or order or for the discharge of statutory duties by the Federal and State authorities for the protection of the Constitution, the Federal Intelligence Service [*Bundesnachrichtendienst*], the Military Counter-Intelligence Service [*Militärischer Abschirmdienst*] or the Customs Criminological Office [*Zollkriminalamt*]. Such disclosures shall be documented. | In certain cases the CA is obliged to provide information on pseudonyms which are otherwise to be treated confidentially.<br>This is a stipulation for the area of documentation and concerns reprocessing of the contents of documents.<br>Derived requirements: REQ-SICO 25, REC-SICO 5, REQ-SICO 32. |
| **Explanatory note on § 14 (1) SigG** | When key generation is effected externally, loading of the chipcard with the private key can be configured in technical and organisational terms (dual control principle) in such a manner as to reliably safeguard the uniqueness and secrecy of the private signature key here also. | The dual control principle for personalisation / prepersonalisation is recommended. If this principle is not applied, an equivalent level of security must be achieved by other technical or organisational safeguards.<br>Derived requirements: REQ-SICO 39, REQ-SICO 40. |

| | | |
|---|---|---|
| **Explanatory note on § 14 (3) SigG** | The certificate directories must be protected above all from the unauthorised revocation of certificates and the removal of revocations. If the holder of the signature key has not consented to his certificate being available for retrieval via public networks (cf. § 5 (1)), it must also be protected against unauthorised retrieval (authorised retrieval for internal purposes of the certification authority remains unaffected). | Unauthorised revocation applies when not at least one of the conditions specified in § 8 (1) sentence 1 SigG is fulfilled.<br><br>The certificates which are not available for public retrieval are subject to special requirements with regard to their confidentiality and must be protected accordingly.<br><br>Derived requirements: REC-SICO 3, REQ-SICO 39, REQ-SICO 40. |
| **§ 14 (4) SigG** | Technical components according to § 14 (1) to (3) above shall be adequately tested against current engineering standards and their compliance with requirements confirmed by a body recognised by the competent authority.. | No other components may be used.<br><br>Derived requirements: REQ-SICO 13, REQ-SICO 48. |
| **§ 3 (1) SigV** | Pursuant to § 5 (1) Sentence 1 of the Digital Signature Act, the certification authority shall establish the identification of the applicant by means of the applicant's personal identity card or passport, or by other suitable means. The applicant must personally sign the application for a certificate in his own hand. If an application for a certificate bears a digital signature of the applicant, the certification authority is not bound to require additional identification and a hand-written signature in the applicant's own hand. | The procedures for submitting applications and identification of the users are stipulated.<br><br>Identification via another suitable means must provide a comparable standard of security.<br><br>Identification serves to ascertain the actual identity, while the personal signature is intended to prevent misuse by the staff of the certification authority and to facilitate the detection of forged identity papers.<br><br>Digitally signed applications are only accepted from users who have already been identified at this certification authority by 'conventional' means. Identification at a different CA involves renewed identification. If 'conventional' identification were to be waived in this case, a user could pose as someone who shares his name, as the exchange of user data between certification authorities is not permissible as standard practice.<br><br>Derived requirements: REQ-SICO 16, REQ-SICO 18. |

| | | |
|---|---|---|
| **Explanatory note on § 3 (1) SigV** | Identification (sentence 1) may also be carried out by local registration offices of the certification authority. Identification 'by other suitable means' requires a comparable standard of security.<br><br>In conjunction with the identification in accordance with sentence 1 and documentation in accordance with § 13 (1) (copy of the presented proof of identify), the personally signed application for a certificate (sentence 2) constitutes an important item of evidence in cases of suspected forgery of a certificate (e.g. by untrustworthy employees of the certification authority or as a result of presentation of a forged identity card by the applicant). In order to enable effective comparison of the signature on the identity card and on the application, the application must be signed at the registration office. | Provision is allowed for the operation of decentralised security structures with branch RAs.<br><br>Identification by other appropriate means must provide a comparable standard of security.<br><br>Identification serves to ascertain the actual identity, while the personal signature is intended to prevent misuse by the staff of the certification authority and to facilitate the detection of forged identity papers.<br><br>Derived requirements: REC-SICO 1, REQ-SICO 16, REQ-SICO 18. |
| **§ 3 (2) SigV** | If, pursuant to § 5 (2) of the Digital Signature Act, information relating to the applicant's authority to represent a third party is to be included in a certificate, such representative authority must be reliably proven, and consent of said third party, in writing or containing a digital signature, must be provided.<br><br>The third party shall be informed, in writing or by electronic message containing a digital signature, about the contents of the certificate and about the possibility for revocation pursuant to § 8 (1). Possession of any professional license or other license must be proven through submission of the relevant license document. | Information in certificates on third parties is to be checked with regard to content and due consent. The third parties concerned are to be notified.<br><br>Derived requirements: REQ-SICO 8, REQ-SICO 24. |
| **Explanatory note on § 4 SigV** | The required notification is intended to enable the applicant, as a future signature key holder, to undertake the safeguards which are necessary on his part in order to generate secure digital signatures, to verify digital signatures in a reliable manner and to prevent misuse of his signature key by unauthorised parties and the signing of false data. | Special requirements apply to the quality of notification, as the applicant is to be 'enabled... ' by means of the notification.<br><br>Derived requirement: REQ-SICO 23. |

| | | |
|---|---|---|
| **Explanatory note on § 4 (1) no. 1 SigV** | The provision in (1) no. 1 is intended to provide additional protection to prevent misuse of the signature key. This requirement can be fulfilled by the certification authority carrying out destruction in an appropriate manner (e.g. of chip cards with signature keys). | The destruction of signature keys in an appropriate manner is an optional service.<br>Derived requirement: REC-SICO 8. |
| **§ 4 (1) no. 5 SigV** | If a particular time can be of considerable significance with regard to use of signed data, a time stamp shall be appended. | A time is always of significance for the use of signed data when the digital signature belonging to these data is to remain valid in the event of revocation of the user certificate or a higher-priority certificate due to compromise of the key.<br>A time stamp also requires to be appended (from the point of view of the verifying party) when the verifying party wishes to ensure that the signing party will not be able to deny the signature at a later juncture via subsequent revocation of his certificate (non-repudiation of origin).<br>It is thus essential that a time stamp be appended to certificates by the CA or the competent authority whenever the validity of digital signatures and/or of user certificates is to remain unaffected by a revocation on the corresponding certification path, insofar as the time of generation of the signature under the certificate cannot be confirmed beyond doubt by other means and in a manner which is verifiable at all times.<br>Derived requirement: REQ-SICO 31. |
| **Explanatory note on § 4 (1) no. 5 SigV** | The question as to whether a particular time is of 'considerable significance' with regard to the use of signed data (no. 5) must be examined in each individual case. A time stamp is necessary for new digital signatures, for example (cf. § 18). | See above.<br>Derived requirement: REQ-SICO 31. |

| | | |
|---|---|---|
| **§ 4 (1) no. 7 SigV** | In verification of digital signatures, it shall be determined whether the signature key certificate and attribute certificates were valid at the time the signature was generated, whether the signature key certificate contains restrictions pursuant to § 7 (1) No.7 of the Digital Signature Act and whether Numbers 4 and 5 were complied with, if applicable. | The time of signature generation must be known without any doubt, in order to carry out verification, unless the corresponding certification path is still completely valid and the generation of a signature prior to the period of validity of the user certificate presents absolutely no grounds for objection.<br>Derived requirement: REQ-SICO 31. |

| | | |
|---|---|---|
| **Explanatory note on § 4 (1) No. 7 SigV** | Verification of the validity of certificates in accordance with Number 7 includes checking the digital signatures which belong to the certificates. It is left to the discretion of the person verifying the signature to decide whether the certificates should additionally be verified via the appropriate public directory of certificates (whether they are registered there and were valid at the time of generation of the signature). | Verification of the complete certification path in relation to the time of generation of the signature concerned is obtained via a process of recursion:<br><br>A document signature is valid when it is mathematically correct and the corresponding user certificate was valid at the time of generation of the document signature. The user certificate was valid if the said time is within the validity period of the certificate, the CA signature under the certificate is mathematically correct and the corresponding CA certificate was valid at the time of generation of the certificate signature. This CA certificate was valid if the time of generation of the certificate signature is within the validity period of the CA certificate, the signature of the competent authority under the CA certificate is mathematically correct and the corresponding certificate of the competent authority was valid at the time of generation of the CA certificate signature. This certificate of the competent authority was valid if the time of generation of the CA certificate signature is within the validity period of the certificate of the competent authority's certificate and the signature of the competent authority under its own certificate is mathematically correct.<br><br>When practices which differ from the procedure in accordance with RFC 1422 for the verification of certificate paths are adopted, it is imperative that a verification of interlinked times be carried out in accordance with the method outlined above.<br><br>Derived requirement: REQ-SICO 31. |
| **§ 5 (1) SigV** | If the signature key holder generates signature keys, the certification authority shall reliably establish whether the signature key holder uses suitable technical components, pursuant to the Digital Signature Act and this Ordinance, for storage and use of the private key signature. | Tested and confirmed components are suitable as a general principle.<br><br>Derived requirement: REQ-SICO 13. |

| | | |
|---|---|---|
| **§ 5 (2) SigV** | If the certification authority provides signature keys, this authority shall take precautions to prevent any disclosure of private keys and any storage of private keys by the certification authority. Similar precautions shall also apply to personal identification numbers and other data used to identify the signature key holder in conjunction with the data storage medium with the private signature key. | The storage of private signature keys and authentication parameters for the signing components must not be possible at the CA.<br><br>Derived requirement: REQ-SICO 39. |
| **Explanatory note on § 5 (2) SigV** | This provision is intended to prevent the disclosure or storage of keys or identification data at the certification authority. If the possibility of disclosure cannot be fully excluded, any disclosures must be ascertainable at least. The checks stipulated in § 15 already provide for verification of the suitability of the technical components employed by a certification authority for generation of the keys. Storage of the private signature key outside of the provided key data storage medium is already precluded by the technical components (cf. § 16 subsection 1). | When implementations are possible which enable the compromise of keys or authentication parameters to be ascertained without any doubt, the prevention of disclosure is not absolutely imperative.<br><br>Derived requirements: REQ-SICO 39, REQ-SICO 51. |
| **§ 6 SigV** | If the certification authority provides signature keys or identification data pursuant to § 5 (2), it shall hand over the private signature key and the identification data to the signature key holder in person and shall obtain written confirmation of such handover from the signature key holder, unless the signature key holder requests a different handover procedure in writing. Upon handing over the private signature key or signature key certificate, the certification authority shall also hand over the public signature key to the competent authority. | As a general rule, the signing component is to be handed over personally and a receipt is to be issued.<br><br>Other modes of handover require an equivalent level of security.<br><br>Derived requirements: REQ-SICO 20, REQ-SICO 21, REQ-SICO 22, REQ-SICO 40, REQ-SICO 46. |

| | | |
|---|---|---|
| **Explanatory note on § 6 SigV** | The provision in sentence 1 is intended to ensure reliable handover of the private signature keys and identification data. Another possible form of handover, for example, would be formal service to the signature key holder in person, in accordance with the German Code of Civil Procedure, insofar as the prospective signature key holder requests this mode of handover and thus accepts any attendant risks.<br><br>The signature key holder requires the public key of the competent authority (sentence 2) in order to enable verification, if necessary, as to whether the certificates concerned originate from a certification authority pursuant to § 4 of the Digital Signature Act. The public key of the competent authority is also to be handed over if the signature key holder generates his keys himself and receives only one certificate from the certification authority. | Reliable handover means that only the entitled recipient is able to acquire possession of the signing component and the appurtenant authentication data.<br><br>Should the user request a mode of handover or service which does not ensure reliable handover, such a request must be refused.<br><br>Derived requirements: REQ-SICO 21, REQ-SICO 22, REQ-SICO 40, REQ-SICO 46. |
| **§ 7 SigV** | The validity period for a certificate shall be no longer than five years and shall not exceed the period during which the applied algorithms and pertinent parameters pursuant to § 17 (2) remain suitable. The validity of an attribute certificate terminates at the latest with the validity of the signature key certificate to which it refers. | As the suitability of the algorithms is confirmed for the next six years, a certificate over the maximum period of validity is possible at all times.<br><br>Derived requirements: REQ-SICO 2, REQ-SICO 30. |

| | | |
|---|---|---|
| **Explanatory note on § 7 SigV** | The limited period of validity for signature key certificates in accordance with sentence 1 arises as a result of the fact that secure and reliable evaluation of the cryptographic methods for digital signatures is possible for a limited period only (cf. explanatory note on § 17 subsection 2). The signature key holder must furthermore be able to rely on the fact that the algorithms and appurtenant parameters specified in the certificate possess the required suitability for the period of validity of the certificate. In order to avoid the need to affix a new digital signature to the certificate pursuant to § 18 (should the suitability of the employed algorithms and parameters lapse prior to expiry of the period of validity for the certificate), the certification authority must also take due account of the security of these algorithms and parameters when issuing certificates. | The CA must not use any algorithms to sign the certificates whose security is not confirmed beyond the period of validity of the certificate to be signed.<br>Derived requirement: REQ-SICO 3. |
| **§ 8 (1) SigV** | (1) The certification authority shall keep certificates issued by it within a register, pursuant to the provisions of § 5 (1) Sentence 2 of the Digital Signature Act; a certificate shall be kept in such directory for at least as long as the algorithm listed in the certificate and its pertinent parameters are considered suitable pursuant to § 17 (2). | As long as the suitability of an algorithm is not revoked, the certificates are to be kept permanently available on line.<br>Derived requirement: REQ-SICO 34. |

| | | |
|---|---|---|
| **Explanatory note on § 8 (1) SigV** | In order to organise the verification of digital signatures in the most practical manner possible, particularly when large-scale applications are involved (e.g. at banks or department stores), the certification authorities can keep all relevant certificates (including those of the competent authority and any foreign bodies)available for verification on a centralised basis, by means of an integrated network of its registers of certificates. In order to avoid repeated on-line inquiries, revocation lists and new revocations can be transmitted automatically to major users, who will then require only to check this information against the data in their own computers. The certification authorities are free to draft corresponding commercial offers. | An integrated network of directory services includes the corresponding revocation management.<br>Derived requirement: REQ-SICO 43. |
| **§ 8 (3) SigV** | At the end of the period mentioned in (1), the certification authority and the competent authority shall permit repeat verification of the certificates upon application in individual cases; such repeat verification shall remain possible until the end of the period mentioned in § 13 (2). | The certificates are to be kept available until the end of the period stated in § 13 (2).<br>Derived requirement: REQ-SICO 33. |
| **§ 9 (1) SigV** | The certification authority shall provide to the signature key holders, to third parties for whom information relating to representative authority has been included in a certificate and to the competent authority a telephone number at which they can arrange for immediate revocation of the certificates, at any time; the certification authority shall also provide an authentication procedure for this purpose. | This provision regulates access to the revocation management system.<br>The telephone revocation service must be manned 'around the clock'. This does not exclude the possibility of a home-based emergency service, provided that an immediate response is possible.<br>Derived requirements: REQ-SICO 24, REQ-SICO 26, REQ-SICO 27. |

| | | |
|---|---|---|
| **Explanatory note on § 9 (1) SigV** | This provision serves to protect the signature key holders and third persons whose information relating to representative authority has been included in a certificate. The requirement for the provision of a telephone number is intended to enable immediate revocation, as contact via telephone is possible at practically any time. The CA remains free to provide the numbers of other telecommunications connections (e.g. fax). An appropriate authentication method is the password method, for example. | The telephone revocation service must be manned 'around the clock', as immediate revocation must be possible.<br>Derived requirements: REQ-SICO 20, REQ-SICO 26. |
| **§ 9 (2) SigV** | The certification authority shall revoke a certificate, in keeping with the prerequisites of § 8 of the Digital Signature Act, if it has received a relevant application, either containing a digital signature or in writing, from the signature key holder, his representative, or an authorised third party pursuant to (1) or if an agreed authentication procedure has been used for this purpose. | This provision stipulates how a legitimate application for revocation can be identified.<br>Derived requirement: REQ-SICO 28. |
| **§ 9 (3) SigV** | Revocation of certificates must be clearly indicated, with inclusion of the relevant date and time, in the directory pursuant to § 8 of the Digital Signature Act, and may not be rescinded. | This requirement relates to the contents of a revocation entry and access to revocation entries.<br>Derived requirements: REQ-SICO 29, REQ-SICO 40. |
| **§ 10 SigV** | The certification authority shall reliably establish the reliability of persons involved in the certification procedure or in issuing time stamps. In particular, it may require presentation of a certificates of good conduct pursuant to § 30 (1) of the Federal Central Directory Act. Unreliable people shall be excluded from the certification procedure and from issuance of time stamps. | The certification process covers all procedures, from application for a certificate, identification, key generation, key certification, personalisation, operation of the directory and time stamping service, handover of the signing component, through to the subsequent documentation.<br>Derived requirements: REQ-SICO 44, REC-SICO 5, REC-SICO 6. |

| | | |
|---|---|---|
| **§ 11 SigV** | The certification authority shall take precautions to protect the following from unauthorised access: private signature keys, and the technical components used to prepare the certificates and time stamps and to ensure that certificates can be checked at any time. | This provision requires protection of the technical components via personnel-related, organisational and infrastructural security safeguards.<br><br>Derived requirements: REQ-SICO 40, REQ-SICO 45, REQ-SICO 46, REQ-SICO 47, REC-SICO 4, REC-SICO 8. |
| **Explanatory note on § 11 SigV** | Protection of the technical components against unauthorised access is intended to prevent possible technical manipulations. Unauthorised access (in either physical or logical form, e.g. via communications networks) must at least be detected prior to renewed use, so as to enable replacement or checking of the technical components.<br><br>The data storage media containing private signature keys which are used to sign certificates or time stamps must also be protected against misappropriation, in order to prevent possible misuse. | If protection of the technical components cannot be ensured, unauthorised accesses must be detected automatically at least.<br><br>Derived requirements: REQ-SICO 45, REQ-SICO 47, REQ-SICO 52. |
| **§ 12 (1) SigV** | The security concept pursuant to § 4 (3) Sentence 3 of the Digital Signature Act shall include all security safeguards and, especially, an overview of the technical components used and a description of the procedures used in certification.<br><br>The concept shall be changed without delay in cases of security-relevant changes. | This provision requires a security concept with specific contents and an appurtenant system of change management.<br><br>Derived requirements: REQ-SICO 37, REQ-SICO 38, REC-SICO 4. |

| | | |
|---|---|---|
| **Explanatory note on § 12 (1) SigV** | The security concept is to provide a comprehensive overview of the security safeguards at the certification authority. Above all, the organisational structure must specify how the signature keys used to sign the certificates and time stamps are protected against unauthorised use and misappropriation. High importance is also attached to the safeguards to protect the data which is intended for a certificate against forgery and manipulation and, in those cases in which the certificates are to be kept available for verification only, and not available for retrieval, in accordance with the wishes of the party affected, high priority is attached to the safeguards to safeguard confidentiality. To this end, the data can, for example, be signed and encoded for the purposes of on-line transmission between the offices receiving applications for certificates and the central office concerned (cf. explanatory note on § 3 subsection 1).<br><br>A certification authority requires the following technical components at least: A signing component (e.g. chipcard) and a PC for generating certificates/time stamps, and a server for the directory of certificates pursuant to § 8. According to requirements, technical components for generating and loading signature keys and identification data and a special server for time stamps may also be necessary. cf. explanatory note on § 16 with regard to suitability of the technical components. | The security concept includes branch offices and - where possible - additionally offered services.<br><br>Protection requirement, weak-point, threat and risk analyses are integral elements of the security concept.<br><br>Derived requirement: REQ-SICO 38. |

| | | |
|---|---|---|
| | Discharge of the certification authority's duties can be organised in various ways (including cooperation agreements), provided that transparency is maintained and compliance with the Digital Signature Act and the Digital Signature Ordinance is guaranteed. Overall responsibility lies with the individual operator (cf. also explanatory note on § 1 subsection 2). When necessary, the competent authority may impose conditions on the operating licence.<br><br>When, in addition to the compulsory services (issuance of certificates and of time stamps), the certification authority offers further services on a contractual basis in connection with digital signatures (e.g. verification of digital signatures with foreign algorithms and parameters), these additional services should also be incorporated into the security concept.<br><br>The security concept also includes presentation of the specific threats and risks which apply at the certification authority. General threats and risks are already taken into consideration in the detailed security requirements stipulated in the Digital Signature Act and the Digital Signature Ordinance, and in the safeguard catalogues pursuant to § 12 subsection 2 and § 16 subsection 6. | |

| | | |
|---|---|---|
| **§ 13 (1) SigV** | The documentation pursuant to § 10 of the Digital Signature Act shall include the security concept, including the changes, the check reports and confirmations pursuant to § 15 (1), the contractual agreements with the applicants and the certificates received by the competent authority. The following records shall be kept for received applications for certificates and for agreements with the applicants: a photocopy of the submitted identity card or other proof of identity; the documents required for inclusion of information relative to third parties; any pseudonyms issued; proof of the required notification of the applicant and third parties; the issued certificates, including the relevant time of issuance and handover; revocation of certificates and information pursuant to § 12 (2) of the Digital Signature Act. If the certification authority provides signature keys or identification data pursuant to § 5 (2), a record shall be kept of the time of the relevant handover, along with a confirmation of the handover. Records kept in digital form must be digitally signed. | The contents of the documentation are specified.<br><br>A separate signature key is required for signing the records (cf. explanatory note on § 4 subsection 5 of the Digital Signature Act).<br><br>Derived requirements: REQ-SICO 12, REQ-SICO 17, REQ-SICO 20, REQ-SICO 32, REQ-SICO 35. |
| **Explanatory note on § 13 (1) SigV** | Documentation of the security safeguards is necessary in particular with regard to checks in accordance with § 13 Digital Signature Act and § 15 Digital Signature Ordinance. Documentation of other records is necessary, for example, in cases of suspected forgery of certificates. Beyond this, insofar as record data (e.g. relating to use of the private signature key of the certification authority) is generated automatically, the documentation of this data lies within the discretion of the certification authority.<br><br>The provision in the final sentence is intended to ensure that the documented data remains unmanipulated. A separate signature key is required for signing the records (cf. explanatory note on § 4 subsection 5 Digital Signature Act). | The documentation is to be drawn up in revisable form.<br><br>Derived requirements: REQ-SICO 10, REQ-SICO 35, REQ-SICO 36. |

| | | |
|---|---|---|
| **§ 13 (2) SigV** | The documentation pursuant to (1) must be kept for at least 35 years from the time of issue of the signature key certificate, and it must be stored in such a manner that it remains available throughout this period. Records of information pursuant to § 12 (2) Sentence 2 of the Digital Signature Act shall be kept for twelve months. | The requirements with regard to the preservation of documentation are stipulated.<br><br>Derived requirement: REQ-SICO 34. |
| **Explanatory note on § 13 (2) SigV** | Insofar as the documentation is produced in digital form (e.g. in the case of certificates), 'available' (sentence 1) includes verifiability, that is, suitable hardware and software must be available for this purpose. Retention periods of comparable length exist, for example, for 'digital documents' in the field of aircraft construction (50 years) or for the digital land register, which is maintained on a permanent basis. | The technical equipment which is required in order to reconstruct the electronic documentation must be kept available in operational condition for the same duration as the documentation.<br><br>Derived requirement: REQ-SICO 33. |
| **14 (2) and (3) SigV** | (2) Prior to cessation of its operation, the certification authority shall carry out the following for each certificate that has not been revoked and that will not have expired at the time of cessation of operation: notify the relevant signature key holder at least three months in advance that it plans to terminate its operation as a certification authority; inform him whether another certification authority will assume the certificate; and, if so, name this certification authority. If no other certification authority assumes the certificates, at the end of the period mentioned in (1) all certificates must be revoked that at this time are not already revoked or have not already expired. The signature key holders of the certificates subject to revocation shall be given relevant proper notification.<br><br>(3) The notification of the competent authority and the notification of the signature key holders shall be in digital (electronic) form, with a digital signature, or shall be in writing. | The user is to be notified of any revocations of certificates which he has not himself initiated. Where appropriate, safeguards must be implemented to provide him with new certificates in authentic form.<br><br>Derived requirement: REQ-SICO 30. |

| | | |
|---|---|---|
| **Explanatory note on § 16 (3) SigV** | [...] By means of an internal check using the public key of the regulatory authority, he is able to ascertain whether the certificate originates from an officially approved certification authority, and whether it was valid at the (stated or assumed) time of generation of the digital signature which requires to be verified, on the basis of the entries in the certificate. | The assumed time of signature generation is of relevance only when proof can be subsequently furnished that the assumption was correct.<br><br>Derived requirement: REQ-SICO 31. |
| **Explanatory note on § 16 (4) SigV** | Reliable verification of the authenticity of the information must also be possible, in order to eliminate the possibility of fake registers being use (so-called 'masquerade').<br><br>In order to prevent complete forgeries and to enable the identification of such at least, in addition to providing a statement concerning revocation, the information should also specify whether the certificate exists in the public directory of certificates. When this procedure is implemented, anyone wishing to put a complete forgery into circulation would not only have to draft a false certificate, but would also have to place this certificate in the directory and, with regard to possible checks, insert a forged application for a certificate in the documentation (which would subsequent provide evidence of the forgery). In the course of subsequent verification of a certificate, the user will then at least be able to ascertain whether the certificate exists in the directory (yes/no) and whether it was invalid at the stated time (of signature generation) (yes/no). With regard to revoked certificates, information on the date and time of revocation is also required. | The directory service must authenticate itself to the inquiring party.<br><br>Positive notification with regard to issued certificates renders misuse within the CA more difficult. This area thus requires special access control mechanisms for the directory service and revocation management.<br><br>The methods and procedures relating to information from the directory service are specified.<br><br>Derived requirements: REQ-SICO 29, REQ-SICO 42. |
| **Explanatory note on § 16 (5) SigV** | The technical components for generating time stamps are not expressly mentioned in § 14 Digital Signature Act. Their inclusion is inferred indirectly from § 9 Digital Signature Act in conjunction with § 14 Digital Signature Act. | Security requirements for the generation of signature key certificates are thus directly applicable to the generation of time stamp certificates.<br><br>Derived requirement: REQ-SICO 5. |

## 5.2 Security requirements and recommendations

### 5.2.1 General security requirements and security policy

REQ-SICO 1 The signature key of the CA may be used solely to produce user certificates or time stamp certificates.
cf.: Explanatory note on § 4 (5) SigG
Safeguards: S-SICO 3.1, S-SICO 3.4

REQ-SICO 2 The maximum permissible period of validity for certificates is five years and the period must be within the period of suitability of the employed algorithms.
cf.: § 7 SigV
Safeguards: S-SICO 3.1

REQ-SICO 3 The algorithms with which the CA signature is generated must be assessed as suitable over the period of validity of the user's certificate at least.
cf.: Explanatory note on § 7 SigV
Safeguards: S-SICO 3.1

REQ-SICO 4 The IT security concept of a certification authority must fulfil all the requirements laid down in the Act and the Ordinance in such a manner as to ensure that forgeries of digital signatures or manipulations of digital data can be reliably ascertained.
cf.: § 1 (1) SigG
Safeguards: All obligatory safeguards for the selected model, cf. Table in Section 5.4.3

REQ-SICO 5 Key certificates, time stamp certificates and attribute certificates are subject to the same security requirements.
cf. Explanatory note on § 2 (3) SigG, explanatory note on § 9 SigG
Safeguards: S-SICO 3.1, S-SICO 3.4, S-SICO 5.11

### 5.1.2 Functional security requirements for the CA

REQ-SICO 6 The CA must perform the following tasks at least:
1. registration and identification of the users (RA),
2. generation and provision of certificates (CA) which confirm the allocation of public keys to natural persons,
3. maintenance of a directory (including revocation management) which enables the verification of certificates,
4. affixing of time stamps to any appropriate data.

cf.: § 5 SigG, § 9 SigG and explanatory note on § 5 SigG, explanatory note on § 9 SigG
Safeguards: S-SICO 3.1, S-SICO 3.2, S-SICO 3.3, S-SICO 3.4, S-SICO 5.3

REQ-SICO 7 The time stamping service is obliged to accept contracts, as it must be available to everyone. Consequently, it must be generally accessible.
cf.: Explanatory note on § 9 SigG
Safeguards: S-SICO 3.6, S-SICO 5.15

REQ-SICO 8 The CA must incorporate entries in the certificate concerning authority to represent third parties and similar, after having verified the legality and correctness of the data relating to a third party and after having informed the third party accordingly.
cf.: § 5 (2) SigG, § 3 (2) SigV
Safeguards: S-SICO 3.1, S-SICO 5.11, S-SICO 6.4, S-SICO 6.5

REQ-SICO 9 On request, the CA is obliged to permit the use of a pseudonym instead of the user's name in the certificate, and to identify this pseudonym as such.
cf.: § 5 (3) SigG and explanatory note on § 5 (3) SigG
Safeguards: S-SICO 3.1, S-SICO 3.2, S-SICO 5.5, S-SICO 5.6

REQ-SICO 10 The CA is obliged to carry out controls or arrange for such controls to be carried out, in order to ensure that data for certificates cannot be forged or manipulated without detection.
cf.: Explanatory note on § 5 (4) SigG, explanatory note on § 13 (1) SigV
Safeguards: S-SICO 5.3, S-SICO 5.4, S-SICO 5.5, S-SICO 5.6,
S-SICO 5.7, S-SICO 5.10, S-SICO 6.3

REC-SICO 1 In the case of certification authorities operating over an extensive catchment area it is recommendable to operate several RAs on a decentralised basis.
cf.: Explanatory note on § 4 (5) SigG
Safeguards: S-SICO 3.1, S-SICO 3.2, S-SICO 6.7

### 5.2.3 Security requirements and recommendations for the registration authority

#### 5.2.3.1 Applications

REQ-SICO 11 An unambiguous name is to be issued for the user.
cf.: § 7 (1) no. 1 SigG
Safeguards: S-SICO 3.2, S-SICO 5.5, S-SICO 5.6

REQ-SICO 12 The user is to be registered.
cf.: § 13 (1) SigV
Safeguards: S-SICO 3.2, S-SICO 5.5, S-SICO 5.6,
S-SICO 6.3

#### 5.2.3.2 Submission of signing components with signature keys

REQ-SICO 13 In the case of keys generated by the user, the RA is to verify that suitable components approved and confirmed in accordance with § 17 have been / are used for storage and application of the private signature keys.
cf.: § 14 (4) SigG, explanatory note on § 5 (4) SigG, § 5 (1) SigV
Safeguards: S-SICO 5.5, S-SICO 5.6, S-SICO 6.4

REQ-SICO 14 The RA or CA must verify that the user key has not been allocated previously to any other users at the RA or CA concerned.
cf.: Explanatory note on § 5 SigG
Safeguards: S-SICO 5.5, S-SICO 5.6, S-SICO 5.9

REQ-SICO 15 The CA is not entitled to reject a submitted key on the grounds that a certificate of the same user already exists for the submitted key at a different CA.
cf.: Explanatory note on § 7 (2) SigG
Safeguards: S-SICO 5.9

#### 5.2.3.3 Identification

REQ-SICO 16 The identification of users must be carried out in a reliable manner.
cf.: § 5 (1) SigG and explanatory note on $ 5 (1) SigG, § 3 (1) SigV
Safeguards: S-SICO3.2, S-SICO 5.5, S-SICO 5.6, S-SICO 5.7

REQ-SICO 17 The ascertainment of and decision regarding identity is to be documented.
cf.: § 13 (1) SigV
Safeguards: S-SICO 3.2, S-SICO 5.7, S-SICO 6.3

REQ-SICO 18 It must not be possible for CA staff to simulate duly performed identification.
cf.: § 3 (1) SigV and explanatory note on § 3 (1) SigV
Safeguards: S-SICO 2.1, S-SICO 2.3, S-SICO 3.2, S-SICO 5.5, S-SICO 5.6, S-SICO 5.7, S-SICO 5.10, S-SICO 6.3

#### 5.2.3.4 Issuance of certificates and/or signing components

REQ-SICO 19 A certificate to be issued to the user must contain the information specified in § 7 (1) SigG.
cf.: § 7 (1) SigG
Safeguards: S-SICO 3.1, S-SICO 5.5, S-SICO 5.6

REQ-SICO 20 The time of drafting and issuing of the certificate or of the signing component is to be documented. Issue of the certificate is to be receipted by the user. The receipt is to be attached to the documentation..
cf.: Explanatory note on § 8 (1) SigG, § 6 SigV, § 13 (1) SigV
Safeguards: S-SICO 5.10, S-SICO 6.3, S-SICO 6.4

REQ-SICO 21 Issuance of the signing component and the appurtenant knowledge-based authentication data must be effected in a reliable manner.
cf.: Explanatory note on § 6 SigV
Safeguards: S-SICO 1.1, S-SICO 1.2, S-SICO 1.3, S-SICO 2.1, S-SICO 2.3, S-SICO 3.5, S-SICO 5.5, S-SICO 5.6

REQ-SICO 22 In addition to the user certificate, the key of the competent authority must also be issued to the user in authentic form.
cf.: Explanatory note on 4 (5) SigG, § 6 SigV and explanatory note on § 6 SigV
Safeguards: S-SICO 3.5, S-SICO 5.5, S-SICO 5.6

REC-SICO 2 The signing component is to contain the following data:
1. the user's certificate,
2. the user's private key,
3. the public key of the CA,
4. where appropriate, a supply of public back-up keys of the CA, for the purposes of key changing,
5. the public key of the competent authority,
6. where appropriate, the public keys of the time stamp and directory services, when these services possess their own keys

cf.: § 7 SigG, explanatory note on § 4 (5) SigG
Safeguards: S-SICO 3.5, S-SICO 4.3, S-SICO 5.5, S-SICO 5.6, S-SICO 5.14, S-SICO 6.7

#### 5.2.3.5 Notification

REQ-SICO 23 The users are to be provided with comprehensive information in such a manner as to enable them to apply the digital signatures in a secure manner.
cf.: § 6 SigG, § 4 SigV
Safeguards: S-SICO 6.6

REQ-SICO 24 The CA is required to inform users and any third parties of the procedures relating to revocations and to notify them of a telephone number for use in such instances.
cf.: § 9 (1) SigV and explanatory note on § 9 (1) SigV, § 3 (2) SigV
Safeguards: S-SICO 4.3, S-SICO 6.6

#### 5.2.3.6 Disclosure

REQ-SICO 25 On justified request, pseudonymised user data are to be disclosed to entitled parties in accordance with § 12 (2) SigG. Disclosures are to be documented.
cf.: § 12 (2) SigG
Safeguards: S-SICO 6.3, S-SICO 6.5

### 5.2.4 Security requirements and recommendations for revocation management

REQ-SICO 26 The receipt of revocation notices must be possible without delay and 'around the clock'.
cf.: § 9 (1) SigV and explanatory note on § 9 (1) SigV
Safeguards: S-SICO 3.3, S-SICO 4.1, S-SICO 4.3

REQ-SICO 27 The CA is to enable the revocation of a certificate at any time
- on request from an entitled party,
- in cases of false information,
- when it ceases operation and no other CA takes on the user,
- on instruction from the competent authority.
cf.: § 8 (1) SigG, § 9 (1) SigV
Safeguards: S-SICO 3.3, S-SICO 4.1, S-SICO 4.3

REQ-SICO 28 Revocation may be effected by authorised parties only. The revocation notice must be digitally signed and must be issued on the basis of a written application or in accordance with a specified authentication procedure.
cf.: § 9 (2) SigV
Safeguards: S-SICO 1.1, S-SICO 1.2, S-SICO 3.3, S-SICO 4.3, S-SICO 5.8, S-SICO 5.10

REQ-SICO 29 The date and time of revocation are to be documented. Retroactive revocations or the withdrawal of revocations are to be prevented.
cf.: § 8 (1) SigG and explanatory note on § 8 (1) SigG, § 9 (3) SigV, explanatory note on § 16 (4) SigV
Safeguards: S-SICO 3.3, S-SICO 4.3, S-SICO 5.10, S-SICO 6.3

REQ-SICO 30 When a user certificate is revoked, all corresponding attribute certificates must also be revoked. The user is to be informed of every revocation relating to his person. Mechanisms are to be provided for issuing new certificates and keys to the user in authentic form.
cf.: Explanatory note on § 8 SigG, § 7 SigV, § 14 (2) and (3) SigV
Safeguards: S-SICO 4.2, S-SICO 4.3, S-SICO 5.14, S-SICO 6.3

REQ-SICO 31 As the validity of user certificates must not necessarily be affected by the revocation of higher-priority certificates the time of generation of certificates must be ascertainable without doubt and on-line (in cases in which it is not evident on the basis of a time stamp in the certificate), so that it can be established whether the user certificate was generated before or after the revocation of a higher-priority certificate in the course of verifying document signatures.
cf.: Explanatory note on § 8 SigG, explanatory note on § 8 (1) SigG, § 4 (1) No. 5 and Nr.7 SigV and appurtenant explanatory note, explanatory note on § 16 (3) SigV
Safeguards: S-SICO 4.3, S-SICO 5.2, S-SICO 5.12

REC-SICO 3 Appropriate technical and/or organisational procedures are to be adopted for revocation entries to ensure that they cannot be initiated by an individual person without justification.
cf.: Explanatory note on § 14 (3) SigV
Safeguards: S-SICO 1.1, S-SICO 1.2, S-SICO 4.3, S-SICO 5.8, S-SICO 5.10, S-SICO 6.3

### 5.2.5 Security requirements and recommendations for security concept and documentation

#### 5.2.5.1 Documentation

REQ-SICO 32 Documentation must be drafted and maintained, containing the following:

1. the current security concept
2. check reports and confirmations on the security concept
3. contractual agreements between user and CA
4. the CA's own certificates and all user certificates, specifying the times of issue
5. applications for certificates, each accompanies by a copy of an identification document
6. pseudonyms
7. records substantiating information in attribute certificates or concerning third parties
8. records of effected notifications
9. time of issuing of the certificate and confirmation of issue
10. revocation of certificates
11. disclosures in accordance with § 12 (2) SigG
12. where appropriate, the time of issue of signing keys, of signing components, together with their authentication data and confirmation of issue

cf.: § 12 (2) SigG, § 13 (1) SigV
Safeguards: S-SICO 6.3

REQ-SICO 33 Certificates and security safeguards are to be documented in a traceable manner, certificates in particular are further to be documented in a verifiable manner.
cf.: § 10 SigG, § 8 (3) SigV, explanatory note on § 13 (2) SigV
Safeguards: S-SICO 4.1, S-SICO 4.2, S-SICO 6.3

REQ-SICO 34 The documentation is to be kept available for at least 35 years. An exception applies to records of disclosures in accordance with § 12 (2) SigG, which must be retained for at least one year. In cases in which the suitability of algorithms to which reference is made in a document is confirmed over a total period of 35 years, appurtenant documentation is to be retained for a correspondingly longer period.
cf.: § 8 (1) SigV, § 13 (2) SigV
Safeguards: S-SICO 6.3

REQ-SICO 35 Digital records of the documentation must be digitally signed by the CA. A signature key other than the certification key is required for this purpose.
cf.: § 13 (1) SigV and explanatory note on § 13 (1) SigV, explanatory note on § 4 (5) SigG
Safeguards: S-SICO 6.3

REQ-SICO 36 The documentation must be protected against unauthorised access.
cf.: Explanatory note on § 13 (1) SigV
Safeguards: S-SICO 1.1, S-SICO 1.2, S-SICO 5.4, S-SICO 5.8, S-SICO 5.10, S-SICO 6.1

#### 5.2.5.2 Security concept

REQ-SICO 37 A security concept is to be drafted and continually updated, establishing that all security requirements imposed by the Act and the Ordinance are fulfilled in an adequate manner and in accordance with the specific protection requirements. It must be possible to verify the implementation of required security safeguards on the basis of the security concept.
cf.: § 4 (3) SigG, § 12 (1) SigV
Safeguards: S-SICO 5.3, S-SICO 6.2, S-SICO 6.3, S-SICO 6.7

REQ-SICO 38 The security concept must specify all security safeguards, the deployed technical components and the organisational structure.
cf.: § 12 (1) SigV and explanatory note on § 12 (1) SigV
Safeguards: S-SICO 6.1, S-SICO 6.7

REC-SICO 4 IT baseline protection should be observed and implemented in drafting the security concept.
cf.: § 1 (1) SigG, § 11 SigV, § 12 (1) SigV
Safeguards: S-SICO 6.1

### 5.2.6 Security requirements and recommendations for the organisational tructure

REQ-SICO 39 Private user keys and knowledge-based authentication data are to be kept secret and must not be stored at the CA.
cf.: Explanatory note on § 14 (1) SigG, § 5 (2) SigV and explanatory note on § 5 (2) SigV, explanatory note on § 14 (3) SigV
Safeguards: Safeguards: S-SICO 1.1, S-SICO 1.2, S-SICO 1.3, S-SICO 1.4, S-SICO 2.1, S-SICO 2.2, S-SICO 2.3, S-SICO 3.1, S-SICO 3.5, S-SICO 5.1, S-SICO 5.4, S-SICO 5.13

REQ-SICO 40 All procedures are to be specified and implemented in such a manner as to ensure that it will never be possible for an individual person
- to produce forged certificates or time stamps or to forge authentic certificates or time stamps, or
- to incorporate signature keys into approved signature components without authorisation, or
- to obtain unauthorised access to a signature key, or to effect revocation entries in an unauthorised manner.

cf.: § 1 (1) SigG, § 5 (4) SigG, § 11 SigV, explanatory note on § 14 (1) SigG, § 6 SigV and explanatory note on § 6 SigV, § 9 (3) SigV, explanatory note on § 14 (3) SigV
Safeguards: S-SICO 1.1, S-SICO 1.2, S-SICO 1.3, S-SICO 1.4, S-SICO 2.1, S-SICO 2.2, S-SICO 2.3, S-SICO 3.1, S-SICO 3.3,

S-SICO 3.4, S-SICO 3.5, S-SICO 5.1, S-SICO 5.4, S-SICO 5.5, S-SICO 5.6, S-SICO 5.7, S-SICO 5.13

REQ-SICO 41 On request, user certificates are to be treated confidentially. Confidential certificates are to be protected.
cf.: § 5 (1) SigG and explanatory note on § 5 (1) SigG
Safeguards: S-SICO 3.3

REQ-SICO 42 The directory service must identify and authenticate itself to the inquirer and enable inquiries as to the existence of a certificate in the directory.
cf.: Explanatory note on § 16 (4) SigV
Safeguards: S-SICO 3.3

REQ-SICO 43 When directories of other certification authorities are offered, the corresponding revocation lists are also to be offered and continually updated.
cf.: Explanatory note on § 8 (1) SigV
Safeguards: S-SICO 3.3

### 5.2.7 Security requirements and recommendations for the personnel

REQ-SICO 44 The staff must possess the required reliability and specialised knowledge.
cf.: § 4 (3) SigG, § 5 (5) SigG, § 10 SigV
Safeguards: S-SICO 2.1, S-SICO 2.2

REC-SICO 5 The CA should appoint an IT security officer and a data protection officer, and should establish a system of cryptomanagement.
cf.: § 12 (2) SigG, § 10 SigV
Safeguards: S-SICO 2.3, S-SICO 5.3, S-SICO 5.4

REC-SICO 6 The staff should be trained with regard to new technical and legal developments.
cf.: § 4 (3) SigG, § 5 (5) SigG, § 10 SigV
Safeguards: S-SICO 2.2

REC-SICO 7 The staff should be instructed as to the relevance of their duties and bound to comply with the provisions of the Act and the Ordinance.
cf.: § 1 (1) SigG
Safeguards: S-SICO 2.3

### 5.2.8 Security requirements and recommendations for the infrastructure

REQ-SICO 45 Unauthorised access to signature keys and technical components to produce certificates or time stamps and to maintain certificates in a verifiable state, in the form of both physical access and access via communications technology, is to be prevented. All areas in which these components are located are to be protected against unauthorised access.
cf.: § 5 (4) SigG, explanatory note on § 11 SigV
Safeguards: S-SICO 1.1, S-SICO 1.2, S-SICO 1.3, S-SICO 1.4, S-SICO 5.3, S-SICO 5.4

REQ-SICO 46 The knowledge-based authentication data for the signing components are to be transmitted to the user in a manner which affords adequate protection against compromise.
cf.: Explanatory note on § 11 SigV, § 6 SigV
Safeguards: S-SICO 1.1, S-SICO 1.2, S-SICO 1.3, S-SICO 1.4, S-SICO 2.2, S-SICO 3.5, S-SICO 5.5, S-SICO 5.6, S-SICO 5.13

REQ-SICO 47 Individual physical secure areas are to be established for the respective services of a CA so as to prevent unauthorised persons from gaining access to rooms containing IT systems, and so as to eliminate the possibility of sabotage to services which are subject to high availability requirements.
cf.: Explanatory note on § 11 SigV
Safeguards: S-SICO 1.1, S-SICO 1.2

REC-SICO 8 The CA should operate a secure disposal facility for signing components and key material.
cf.: § 11 SigV, explanatory note on § 4 (1) No. 1 SigV
Safeguards: S-SICO 1.1, S-SICO 1.2, S-SICO 1.3, S-SICO 3.1

### 5.2.9 Security requirements and recommendations on IT

REQ-SICO 48 The CA is to deploy technical components in accordance with § 14 SigG.
cf.: § 14 (4) SigG, § 5 (5) SigG
Safeguards: S-SICO 6.2

REQ-SICO 49 Mechanisms for producing records are to be implemented on the IT systems. The record data are to be evaluated on a regular basis.
cf.: § 5 (4) SigG and explanatory note on § 5 (4) SigG
Safeguards: S-SICO 6.2

REQ-SICO 50 Mechanisms which detect manipulations to data automatically are to be implemented on the IT systems (integrity control).
cf.: Explanatory note on § 5 (4) SigG
Safeguards: S-SICO 6.2

REQ-SICO 51 Mechanisms are to be implemented on the IT systems which will automatically detect the compromising of keys or authentication parameters, should secrecy no longer be adequately ensured.
cf.: Explanatory note on § 5 (2) SigV
Safeguards: S-SICO 6.2

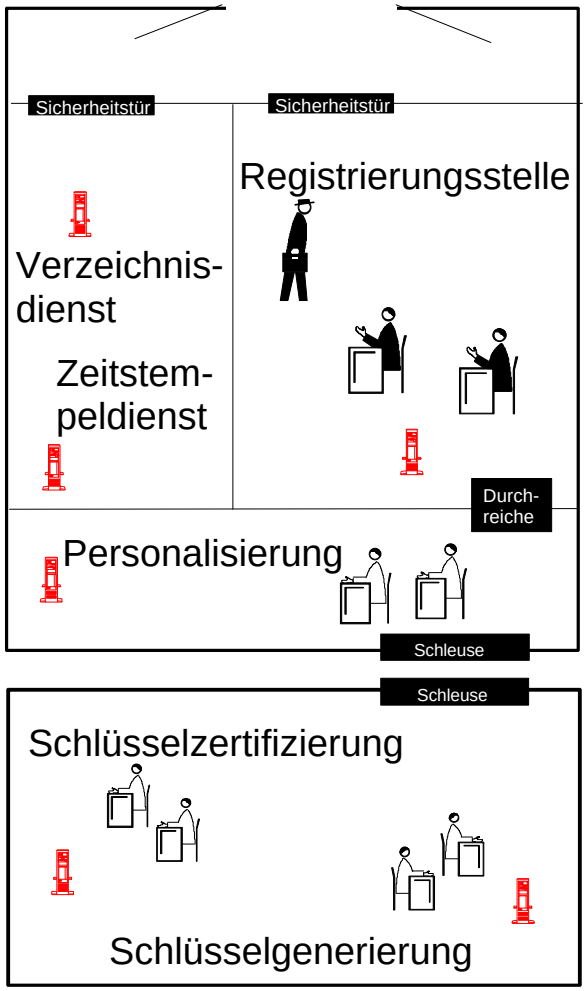
REQ-SICO 52 Mechanisms are to be implemented on the IT systems which will detect manipulations automatically, should it not be possible to eliminate unauthorised access with adequate certainty.
cf.: Explanatory note on § 5 (2) SigV, explanatory note on § 11 SigV
Safeguards: S-SICO 6.2

## 5.3 Proposals

### 5.3.1 Proposal 1: Central model

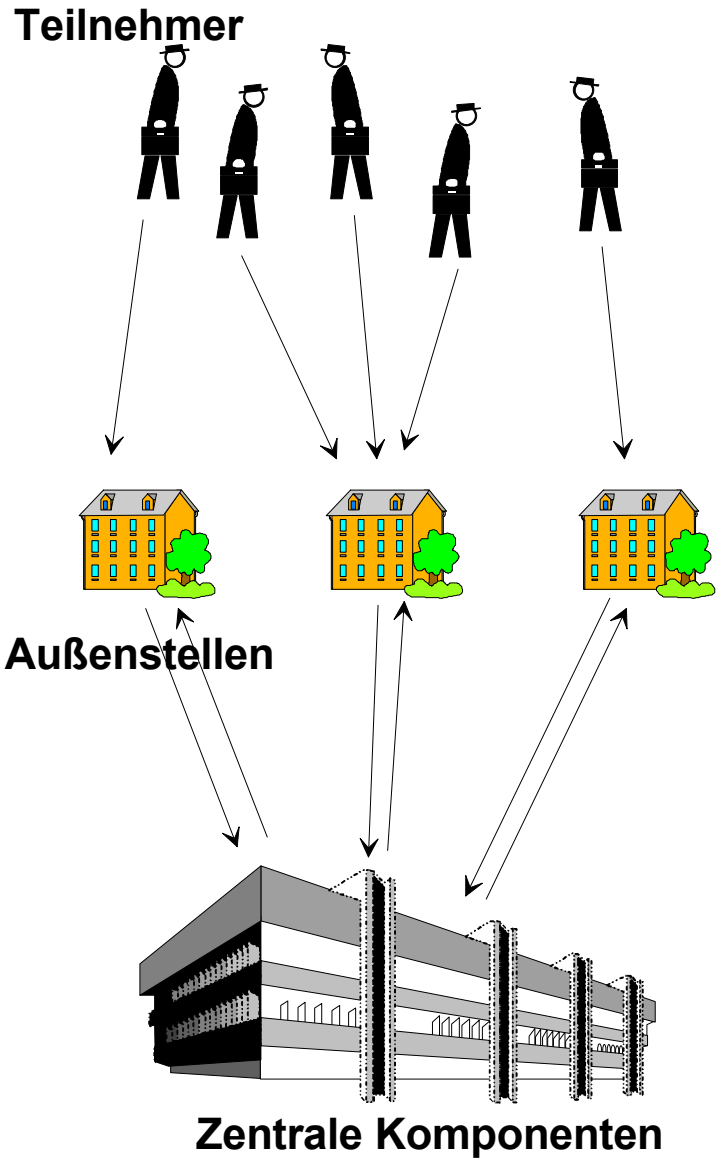
In this completely centralised model, the CA has no branch offices; the user keys are generated by the CA.

The services required for operation of a certification authority are all provided by an institution within a narrowly defined area (generally within a building complex). For example:



### 5.3.2 Proposal 2: Decentralised model

In this model, which provides for the widest possible distribution of operations, the CA runs branch offices which perform the tasks of registration (and identification) and personalisation. Key generation is additionally carried out by the users. All other services continue to be performed centrally.




### 5.3.3 Hybrids of proposals 1 and 2

In hybrid forms key generation may be carried out by the CA, for example, while the users come into contact with branch offices only. Decentralised key generation by the user is also conceivable, when the CA does not possess any branch offices.

It is not expedient to examine these hybrid forms in further detail here, as the respective security requirements and security safeguards can be derived directly from proposals 1 and 2.

## 5.4 Safeguard Catalogue

### 5.4.1 Threats

The following enumeration does not draw a strict distinction between threats as defined in ITSEC and any vulnerabilities which may be exploitable as a result of implementation. Equally, the enumeration is certainly not to be regarded as complete or final.

#### 5.4.1.1 General threats

The general situation with regard to threats covers threats from the areas of 'Force majeure', 'Organisational inadequacies', 'Human error', 'Technical failure' and 'Wilful acts'. A summary of these areas is to be found in the IT-Grundschutzhandbuch (IT baseline protection manual) of the BSI (German Information Security Agency) [BSI97]. It is thus unnecessary to provide explicit quotations from this manual here.

1. Risk situation in accordance with [BSI97].
   Safeguards: S-SICO 6.1
2. Requirements stipulated in the Digital Signature Act or the Digital Signature Ordinance are contravened.
   Safeguards: (all obligatory safeguards for the selected model, cf. table in chapter 5.4.3)

#### 5.4.1.2 Specific threats

*Threats relating to key material and/or certificates*

3. Compromised key material or loss of integrity for key material.
   Safeguards: S-SICO 1.1, S-SICO 1.2, S-SICO 1.3, S-SICO 1.4, S-SICO 2.1, S-SICO 2.2, S-SICO 2.3, S-SICO 3.1, S-SICO 3.5, S-SICO 5.1, S-SICO 5.4, S-SICO 5.5, S-SICO 5.6, S-SICO 5.8, S-SICO 5.13, S-SICO 6.1, S-SICO 6.7
4. False or inadmissible data are entered in the certificate.
   Safeguards: S-SICO 2.1, S-SICO 2.2, S-SICO 2.3, S-SICO 3.1, S-SICO 3.2, S-SICO 5.5, S-SICO 5.6, S-SICO 5.7, S-SICO 5.11, S-SICO 6.4
5. A key pair and certificate are generated for a non-existent user.
   Safeguards: SIKO 3.2, S-SICO 5.5, S-SICO 5.6, S-SICO 5.7, S-SICO 6.4
6. The time of drafting of a certificate is no longer ascertainable.
   Safeguards: S-SICO 5.12

*Threats relating to operation of the IT systems*

7. Improper use of an IT system.
   Safeguards: S-SICO 1.1, S-SICO 1.2, S-SICO 5.4, S-SICO 5.8, S-SICO 5.10, S-SICO 6.2
8. Loss of availability of communication channels or IT systems.
   Safeguards: S-SICO 4.1, S-SICO 4.2, S-SICO 6.2, S-SICO 6.7
9. Data loss.
   Safeguards: S-SICO 4.2, S-SICO 6.3, S-SICO 6.4
10. Gaps in regulations for operation of the respective IT systems.
    Safeguards: S-SICO 3.1, S-SICO 3.2, S-SICO 3.3, S-SICO 3.4, S-SICO 3.5

*Threats relating to the organisational structure of a certification authority*

11. Implementation of unsuitable internal procedures after the receipt of an application for a certificate through to issuing of the certificate to the user.
    Safeguards: S-SICO 3.1, S-SICO 3.2, S-SICO 5.1, S-SICO 5.2, S-SICO 5.5, S-SICO 5.6
12. Implementation of unsuitable procedures for external access to the directory service or time stamping service.
    Safeguards: S-SICO 3.3, S-SICO 3.4, S-SICO 4.1, S-SICO 4.3, S-SICO 5.12, S-SICO 5.15
13. Unknown status of an application.
    Safeguards: S-SICO 3.1, S-SICO 3.2, S-SICO 5.5, S-SICO 5.6, S-SICO 5.10, S-SICO 6.3, S-SICO 6.4
14. Inadequate revocation management.
    Safeguards: S-SICO 3.3, S-SICO 4.3, S-SICO 5.14
15. Third parties named in certificates are not provided with an adequate scope of information or not notified, or the furnishing of information to entitled parties is refused.
    Safeguards: S-SICO 5.11, S-SICO 6.3, S-SICO 6.4, S-SICO 6.5

*Threats relating to the user*

16. The user is identified / registered as someone he is not.
    Safeguards: S-SICO 2.2, S-SICO 3.2, S-SICO 5.7, S-SICO 6.3, S-SICO 6.4
17. The user presents a false identity.
    Safeguards: S-SICO 2.2, S-SICO 3.2, S-SICO 5.7
18. The user submits a public key which has already been assigned to another person.
    Safeguards: S-SICO 5.9
19. The user submits an unapproved signing component.
    Safeguards: S-SICO 5.5, S-SICO 5.6
20. The user is not in possession of the private key.
    Safeguards: S-SICO 5.5, S-SICO 5.6
21. The signing component, the certificate or the knowledge-based authentication data are not issued to the user in a reliable manner.
    Safeguards: S-SICO 2.1, S-SICO 2.2, S-SICO 2.3 S-SICO 3.5, S-SICO 5.5, S-SICO 5.6
22. Inadequate instruction or complete failure to instruct users.
    Safeguards: S-SICO 6.6

### 5.4.2 Safeguards

#### 5.4.2.1 Infrastructural safeguards

**S-SICO 1.1 Protection against unauthorised physical access**

The IT systems requiring protection must be located in separate protected rooms. A system is to be evolved for the obligatory burglar alarm and access control facilities in the secure areas, in particular stipulating the installation sites for control centres and connection of the alarms. These areas are also to be protected in accordance with the IT systems. The access control facility further requires the post of doorman, although this can also be performed by staff of the CA ('bell officer').

**S-SICO 1.2 Establishment of secure areas**

Secure areas are to be established, whereby the tasks of identification/registration (RA), key generation and key certification (CS), personalisation and the directory service (DIR) are to be allocated according to the specified form of organisational structure. The directory service can be implemented together with the CS or the personalisation service. Only the area of identification may be accessible to the public. The other areas must be accessible only to the staff working in the respective areas concerned. Due to the high level of security required in the areas of key generation, key certification and personalisation, these areas may only be accessible via a staff control facility (lock). The areas of personalisation and identification (here the issuing of signing components in particular) can be effectively located next to one another. A security hatch is then to be provided between the two areas.

The outer skin of the of the secure areas in which the systems are operated should be protected so as to frustrate an attack before the area can be entered. Resistant outer walls and burglary-resistant doors and windows are necessary to this end. The design should correspond to strength ET 3 / EF 3 in accordance with DIN V 18103 and DIN V 18054 (note comparison tables here!). A burglar alarm system and an access control system should be installed.

In order to eliminate compromising emanations, those areas in which keys requiring protection are used in plain-text form are to be set up in emanation-protected form (e.g. as a 'Faraday cage'), in accordance with the zonal plan. Depending on the mode of implementation, the emanation protection can be provided with regard to the IT system, the data lines or the respective rooms.

**S-SICO 1.3 Provision of key containers**

When key material requiring protection (e.g. signing components initialised with key pairs) requires to be stored, suitable containers and/or areas are to be provided for this purpose. The key material is to be accommodated, for example, in SG II VS steel cabinets in accordance with PTZ standard 7201.30 (issued by the Federal German central physico-technical institute), in rooms monitored by capacitive field-change detectors. Alternatively, the key material may also be accommodated in simpler steel cabinets in rooms whose walls are monitored by structure-borne noise detectors and which possess only one access door and no windows. The access door should comply with the requirements for strong-room doors in accordance with RAL-RG 625/4.

The procedure for gaining access to stored key material requiring protection must preclude the possibility of a single individual being able to access and manipulate the material. To this end, the key material which is to be kept secret (e.g. transport keys) can be encoded for storage

purposes or divided into two appropriate components, for example. Access to both components by a single member of staff must then be impossible.

**S-SICO 1.4 Monitoring of access to internal data transmission channels**

A secure operating location must be established for network distributors through which information requiring protection is transmitted. The rooms concerned are to be monitored using burglar alarm and access control systems.

Should, for reasons which are not presently apparent, transport encoding not be used for compromisable information, all data transmission channels are to be monitored for access instead. For this purpose, the data lines are to be installed in conduits with detection facilities to monitor opening. Emanation protection safeguards are additionally to be implemented in accordance with the zonal model when using copper conductors and for active network components (e.g. routers).

### 5.4.2.2 Personnel safeguards

**S-SICO 2.1 Selection of particularly trustworthy personnel**

As a particularly high degree of trust requires to be placed in the personnel of a CA, all necessary information must be gathered on these persons (police clearance on basis of police records at least).

**S-SICO 2.2 Basic and further training of the operating personnel**

Before carrying out work on their own responsibility, employees must receive adequate instruction and, where necessary, training. Employees are to receive appropriate further training in connection with technical modifications or modernisation safeguards.

**S-SICO 2.3 Advising operating personnel of their responsibilities and obligations**

New employees are to be advised as to their duty to exercise due care, their obligation to comply with the CA's security safeguards and to discharge their duties in a correct manner. This advice is to be repeated at least once per year. The employees are to be obligated to comply with the regulations pertaining to their work (in particular the provisions of SigG/SigV).

### 5.4.2.3 Organisational safeguards

**S-SICO 3.1 Directive for the generation and destruction of keys and for the drafting of certificates**

This directive must stipulate the following at least:

- the preconditions which apply to the generation and certification of pairs of keys,
- the period over which certificates are valid (maximum of five years and only within the period of suitability of the employed algorithms),
- how and by whom key pairs may be generated,
- with which algorithms, with which private signature key of the CA, how and by whom public keys may be certified,
- the information which may be contained in key certificates and attribute certificates and how they are to be structured,
- the general conditions applying to the granting and issuance of an attribute certificate,
- that key material which is no longer required must be destroyed,
- how, under what circumstances and by whom key material may be destroyed,
- the preconditions applying to the transmission of data to the personalisation system,

- the manner in which data is to be exchanged between CA and any distributed RAs, and
- the organisational or technical safeguards which are installed to prevent an individual person from generating, certifying or destroying keys without authorisation.

**S-SICO 3.2 Directive on the identification and registration of users**

It is to be stipulated which external offices (RA) may carry out identification for the CA and the manner in which identification is to be carried out. It must also be specified how reliable identification is to be ensured and how the possibility of identification being declared 'duly executed' is excluded when the identification relates to a fictitious person or when the user has not granted consent. Each identification must be documented and the user must be registered. The directive is to stipulate the means of identification (personal identity card, passport, driving licence, deposited signature, etc.) which may be employed for the purpose of identification.

**S-SICO 3.3 Directive on operation of the directory service**

This directive must stipulate how the public is to access the directory services. Communication must take place in authentic mode. To this end, provisions must be set out to enable the provision of current and non-manipulable information by the service. The corresponding procedures (e.g. authentication) are to be specified. The preconditions for an entry by the CA for a new user and for revocation information must also be specified. When the user does not consent to publication in the directory, the necessary safeguards to protect confidentiality are to be specified. When copies of directories from other certification authorities are made available, the revocation management information of these other authorities is also to be offered. In this connection it is to be specified how it is ensured that these revocation lists are up to date.

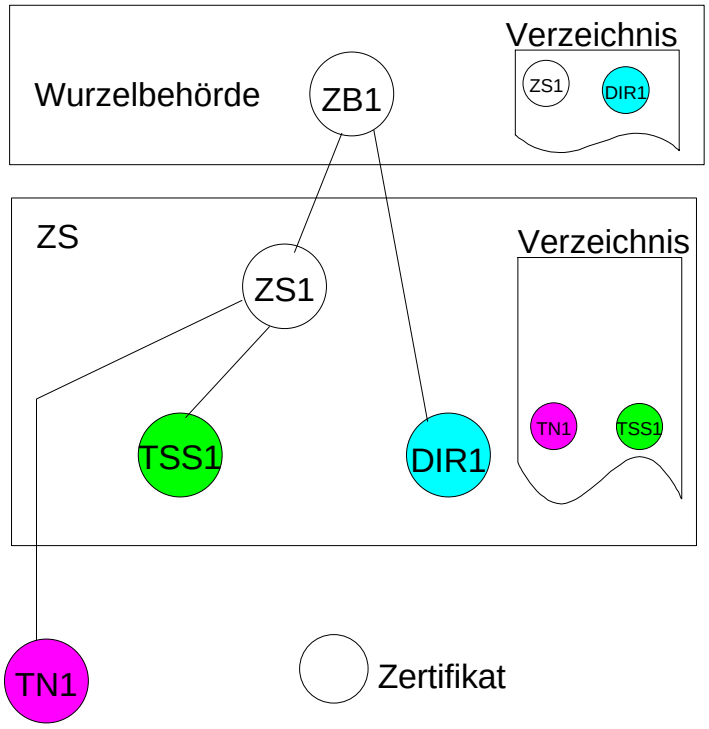
The following times are also to be stipulated, whereby certain upper limits are to be observed:

1. The maximum down time must be less than three hours.
2. Wherever possible, the standard response time[3] should not exceed one minute.
3. The response time for generation of a revocation entry[4] must not exceed ten minutes.

The inquiry facilities and the potential items of information are also to be specified. The information provided by the directory service should be certified by the latter with a signature key which is certified by the root authority for this specific purpose (cf. diagram below). When a directory service key is registered as a user of the service's own CA, the corresponding certificate is nevertheless to be kept in the directory of the root authority, so as to enable the application of revocation management in the event of data being compromised. The users are to be informed that they can obtain the currently valid directory service key from the directory of the root authority.

[3] The time within which a standard item of information is returned to the user.

[4] This is not the time up to which the revocation entry is to remain available on-line, but the point in time from which the revocation is to apply.




**S-SICO 3.4 Directive on operation of the time stamping service**

This directive is to stipulate how the public is to access the time stamping service. It is also to be specified which procedures are to be employed to generate and verify a time stamp and how a precise time stamp is to be managed. The following times are also to be stipulated, whereby certain upper limits are to be observed:

1. The maximum down time must be less than three hours.
2. Wherever possible, the standard response time[5] should not exceed one minute.
3. The response time for generation of a time stamp[6] must not exceed ten minutes.

It is recommended to use a separate signature key for time stamps, which should be registered as a user of the certification authority concerned (cf. diagram for S-SICO 3.3). Where appropriate, it is to be explained why the CA certification key is used for the time stamping service, instead of a separate time stamp key.

The time stamping services may not be refused to any person.

**S-SICO 3.5 Directive on the procedure for the forwarding of key material**

It must be stipulated between which IT systems key material may be exchanged and which cryptographic methods are to be employed for the transport encoding which is recommended for private keys. In this connection, particular attention is to be paid to the quality of the employed algorithm, adequate key length and appropriate key management. When transport encoding is not employed, other suitable safeguards (e.g. infrastructural safeguards) are to be implemented to protect the keys.

It must be stipulated when a signing component may be released. Persons authorised to receive key material within the CA must be designated and stipulated. The signing component may be handed over to the authorised person only on receipt of his signature.

[5] The time within which the time stamp is returned to the user.

[6] The time within which the time stamp is generated.

It must be specified what organisational or technical safeguards are to be undertaken to prevent an individual person from storing or passing on without authorisation keys which require protection (including authentication data for signing components). It must further be specified what organisational or technical safeguards are to be undertaken to ensure that the certification key of the CA is exchanged directly and exclusively between the generating system and the certification computer.

#### 5.4.2.4 Business continuity

**S-SICO 4.1 Maintenance of redundant IT systems**

In order to meet the availability requirements as specified in SigG/SigV, a certification authority should maintain redundant IT systems for key generation, certification and personalisation. Redundant configuration is compulsory for the directory service. The redundancy must relate to accessibility via public communications facilities, to the appurtenant computer and to the data offered on this computer, so as to enable everyone to avail themselves of the directory services at all times. In all circumstances, it is to be ensured that the IT security safeguards stipulated elsewhere in this safeguard catalogue are also implemented for the redundant IT systems. If appropriate, a back-up certification authority which is able to take over the tasks when necessary can be set up at a second location. A suitable and secure method of data transmission is to be created between the redundant system components.

**S-SICO 4.2 Data back-up**

In view of the high availability requirements for the directory services and the requirement to keep certificates[7] available for verification for a certain time, a data saving concept is to be developed which fulfils these requirements. It is expedient to provide a system of data mirroring or a completely redundant directory service (cf. S-SICO 4.1). The identification parameters are to be saved in order to ensure the accessibility of the users at all times, including circumstances under which the disaster recovery management system comes into effect. To this end, back-up copies of the documents concerned are to be produced (where applicable on microfilm) and stored in a back-up archive.

**S-SICO 4.3 Revocation management**

A revocation management system must specify the following items at least:

1. Procedures for the receipt of revocation notices, including
   - availability of the office receiving revocation notices,
   - structure and content of a revocation notice,
   - stipulation of persons possessing authorisation for revocation notices,
   - stipulation of justified grounds for revocation notices, and
   - authentication mechanisms to identify authorised persons.
2. Procedures for effecting revocation entries in revocation lists, including
   - authentication of the CA employee vis-à-vis the directory service, and
   - structure and content of a revocation entry.
3. Follow-up activities in response to revocation entries, including
   - revocation of dependent certificates (e.g. attribute certificates, user certificates under certain conditions when CA certificates are revoked),
   - notification of the users and certification authorities affected by revocations, and
   - where appropriate, the changing of keys and certificates.

[7] This includes the certificate of the CA itself.

In drafting the above points, consideration must be given to the following aspects[8]:

Revocation of key certificates or attribute certificates of individual users

Revocation entries by a CA employee may only be possible when a person authorised to effect revocation has communicated the authentication characteristic. The CA employee is not aware of the agreed authentication characteristic, which is stored in protected mode in the directory service and must be entered in order to effect a revocation entry. Upon revocation of a key certificate, all related attribute certificates must be revoked automatically.

Compromise of the time stamping service's signature key

The certificate of the compromised time stamp key is to be revoked, stating the time of revocation in the directory. In order to minimise the consequences of compromise of the time stamping service's key signature, special mechanisms must be installed to prevent back-dating.

Examples of such mechanisms are:

1. All submitted time stamp signatures are dependent on all or specific preceding time stamps. This results in a chronological sequence of time stamps in which it will not be possible to insert a back-dated time stamp, even in the event of the signature key being compromised.
2. All submitted time stamp signatures are documented in chronological order on a medium which permits writing once only (hashed value or plain text including time stamp signature). This documentation must be available for retrieval via public communications facilities after a case of compromise. The subsequent insertion of back-dated time stamps is not possible.
3. The time stamp key is changed on a daily basis. In the event of compromise, back-dating can be effected only to the day on which the compromised key was valid. All time stamps submitted on this day lose their validity. This solution reduces the scope for manipulation, but does not fully exclude manipulation. This mechanism furthermore involves extensive procedures for daily key-changing, and is thus of only limited suitability.

Should none of these mechanisms be implemented, all time stamps submitted with the compromised key will lose their validity. These time stamps will then possess no informational value, irrespective of when they were submitted.

Compromise of the CA's signature key

The certificate of the compromised signature key is to be revoked in the directory of the root authority, stating the time of revocation. In order to ensure that not all user certificates are affected by the revocation of a compromised CA signature key and thus also require to be revoked, the following conditions must be fulfilled:

1. User certificates must bear a time stamp providing information on the time of generation of the CA's signature, so as to enable ascertainment of whether the user certificate was drafted before or after revocation of the CA's signature key in the course of verifying document signatures.
2. The time stamp key itself must not be compromised, or mechanisms must be in place to prevent back-dating (see above).
3. The time stamp key which was authentic and valid at a specific point in time must be ascertainable without any doubt and available via an uncompromised directory service.

When any one of these conditions is not fulfilled, all user certificates of this CA will be revoked automatically. It may be necessary to draw up an emergency plan to ensure a rapid response in such a situation.

Compromise of the directory service's signature key

[8] The revocation management activities outlined here have been based on the model in the diagram for S-SICO 3.3.

When the certification authorities organisational structure provides for directory service inquiries to be provided with a digital signature using a private key of the directory service and this key is compromised or lost, the new directory service key is to be offered via the directory of the root authority.

Compromise of the competent authority's signature key

The same procedure applies as for compromise of the CA's signature key, whereby the individual certification authorities are to be interpreted as users of the competent authority.

Action to be taken after revocation in cases of compromise or loss of signature keys

In cases of compromise, all affected users must be notified directly and in writing of the nature and time of the incident concerned. New CA signature keys and directory service keys can be provided in authentic form via certificates in the directory of the competent authority. When, in the course of personalisation of their signing components, the users have been handed over several CA keys for which certificates already exist, a key change is effected via notification as to which key is now valid. New time stamp keys can be provided via the directory of the CA.

#### 5.4.2.5 Safeguards relating to the organisational structure

**S-SICO 5.1 Operation of the key generating system in dedicated mode**

Maximum confidentiality applies to the private key of the CA, which is used by the CA to certify the user keys. In order to minimise the possibility of this key being compromised, key generation should be carried out on a dedicated IT system which is not networked. Key generation for the user should also take place on this IT system.

Operation of this IT system in dedicated mode also appears expedient for the following reasons: key generation for the CA will take place relatively rarely and advance reserves of key pairs for users can be generated. The public user keys are then exported in an appropriate manner to the certification system, and the private keys to the personalisation system. Consequently, the IT system for key generation will be out of operation for most of the time.

**S-SICO 5.2 Use of a signature key exclusively for time stamps**

The signature key for time stamps must not be identical to the certification key. A separate certificate from the CA or the competent authority should exist for this key.

**S-SICO 5.3 Duties and allocation of roles**

The certification authority must perform the task of identifying users. It must offer a key generating service, key certification, a time stamping service and a directory service (incl. revocation management). To enable the discharge of these duties in accordance with SigG, provision should be made for the following posts within the overall organisational structure at the CA:

- IT security officer,
- data protection officer,
- review (where appropriate by external party),
- data processing 1 (relating to the IT systems for certification, key generation and personalisation),
- data processing 2 (registration and identification, directory service),
- technical service (cabling, safety equipment, fire protection, etc.) and
- cryptomanagement (supervision of cryptographic processes, drafting of a key management concept (e.g. in acc. with [ISO11770-3]) etc.

### S-SICO 5.4 Separation of posts

When allocating posts it is to be noted that certain tasks must not be carried out by one and the same person: Data processing 1, data processing 2 and revision are mutually preclusive. The same applies to cryptomanagement and review.

### S-SICO 5.5 Application procedure for a certificate when key generation is carried out by the user

The user's application must permit clear identification of the user. Name, date of birth, address, etc. are to be stated as minimum requirements. The RA allocates a user name (or, on request, an unambiguous pseudonym) which is unique within the certification authority. Wherever possible this name should, however, be unique at national level.

The user must already be in possession of an approved signing component on which the key pair has been generated. The user notifies the CA of the public key[9] and furnishes proof [10] that he is in possession of an approved signing component and that the key originates from this component.

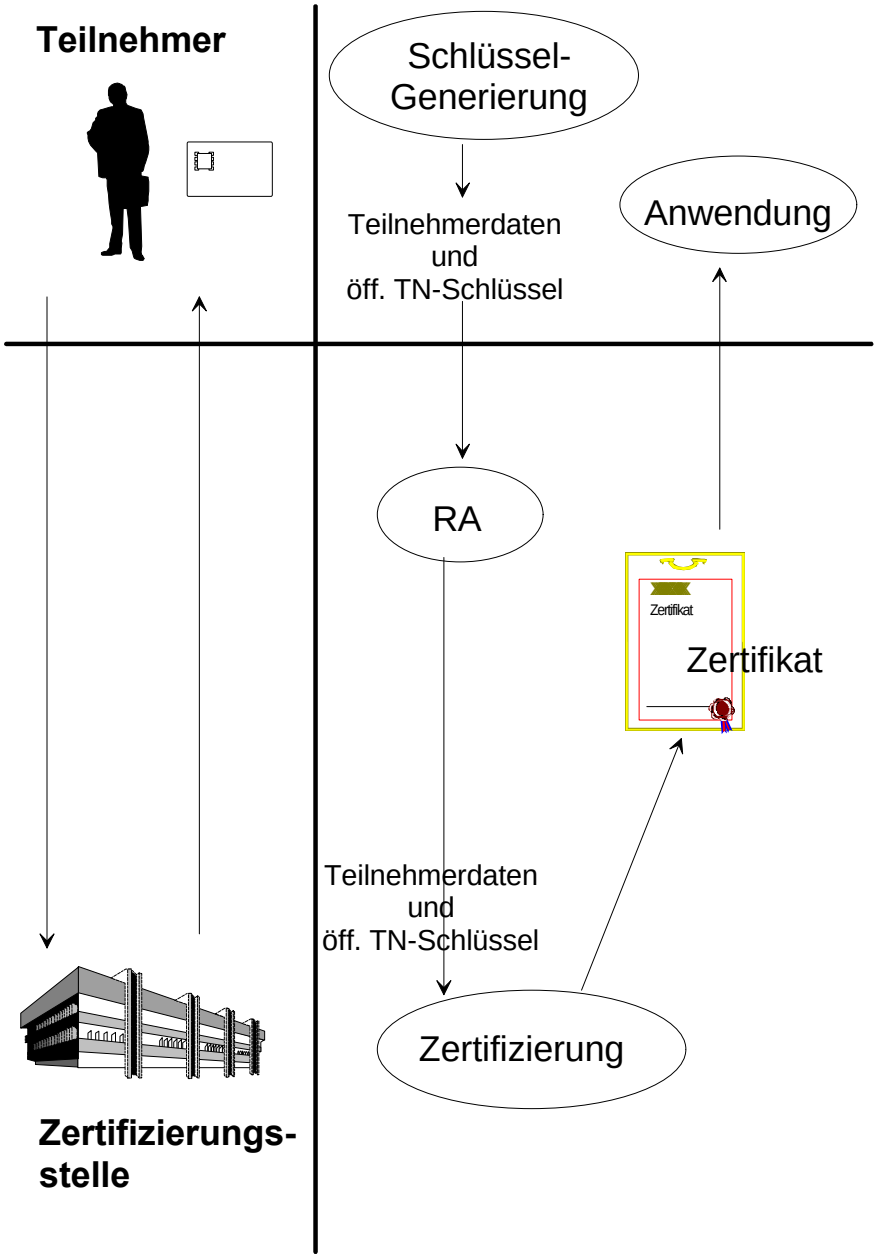
The application is forwarded to the CA for generation of the certificate. The received public key is checked on the certification computer to verify that it is unambiguous, e.g. by reference to the directory services of the CA concerned. If the public key has already been assigned to another user, the process will be aborted[11]. The user data, CA data, public key and other data in accordance with § 7 SigG are digitally signed with the CA's private key (certificate generation).

The certificate and the public key of the competent authority are now to be forwarded to the user; prior to handover of the certificate or its publication in the directory, however, it is to be reliably verified that the person deemed to have been identified is not fictitious and has actually submitted an application for a certificate. This verification must not be carried out by the CA employee who carried out identification. Technical or organisational safeguards must be implemented to ensure that handover or publication of a certificate cannot take place without this verification.

[9] It remains at the user's discretion whether he wishes to relinquish the signing component to the RA.

[10] cf. Chapter 6.3 Personalisation.

[11] The user who has been assigned the key which is now compromised is to be notified and an appurtenant revocation entry is to be effected.


Teilnehmer
Schlüssel-
Generierung
Anwendung
Teilnehmerdaten
und
öff. TN-Schlüssel
RA
Zertifikat
Zertifikat
Teilnehmerdaten
und
öff. TN-Schlüssel
Zertifizierung
Zertifizierungs-
stelle

### S-SICO 5.6 Application procedure for a certificate when key generation is carried out by the CA

The user's application must permit unambiguous identification of the user. Name, date of birth, address, etc. are to be stated as minimum requirements. The RA allocates a user name (or, on request, an unambiguous pseudonym) which is unique within the certification authority. Wherever possible this name should, however, be unique at national level. If the user already possesses an approved component but without a key pair, this component is to be attached to the application for the purpose of personalisation and the license is to be verified.

The application is forwarded to the CA for certificate generation and key generation and, where appropriate, the user's signing component is forwarded to the personalisation environment. Should the user not possess a signing component of his own, signing components are available in the personalisation environment. The certification computer receives a public key from the key generating service. The received public key is checked on the certification computer to verify that it is unambiguous, e.g. by reference to the CA's directory services. If the public key already exists, the key generating service will request a new public key[12]. The personalisation environment receives the corresponding private key from the generating service in transport-encoded form, stores it on the signing component and activates a knowledge-based (and biometric, where necessary) authentication process for use of the signing component. The user data, CA data, the public key and other data in accordance with § 7 SigG are digitally signed with the CA's private key (certificate generation). These data can also be incorporated into the signing component via the personalisation environment.

The certificate, the signing component (now with the private key) and the public key of the competent authority[13] are now to be forwarded to the user. Prior to handover of the certificate and the signing component or publication of the certificate in the directory, however, it is to be reliably verified that the person deemed to have been identified is not fictitious and has actually submitted an application for a certificate. This verification must not be carried out by the CA employee who carried out identification. Technical or organisational safeguards must be implemented to ensure that handover or publication of a certificate cannot take place without this verification.

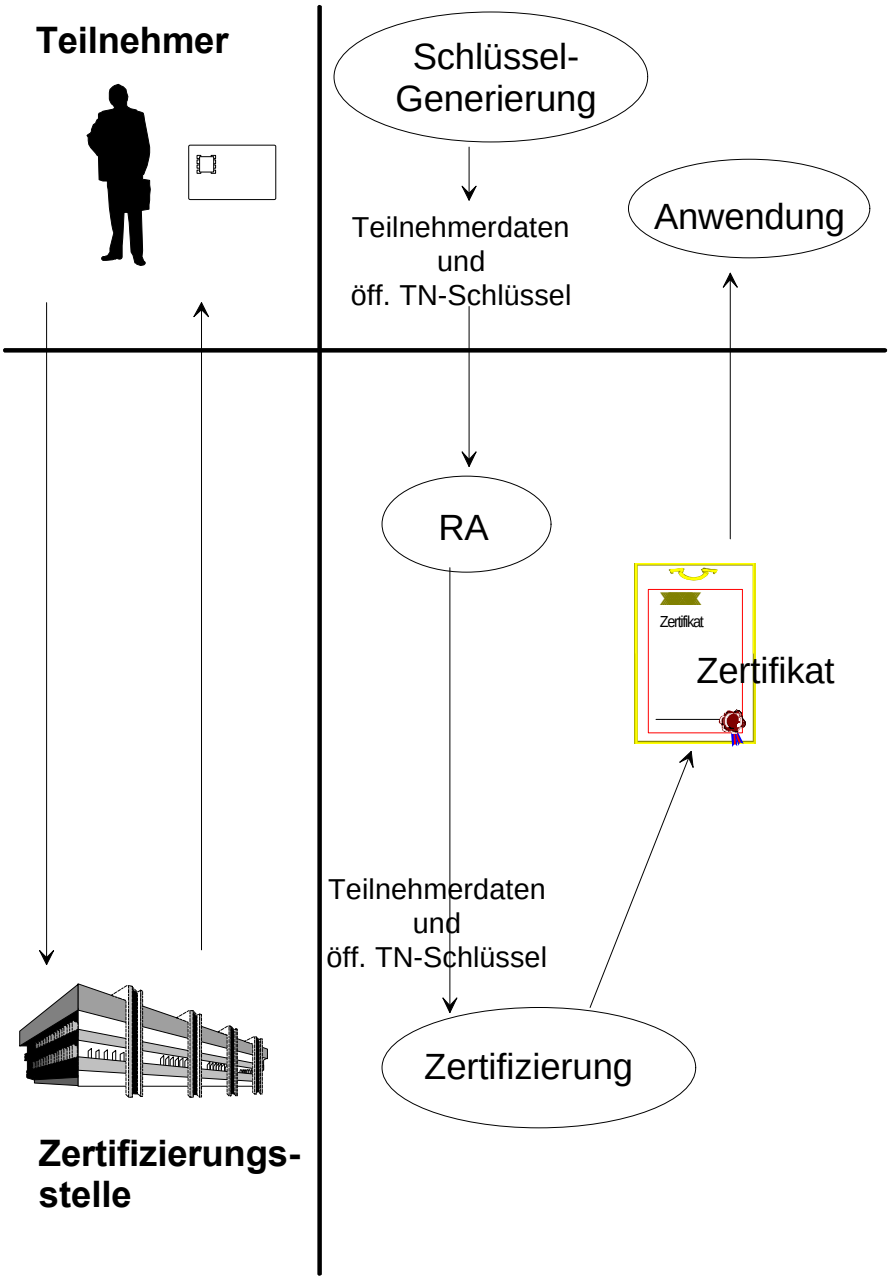
On handing over the signing component with the private user keys to the user, it is to be ensured

1. that either the signing component or the corresponding knowledge-based authentication data are handed over personally or, when signing component and authentication data are delivered at different times, that the second delivery is effected only after receiving written confirmation of receipt of the first delivery, and that
2. it is never possible for a person other than the entitled user to obtain possession of the signing component or of the appurtenant authentication data.

Receipt of the signing component is to be acknowledged and documented in each case. Only after due acknowledgement and documentation may the certificate be made available for verification in the directory.

[12] The user who has been assigned the key which is now compromised is to be notified and an appurtenant revocation entry is to be effected.

[13] Where appropriate, all these items may be provided together on the signing component.




**S-SICO 5.7 Identification of a user**

Identification can be carried out by various methods:

1. personal identification, on the basis of an identification document submitted to an RA or the CA or to an authorised third party,
2. in writing, when a contractual relationship already exists and a personal signature has been deposited, on condition that identification in accordance with 1. has taken place in connection with initial conclusion of the contract,
3. via digital signature, when the user possesses a certified public key of this CA.

Where statutory regulations permit variation of the above methods, e.g. on the basis of statutory powers of representation or guardianships or in the case of legal entities, the procedure may be modified accordingly.

The method of identifying a user must reliably verify that the user is actually the person he purports to be.

If the user already possesses a certified public key of a CA, he may submit his application for a certificate in digitally signed form. The signature is to be verified by the RA. On verification of the signature, no further identification shall be necessary. Due identification is to be documented.

### S-SICO 5.8 Identification and authentication of the operating personnel via knowledge and possession

Access to the IT systems specified in SigG/SigV and to the IT systems on which registration and all types of documentation within the meaning of SigG/SigV are carried out must be effected via knowledge and possession only.

### S-SICO 5.9 Verification of the uniqueness of the public key

Each submitted key is to be checked to verify whether it has already been assigned to another user within the same CA[14]. Key pairs which are no longer valid are also to be taken into account here. Duplicate keys are to be rejected. If an identical key is found which is still valid, the user concerned is to be notified accordingly and the appurtenant certificate is to be revoked.

### S-SICO 5.10 Records

All activities on the IT systems specified in SigG/SigV and on the IT systems on which registration and all types of documentation within the meaning of SigG/SigV are carried out are to be recorded in a manner providing protection against access and evaluated on a regular basis by a revisor.

### S-SICO 5.11 Requirements relating to applications for issuance of an attribute certificate

On applying for attribute certificates, the relevant attributes are to be specified and any declarations of consent from third parties are to be attached. The CA verifies the information and informs the third party concerned.

### S-SICO 5.12 Affixation of time stamps to certificates

Certificates must bear a time stamp providing information on the time of generation of the signature of the authority issuing the certificate, as the validity of user certificates is to remain unaffected by the revocation of a higher-priority certificate.

[14] Other CAs are not to be taken into account.

**S-SICO 5.13 Encoding for the exchange of sensitive data between systems**

When keys which require to be kept secret are exchanged between IT systems, such keys should be encoded as a general principle. An encoding method offering an appropriate level of security must be employed for this purpose.

In the course of transportation of the private certification key from the key generator to the certification computer, for example, it must be ensured that no individual person has access to the key in plain text. To this end, the key material which requires to be kept secret can be encoded or divided into two appropriate component parts, for example. Under no circumstances is an individual person then to have access to the correlated component parts in such a manner as to enable him to determine the private key.

**S-SICO 5.14 Generation of personalisation data to facilitate revocation management**

The only item of data which is absolutely essential on the signing component is the user's private signature key. For the purposes of the obligatory revocation management system it is, however, recommendable to supplement the private key and, where appropriate, the user key certificate with the following data:

1. the public key of the CA,
2. where appropriate, a reserve supply of public back-up keys of the CA,
3. the public key of the root authority,
4. the public key of the time stamping service,
5. the public key of the directory service and,
6. where appropriate, card-related data.

Knowledge-based authentication data are generated and activated for the signing component. These data are to be provided in protected form (e.g. in a PIN letter) for handover to the user. The signing component and, where appropriate, the PIN letter should be kept in closed archives until collected or dispatched.

**S-SICO 5.15 Utilisation of the time stamping service**

Time stamps for data without further specification or for digitally signed documents can be obtained from the time stamping service. These time stamps serve to provide authentic and irrevocable confirmation of the existence of the data concerned at the time of affixation of the time stamp.

The following procedure is required for this purpose:

- Non-confidential documents, including signature and any data which - from the user's point of view - are not confidential, are transmitted to the time stamping service. The time stamping service affixes the authentic time, signs the data with the time stamp signature key and returns everything to the user.

or

- Confidential documents, including signature and any confidential data, are hashed by the user using the hashing function which is declared valid by the time stamping service at the time of requesting the time stamp, and the hashed value is transmitted to the time stamping service. The latter affixes the authentic time, signs the data with the time stamp signature key and returns everything to the user. This procedure is also recommendable when time stamps are required for particularly extensive (non-confidential) documents, as then only the hashed value requires to be transmitted to the CA.

In order to facilitate revocation management in the event of compromise of the time stamping service (S-SICO 4.3), the following mechanisms can be applied with regard to the issuance of time stamps:

1. All submitted time stamp signatures are dependent on all or specific preceding time stamps. This results in a chronological sequence of time stamps into which it will not be possible to insert any back-dated time stamps, even in the event of the time stamping service being compromised.
2. All submitted time stamp signatures are documented in chronological order on a medium which permits writing once only (hashed value or plain text including time stamp signature). This documentation must be available for retrieval via public communications facilities after a case of compromise. The subsequent insertion of back-dated time stamps is not possible.
3. The time stamp key is changed on a daily basis. In the event of compromise, back-dating can be effected only to the day on which the compromised key was valid. All time stamps submitted on this day lose their validity. This solution reduces the scope for manipulation, but does not fully exclude manipulation. This mechanism furthermore involves extensive procedures for daily key-changing, and is thus of only limited suitability.

#### 5.4.2.6 General IT security safeguards

**S-SICO 6.1 IT baseline protection safeguards**

On the basis of the IT baseline protection manual of the BSI, provision is to be made for implementation of the safeguards proposed in the relevant chapters (see table below), in order to provide basic protection.

| | **Element** | **Certification authority** |
|---|---|---|
| 3.1 | Organisation | X |
| 3.2 | Personnel | X |
| 3.3 | Contingency Planning | X |
| 3.4 | Data Back-up concept | X |
| 4.1 | Buildings | X |
| 4.2 | Cabling | X |
| 4.3.1 | Office room | X |
| 4.3.2 | Server room | X1 |
| 4.3.3 | Storage Media Archives | X |
| 4.3.4 | Room for Technical Infrastructure | X |
| 4.4 | Protective Cabinets | X1 |
| 5.1 | DOS PC (single user) | A |
| 5.2 | Unix System | A |
| 5.3 | Portable PC | # |
| 5.4 | DOS PC (several users) | # |
| 5.5 | PC with Windows NT | A |
| 5.6 | PC with Windows 95 | A |
| 6.1 | Server-supported Network | A |
| 6.2 | Networked Unix System | A |
| 6.3 | Peer-to-peer Network | # |

| | | |
|---|---|---|
| 6.4 | Windows NT Network | A |
| 6.5 | Novell Netware 3.x | A |
| 7.1 | Exchange of Data Carriers | (X) |
| 7.2 | Modem | A |
| 7.3 | Firewall | X |
| 8.1 | Telecommunications System | (X) |
| 8.2 | Fax | (X) |
| 8.3 | Telephone Answering Machine | (X) |
| 9.1 | Standard software | A |

Legend:

X: to be observed
(X): to be observed, if installed
X1: A server room may be replaced by a server cabinet.
A: applicable if the certification authority's IT is implemented with this equipment
#: implementation does not appear expedient

## S-SICO 6.2 Security mechanisms of deployed IT systems

The IT systems deployed in accordance with § 14 SigG and § 16 SigV must possess a licence and confirmation pursuant to § 17 SigV and must support mechanisms specified in the table below. With regard to implementation of the necessary mechanisms it is to be ensured that the mechanisms cannot be bypassed and that they possess adequate resistance to manipulations or any other forms of attack.

| IT system / Mechanism | Key generation | Certification | Personalisation | Registration | Directory service | Time stamping service |
|---|---|---|---|---|---|---|
| Authentication/Identification | X | X | X | X | X | X |
| Access control | X | X | X | X | X | X |
| Record generation | X | X | X | X | X1) | X1) |
| Evaluation of records | X | X | X | X | X1) | X1) |
| Reprocessing | X | X | X | | X | X |
| Cryptographic mechanisms | X | X | X | | X | X |
| Integrity control | X | X | X | X | X | X |
| Fail-safe operation | | | | X | X | X |
| Reliability | X | X | X | X | X | X |
| Transmission security | | X | X | X | X | X |
| Data security | | | | X | X | X |

Note: The IT system number refers in each case to the sections below.
X denotes: appropriate mechanisms must be implemented.
1) a distinction is to be made between external and internal access

When the secrecy of keys or authentication parameters on an IT system cannot be guaranteed with adequate certainty, additional mechanisms which will detect any compromising of data automatically are to be implemented on the IT system concerned. When the possibility of

unauthorised access cannot be excluded with adequate certainty, additional safeguards are to be implemented to detect any manipulation automatically.

**S-SICO 6.3 Documentation**

The documentation to be drafted and updated by a certification authority comprises:

1. the security concept,
2. check reports on the security concept of the body approved by the competent authority,
3. contractual agreements between user and certification authority,
4. the CA's own certificates and all user certificates, specifying the times of issue,
5. applications for certificates and copies of the appurtenant identification papers,
6. pseudonyms,
7. a record of the information contained in attribute certificates,
8. a record confirming due notification,
9. the time of handover of the certificate and the confirmation of handover,
10. revocation of certificates,
11. information supplied to entitled parties in accordance with § 12 (2) SigG and
12. the time of handover of the signing component, with confirmation of handover.

The mode and manner of documentation must permit verification of and inquiries relating to the certificates at any time and for a period of at least 35 years. This requirement does not apply to information supplied in accordance with § 12 (2) SigG, which must be documented in verifiable form for a period of one year only. The components required for this purpose must also be available and in an operational condition for the same duration. Documentation in digital form is to be signed digitally.

The security concept must be incorporated into the documentation in such a manner as to enable it to be updated. Documentation relating to identification decisions is to specify by whom and according to what method identification was carried out.

**S-SICO 6.4 Application of a management system**

The management system must be capable of recording all procedures on the basis of the individual user and the involved CA employees, from the initial application through to handover of the signing component, verifying the plausibility of all these procedures and providing information on the status of an application on a continual basis. The various times relating to specific activities are to be recorded by the management system (e.g. the time of handover of the certificate). Integrity-assuring mechanisms which exclude the possibility of accidental or intentional losses of integrity or manipulations are also to be implemented.

When information on third parties is involved, the management system must require verification of the third party's consent, and when a signing component with externally generated keys is submitted the management system must require a confirmation pursuant to § 17 SigV. When these preconditions are not fulfilled, the management system must prevent further processing of the application.

**S-SICO 6.5 Establishment of a notification and information system**

The following points are to be observed:

- Third parties are to be notified of submitted information which relates to them.
- Entitled parties are to be provided with pseudonymised user names on request and attendant notifications are to be recorded.

**S-SICO 6.6 Drafting of a concept for the instruction of users**

Instruction of the user is to take place prior to handover of the signing component and/or the certificate and at an adequate standard of quality. In the course of this instruction, the user is to be notified in writing of the aspects covered in § 4 SigV. The relevant risks and security safeguards are also to be explained in the course of a personal meeting.

**S-SICO 6.7 Organisation of a security concept pursuant to § 4 (3) SigG**

The security concept must specify the planned security and the established security which requires to be maintained at the CA in a comprehensible manner and thus provide the basis for an independent security check. In the event of changes which are of relevance to security, the security concept must be adapted and, where appropriate, checked once again. A responsible party is to be designated for this task. The required contents of such a security concept are outlined below by way of example:

General information

1. Specification of the model (centralised/decentralised, branch offices, services offered by third parties, etc.)
2. Identification of properties which are of relevance to security
3. Allocation of the services to branch offices and properties

For each property:

1. Location and local conditions (layout plans, etc.)
2. Security safeguards for the outer skin
3. Building plan, specifying infrastructural security safeguards (danger alarm systems, access control facilities, cabling)
4. Specification of the personnel and the organisational structure
5. Stipulation of responsibilities:
   - general manager/holder of overall responsibility,
   - IT security officer,
   - review officer,
   - person responsible for change management regarding the security concept,
6. ...

General and property-oriented structural analysis

1. Cryptographic aspects:
   - Specification of the employed algorithms, including relevant parameters:
     - signature algorithms,
     - hashing algorithms,
     - authentication protocols,
     - algorithms for transport encoding
   - Confirmation of suitability of the employed algorithms,
   - Presentation of the employed key model (cf. fig. for S-SICO 3.3)
   - Key management (key changing, key transport, revocation management),
   - etc.
2. Specification of CA procedures:
   - Registration and identification
   - Key generation (internal/external)
   - Generation of certificates
   - Personalisation
   - Handover procedures for the signing component
   - Internal and external accesses to the directory service

- Internal and external accesses to the time stamping service
- Revocation management
- Any additional services
- Change management for the security concept and
- Revision.

3. Specification of the deployed components with reference to § 14 SigG:
   - Description of the components
   - Confirmation of suitability
   - Installation site
   - Operational configuration
   - Networking
   - Confirmation of compliance with the security requirements for operation
   - Operating personnel
   - ...
4. Specification of other deployed components:
   - Description
   - Installation site
   - Operational configuration
   - Networking
   - Operating personnel
   - ...
5. Presentation of the organisational structure:
   - Implementation of the planned CA procedure in conjunction with the available infrastructure, the personnel and the technical components
   - Data flow analysis.

Individual security concept

1. Description of individual security requirements:
   - Generic security requirements stipulated in the Act and the Ordinance
   - Derivation of the individual security requirements for the specific form of implementation
2. Detailed assessment of protection requirements
3. IT baseline protection concept:
   - Identification of relevant elements
   - Table of implemented safeguards,
   - Table of outstanding or only partially implemented safeguards
4. Individual risk analysis and selection of safeguards:
   - Specification of the realistic threats which apply in the actual given circumstances
   - Relevance and probability of occurrence of these threats
   - Estimation of potential damage on these threats materialising
   - Identification of potential risks
   - Specification of all security safeguards undertaken beyond the scope of IT baseline protection, in particular:
     - infrastructural safeguards,
     - organisational safeguards and arrangements,
     - personnel-related safeguards,
     - technical safeguards,
     - communications-related safeguards,

- business continuity safeguards and
- insurance coverage.

5. Checking of implemented safeguards via comparison with the safeguards recommended in the catalogue:
- Table of recommended safeguards which have been implemented
- Table of deviations from recommended safeguards and
- Statement of reasons for deviations, including security level.

6. Residual risk analysis:
- Substantiation of fulfilment of the individual security requirements
- Presentation of prevailing residual risks
- Substantiation of acceptability of residual risks.

Other aspects

1. Liability arrangements
2. Contractual arrangements between CA and user
3. Special legal aspects
4. Specification of procedures for instructing users
5. ...

### 5.4.3 Assignment of Safeguards to Solutions

| **Safeguard** | **Counteracts threat** | **Centralised/ decentralised model*** |
|---|---|---|
| S-SICO 1.1 | 2, 3, 7 | required |
| S-SICO 1.2 | 2, 3, 7 | required |
| S-SICO 1.3 | 2, 3 | required |
| S-SICO 1.4 | 2, 3 | required |
| S-SICO 2.1 | 2, 3, 4, 21 | required |
| S-SICO 2.2 | 2, 3, 4, 16, 17, 21 | required |
| S-SICO 2.3 | 2, 3, 4, 21 | required |
| S-SICO 3.1 | 3, 4, 10, 11, 13 | not required |
| S-SICO 3.2 | 4, 5, 10, 11, 13, 16, 17 | not required |
| S-SICO 3.3 | 10, 12, 14 | not required |
| S-SICO 3.4 | 10, 12 | not required |
| S-SICO 3.5 | 2, 3, 10, 21 | required |
| S-SICO 4.1 | 2, 8, 12 | required |
| S-SICO 4.2 | 2, 8, 9 | required |

| | | |
|---|---|---|
| S-SICO 4.3 | 2, 12, 14 | required |
| S-SICO 5.1 | 3, 11 | not required |
| S-SICO 5.2 | 11 | not required |
| S-SICO 5.3 | 2 | required |
| S-SICO 5.4 | 2, 3, 7 | required |
| S-SICO 5.5 | 2, 3, 4, 5, 11, 13, 19, 20, 21 | required |
| S-SICO 5.6 | 2, 3, 4, 5, 11, 13, 19, 20, 21 | required |
| S-SICO 5.7 | 2, 4, 5, 16, 17 | required |
| S-SICO 5.8 | 2, 3, 7 | required |
| S-SICO 5.9 | 2, 18 | required |
| S-SICO 5.10 | 2, 7, 13 | required |
| S-SICO 5.11 | 2, 4, 15 | required |
| S-SICO 5.12 | 6, 12 | not required |
| S-SICO 5.13 | 2, 3 | required |
| S-SICO 5.14 | 2, 14 | required |
| S-SICO 5.15 | 2, 12 | required |
| S-SICO 6.1 | 1, 3 | not required |
| S-SICO 6.2 | 2, 7, 8 | required |
| S-SICO 6.3 | 2, 9, 13, 15, 16 | required |
| S-SICO 6.4 | 4, 5, 9, 15, 16 | not required |
| S-SICO 6.5 | 15 | not required |
| S-SICO 6.6 | 2, 22 | required |
| S-SICO 6.7 | 2, 3, 8 | required |

* Assignment of the safeguards is independent of the model.

### 5.4.4 Assignment of safeguards to the security requirements

| Security requirements/ recommendations | Safeguards |
|---|---|
| REQ-SICO 1 | S-SICO 3.1, S-SICO 3.4 |
| REQ-SICO 2 | S-SICO 3.1 |
| REQ-SICO 3 | S-SICO 3.1 |
| REQ-SICO 4 | all safeguards which are required for the selected model, cf. table in chapter 5.4.3 |
| REQ-SICO 5 | S-SICO 3.1, S-SICO 3.4, S-SICO 5.11 |
| REQ-SICO 6 | S-SICO 3.1, S-SICO 3.2, S-SICO 3.3, S-SICO 3.4, S-SICO 5.3 |
| REQ-SICO 7 | S-SICO 3.6, S-SICO 5.15 |
| REQ-SICO 8 | S-SICO 3.1, S-SICO 5.11, S-SICO 6.4, S-SICO 6.5 |
| REQ-SICO 9 | S-SICO 3.1, S-SICO 3.2, S-SICO 5.5, S-SICO 5.6 |
| REQ-SICO 10 | S-SICO 5.3, S-SICO 5.4, S-SICO 5.5, S-SICO 5.6, S-SICO 5.7, S-SICO 5.10, S-SICO 6.3 |
| REQ-SICO 11 | S-SICO 3.2, S-SICO 5.5, S-SICO 5.6 |
| REQ-SICO 12 | S-SICO 3.2, S-SICO 5.5, S-SICO 5.6, S-SICO 6.3 |
| REQ-SICO 13 | S-SICO 5.5, S-SICO 5.6, S-SICO 6.4 |
| REQ-SICO 14 | S-SICO 5.5, S-SICO 5.6, S-SICO 5.9 |
| REQ-SICO 15 | S-SICO 5.9 |
| REQ-SICO 16 | S-SICO 3.2, S-SICO 5.5, S-SICO 5.6, S-SICO 5.7 |
| REQ-SICO 17 | S-SICO 3.2, S-SICO 5.7, S-SICO 6.3 |
| REQ-SICO 18 | S-SICO 2.1, S-SICO 2.3, S-SICO 3.2, S-SICO 5.5, S-SICO 5.6, S-SICO 5.7, S-SICO 5.10, S-SICO 6.3 |
| REQ-SICO 19 | S-SICO 3.1, S-SICO 5.5, S-SICO 5.6 |
| REQ-SICO 20 | S-SICO 5.10, S-SICO 6.3, S-SICO 6.4 |
| REQ-SICO 21 | S-SICO 1.1, S-SICO 1.2, S-SICO 1.3, S-SICO 2.1, S-SICO 2.3, S-SICO 3.5, S-SICO 5.5, S-SICO 5.6 |
| REQ-SICO 22 | S-SICO 3.5, S-SICO 5.5, S-SICO 5.6 |
| REQ-SICO 23 | S-SICO 6.6 |
| REQ-SICO 24 | S-SICO 4.3, S-SICO 6.6 |

| | |
|---|---|
| REQ-SICO 25 | S-SICO 6.3, S-SICO 6.5 |
| REQ-SICO 26 | S-SICO 3.3, S-SICO 4.1, S-SICO 4.3 |
| REQ-SICO 27 | S-SICO 3.3, S-SICO 4.1, S-SICO 4.3 |
| REQ-SICO 28 | S-SICO 1.1, S-SICO 1.2, S-SICO 3.3, S-SICO 4.3, S-SICO 5.8, S-SICO 5.10 |
| REQ-SICO 29 | S-SICO 3.3, S-SICO 4.3, S-SICO 5.10, S-SICO 6.3 |
| REQ-SICO 30 | S-SICO 4.2, S-SICO 4.3, S-SICO 5.14, S-SICO 6.3 |
| REQ-SICO 31 | S-SICO 4.3, S-SICO 5.2, S-SICO 5.12 |
| REQ-SICO 32 | S-SICO 6.3 |
| REQ-SICO 33 | S-SICO 4.1, S-SICO 4.2, S-SICO 6.3 |
| REQ-SICO 34 | S-SICO 6.3 |
| REQ-SICO 35 | S-SICO 6.3 |
| REQ-SICO 36 | S-SICO 1.1, S-SICO 1.2, S-SICO 5.4, S-SICO 5.8, S-SICO 5.10, S-SICO 6.1 |
| REQ-SICO 37 | S-SICO 5.3, S-SICO 6.2, S-SICO 6.3, S-SICO 6.7 |
| REQ-SICO 38 | S-SICO 6.1, S-SICO 6.7 |
| REQ-SICO 39 | S-SICO 1.1, S-SICO 1.2, S-SICO 1.3, S-SICO 1.4, S-SICO 2.1, S-SICO 2.2, S-SICO 2.3, S-SICO 3.1, S-SICO 3.5, S-SICO 5.1, S-SICO 5.4, S-SICO 5.13 |
| REQ-SICO 40 | S-SICO 1.1, S-SICO 1.2, S-SICO 1.3, S-SICO 1.4, S-SICO 2.1, S-SICO 2.2, S-SICO 2.3, S-SICO 3.1, S-SICO 3.3, S-SICO 3.4, S-SICO 3.5, S-SICO 5.1, S-SICO 5.4, S-SICO 5.5, S-SICO 5.6, S-SICO 5.7, S-SICO 5.13 |
| REQ-SICO 41 | S-SICO 3.3 |
| REQ-SICO 42 | S-SICO 3.3 |
| REQ-SICO 43 | S-SICO 3.3 |
| REQ-SICO 44 | S-SICO 2.1, S-SICO 2.2 |
| REQ-SICO 45 | S-SICO 1.1, S-SICO 1.2, S-SICO 1.3, S-SICO 1.4, S-SICO 5.3, S-SICO 5.4 |
| REQ-SICO 46 | S-SICO 1.1, S-SICO 1.2, S-SICO 1.3, S-SICO 1.4, S-SICO 2.2, S-SICO 3.5, S-SICO 5.5, S-SICO 5.6, S-SICO 5.13 |
| REQ-SICO 47 | S-SICO 1.1, S-SICO 1.2 |
| REQ-SICO 48 | S-SICO 6.2 |
| REQ-SICO 49 | S-SICO 6.2 |

| | |
|---|---|
| REQ-SICO 50 | S-SICO 6.2 |
| REQ-SICO 51 | S-SICO 6.2 |
| REQ-SICO 52 | S-SICO 6.2 |
| REC-SICO 1 | S-SICO 3.1, S-SICO 3.2, S-SICO 6.7 |
| REC-SICO 2 | S-SICO 3.5, S-SICO 4.3, S-SICO 5.5, S-SICO 5.6, S-SICO 5.14, S-SICO 6.7 |
| REC-SICO 3 | S-SICO 1.1, S-SICO 1.2, S-SICO 4.3, S-SICO 5.8, S-SICO 5.10, S-SICO 6.3 |
| REC-SICO 4 | S-SICO 6.1 |
| REC-SICO 5 | S-SICO 2.3, S-SICO 5.3, S-SICO 5.4 |
| REC-SICO 6 | S-SICO 2.2 |
| REC-SICO 7 | S-SICO 2.3 |
| REC-SICO 8 | S-SICO 1.1, S-SICO 1.2, S-SICO 1.3, S-SICO 3.1 |

## Literature

[ISO11770-3] Key Management: Part 3: Mechanisms using asymmetric techniques, ISO/IEC Draft 1996

[ISO14516-2] Guidelines for the use and management of Trusted Third Parties - Part 2: Technical aspects, ISO/IEC Draft 1995

[BSI97] Bundesamt für Sicherheit in der Informationstechnik (publisher): IT-Grundschutzhandbuch 1997, Federal German Law Gazette, Cologne 1997

[RFC1422] Kent, S., 'Privacy Enhancement for Internet Electronic Mail: Part II: Certificate-Based Key Management', RFC 1422, BBN, February 1993.

[X.509] ITU-T Recommendation X.509 (1993), Information technology - Open Systems Interconnection - The directory: authentication framework

[X.509v3] ITU-T Recommendation X.509, Information technology - Open Systems Interconnection - The directory: authentication framework, amendment 1: Certificate Extensions, Final Draft 1996

# 6. Safeguard catalogue pursuant to § 16 (6) SigV

## 6.1 Cryptographic algorithms

The security of a digital signature depends primarily on the strength of the applied cryptographic algorithms. This section describes the algorithms which are considered suitable by the BSI. The bit-accurate specifications are to be found in the appropriate standards of various organisations (ISO/IEC, NIST, IEEE etc.), and do not fall within the scope of this document.

### 6.1.1 Requirements Stipulated in the Act and the Ordinance

| Reference | Quotation | Interpretation |
|---|---|---|
| **§ 17 (2) SigV (see also explanatory note on § 17 (2) SigV)** | The competent authority shall publish in the Federal Gazette an overview of the algorithms and pertinent parameters considered suitable for generation of signature keys, for hashing of data to be signed or for generation and verification of digital signatures; such published information shall include the date until which the suitability is valid.<br>[...] Suitability shall be determined in keeping with provisions of the Federal Agency for Security in Information Technology, taking relevant international standards into account. Experts from the areas of industry and science shall be consulted in this regard. | The suitable algorithms and appurtenant parameters are described below. |
| **§ 2 (1) SigG (see also explanatory note on § 2 (1) SigG)** | For the purposes of this Act "digital signature" shall mean a seal affixed to digital data which is generated by a private signature key and establishes the holder 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 of this Act. | This is the definition of a digital signature. |

| | | |
|---|---|---|
| **§ 16 (1) SigV (see also explanatory note on § 16 (1) SigV)** | The technical components required for generation of signature keys must function in such a manner that it is nearly certain that any given key can occur only once and that a private key cannot be derived from the relevant public key. The secrecy of private keys must be assured, and it must not be possible to duplicate keys. Security-relevant changes in technical components must be apparent for the user. | This provision concerns secure key generation. |

The following pages specify cryptographic algorithms which, in the view of the BSI, are to be regarded as suitable for digital signatures for the **next six years** (at least). We have restricted the selected algorithms to the most important algorithms of relevance to practical applications, the cryptographic characteristics of which can be assessed most effectively on the basis of the currently available results of many years of discussion.

The certification authorities may apply processes which involve algorithms other than those proposed here, provided that the suitability of these algorithms in accordance with the provisions of the German Information Security Agency is confirmed by the competent authority.

The list of algorithms stated here is to be regarded as incomplete and provisional. It will be updated and, where appropriate, supplemented in accordance with the further course of development in the field of cryptological research and experience acquired with the practical implementation of signature processes.

### 6.1.2 Cryptographic Requirements

A digital signature scheme within the meaning of the Act comprises the following cryptographic algorithms:

- a fast algorithm for hashing data (a hash function) which reduces the data to be signed to a hashed value, i.e. a bit sequence of a fixed short length. In each case it is then not the data themselves which are signed, but their hashed value,
- a signature algorithm, consisting of a signing and a verification algorithm. The signature algorithm is dependent on a key pair, comprising a private (i.e. secret) key for signing (generating a signature) and the appurtenant public key for verifying (checking) the signature, and
- a process for generating key pairs for the individual users.

Such a scheme is secure when only the holder of the private key is able to generate a signature which the verification algorithm will identify as valid (this relates here only to the abstract mathematical characteristics of the scheme; security problems which may occur in concrete technical implementation have been left aside here). The following sections outline the resultant requirements for the above-stated cryptographic algorithms:

#### 6.1.2.1 Hash functions

On submitting a signature, the hashed value of the data to be signed is used, as it were, as a 'digital fingerprint'. In order to prevent a gap in security here, the hash function, *H*, must satisfy the following criteria:

- *H* must be a *one-way function*; i.e. it must be practically impossible to find a pre-image for *H* for a given bit string from the value range, and
- *H* must be *collision-resistant*; i.e. it must be practically impossible to find collisions (two different digital documents mapped onto the same hashed value form a collision).

The existence of collisions and - assuming that the hash function behaves in a pseudo-random manner and is thus surjective - the existence of pre-images is unavoidable. This is only a theoretical statement, however. For the purposes of practical application, the sole criterion is, as required above, that it should be impossible to *find* collisions and pre-images.

#### 6.1.2.2 Signature algorithms

No-one other than the holder of the signature key must be able to generate signatures. In particular, this means that it must be practically impossible to calculate the signature key from the (public) verification key.

#### 6.1.2.3 Key generation

The different signature algorithms require keys which fulfil certain conditions. In some instances additional conditions apply, the failure to observe which could lead to weaknesses in the process concerned. In accordance with these requirements, the keys must be generated randomly (see section 6.1.5).

### 6.1.3 Proposals for suitable hashing functions

Hash function MD4 was introduced by Ron Rivest in 1990 ([9], [6]). The design places a very strong emphasis on good performance and is geared especially to the 32-bit processors which are very widespread today. MD4 has three internal rounds. A number of additional, more complex hash functions (with a larger number of rounds) have subsequently been proposed in due course on the basis of the MD4 design principles. The hash functions of this MD4 family have undergone highly intensive investigation in recent years. While MD4 has proven to lack collision resistance, essentially on account of the insufficient number of rounds, on the basis of the findings of analysis work to date the following two hash functions of the MD4 family may be assumed to offer long-term security:

- RIPEMD-160 ([7], [3]),
- SHA-1 ([2], [3]).

In the view of the BSI, these two hashing functions will be suitable for application in the area of digital signatures for the **next six years** (at least), i.e. until 2003.

### 6.1.4 Proposals for suitable signature algorithms

In 1977, Rivest, Shamir and Adleman were the first to describe a method for generating digital signatures in explicit terms. This is the RSA method, which was thus named after its inventors [10]. In 1984, El'gamal [8] proposed a different signature algorithm. A variant of this El´gamal method is the Digital Signature Standard (DSS) published by the National Institute of Standards in Technology (NIST) in 1991 [1], which specifies the digital signature algorithm (DSA). A relatively new development takes the form of variants of the DSA based on point groups E(K) of elliptic curves over finite fields, whereby $K = F_p$ is a finite prime field and $K = F_{2^m}$ is a finite field of characteristic 2.

In the view of the BSI, the following signature algorithms are suitable:

1. RSA [10],
2. DSA [1]
3. DSA variants, based on elliptic curves:
    - ISO/IEC 14883-3 [4], Annex A.2.2 ('Agnew-Mullin-Vanstone analogue'),
    - IEEE-Standard P1363 [5], Section 5.3.3 ('Nyberg-Rueppel version'),
    - IEEE-Standard P1363 [5], Section 5.3.4 ('DSA version').

This also applies to other methods described in ISO/IEC 14883-3 [4]. Some of these methods will probably be taken into account in future versions of this document.

In each instance, the security of the above-stated methods is connected with

1. the factorisation problem for integers,
2. the discrete logarithm problem (DLP) in the multiplicative group of prime fields $F_p$,
3. the DLP in groups of the form $E(F_p)$ or $E(F_{2^m})$.

In order to define the size of system parameters which is required to guarantee the security of these methods, the best algorithms which are presently known for factorizing integers and calculating discrete logarithms (in the above-stated groups) must be considered, together with the performance capability of present-day computer technology. To enable an assessment of security for a certain period in the future, a forecast for the two stated aspects is additionally required. Such forecasts are only possible for relatively short periods (and may, of course, turn out to be incorrect at any time as a result of dramatic, unforeseen developments).

In the view of the BSI, the security of the respective methods is ensured for the **next six years** (at least), i.e. until 2003, if the parameters are selected as follows:

1. **RSA**

   The basic module $n = pq$ ($p$ and $q$ prime numbers) should have a bit length of at least 1024:

   $\log_2(n) = \log_2(p) + \log_2(q) \geq 1024$.

   For the period of the **next 3 years**, a minimal length for the module of 768 Bit is sufficient:

   $\log_2(n) \geq 768$.

   The prime factors $p$ and $q$ of n should be of roughly the same magnitude, but should not be too close together, i.e. in concrete terms roughly

$0.5 < \left|\log_2(p) - \log_2(q)\right| < 30$

The prime factors *p* and *q* are generated randomly independently of one another, observing the stated secondary conditions.

The public exponent *e* is selected as $ggT(e,(p-1)(q-1)) = 1$. The appurtenant secret exponent, *d* is then calculated such that $ed \equiv 1 \bmod (p-1)(q-1)$.

Comments:

1. The requirement for *p* and q to be *strong* prime numbers (i.e. $p-1$ and $q-1$ have large prime factors, etc.) no longer appears adequately substantiated, in view of the best factorisation algorithms known today.

2. In principle, the public exponent should be selected randomly. On the other hand, small public exponents have the advantage that verification of the signature can be carried out very quickly. Provided that the hashed value is appropriately formatted, i.e. expansion of the hashed value to the block width of the asymmetric method, no risk is known here (in contrast to encoding with small exponents).

2. **DSA**

FIPS-186 requires a bit length of at least 512 and at most 1024 for the parameter *p* (*p* prime number). The BSI proposes 1024 bit as the lower limit:

$\log_2(p) \geq 1024$.

See [1] with regard to the generation of *p* and the other parameters. The DSA requires a bit length of 160 for the parameter *q*. This permits the construction of 'collisions' within the meaning of Serge Vaudenay ('Hidden collisions in DSS', Proceedings of Crypto'96, Lecture Notes in Computer Science, Vol. 1109, published by Springer Verlag, 1996, pp. 83-88) in the course of parameter generation. BSI considers these collisions to have no significance in practice, however. If one wishes to exclude the possibility of constructing these collisions, $\log_2(q) > 160$ must be selected.

3. a) **DSA variants based on** $E(F_p)$

In order to define the system parameters, an elliptic curve *E* and a point *P* are generated on the basis of $E(F_p)$ such that the following conditions apply:

- with a prime number *q* which differs from *p* and

$$\log_2(q) \geq 160.$$

- $ord(P) = q$.
- $r_0 := \min(r : q \text{ divides } p^r - 1)$ is large, in concrete terms roughly $r_0 > 10^4$.
- The class number of the ring endomorphism of *E* is at least 100.

Comment: The lower estimation for $r_0$ is intended to exclude attacks based on imbedding of the subgroup generated by *P* in the multiplicative group of a field $F_{p^r}$. Generally (when

random selection of the elliptic curve is carried out), this estimate is fulfilled, as $r_0$ is the order of $p \pmod q$ in $F_q^*$ and thus generally even has the same order of magnitude as $q$. Ideally, $r_0$ should be determined explicitly, though this requires the somewhat more complex factorisation of $q-1$. By comparison, $r_0 > 10^4$ can be verified substantially more quickly and is considered to be adequate in this context.

3. b) **DSA variants based on $E(F_{2^m})$**

In order to define the system parameters, an elliptic curve $E$ and a point $P$ are generated on the basis of $E(F_{2^m})$ such that the following conditions apply:

- $E(F_{2^m})$ is not definable in any proper subfield of $F_{2^m}$ (i.e. the j-invariant of the curve does not lie in a proper subfield of $F_{2^m}$).
- $\#E(F_{2^m}) = a \cdot q$, with $q$ prime and

$$\log_2(q) \geq 160 .$$

- $ord(P) = q$.
- $r_0 := \min(r : q \text{ divides } 2^{mr} - 1)$ is large, in concrete terms roughly $r_0 > 10^4$.
- The class number of the ring endomorphism of $E$ is at least 100.

Comment: With regard to the above-mentioned 'collisions' within the meaning of Vaudenay, the same applies to methods based on elliptic curves as to DSA.

### 6.1.5 Generation of random numbers

Random numbers are required in the generation of system parameters for signature algorithms and key generation. When DSA-type signature algorithms are used, a new random number is required each time a new signature is generated.

Suitable random number generators for these purposes are systems which incorporate

- a physical noise source and
- cryptographic (or mathematical) post-treatment of the primary noise.

Adequate description of the process for extracting the bits from the physical noise source should be possible by means of a stochastic model. The primary noise should be subjected to an adapted statistical test on a continuous basis, insofar as this is technically feasible. The mathematical post-treatment should resolve model-related dependencies.

A physical random number generator should always be used for key generation.

When no physical random number generator is available for other applications (e.g. signing with a DSA variant), a pseudo-random generator represents a possible alternative. This generator must be initialised by a genuine random number (seed). The decisive criterion is that a bit sequence taken from the pseudo-random generator - similarly to a bit sequence generated by physical chance - must fulfil the following requirement:

- no information is ascertainable a priori as to the bits which are generated. The knowledge of a partial sequence permits no inferences with regard to the remaining bits.

Every digital signature method becomes non-secure when the employed random number generator does not fulfil the stated requirements. Every random number generator is thus to be examined carefully with regard to its suitability. Extensive experience is required, in order to carry out a meaningful assessment of a random number generator. The BSI possesses such experience, and it is recommended to utilise the BSI's know-how in this connection.

A very useful compilation of practical criteria and tips for random number generators and pseudo-random generators is to be found in [5], Section G.

## Literature


[1] NIST: FIPS Publication 186: Digital Signature Standard (DSS), May 1994

[2] NIST: FIPS Publication 180-1: Secure Hash Standard (SHS-1), May 1995

[3] ISO/IEC 10118-3: Information technology - Security techniques - Hash functions - Part 3: Dedicated hash functions, draft, 1997

[4] ISO/IEC 14888-3: Information technology - Security techniques - Digital signatures with appendix - Part 3: Certificate-based mechanisms, draft, 1997

[5] IEEE: P1363 Standard (Draft), 6th February 1997

[6] Request for Comments (RFC) 1320: The MD4 message-digest algorithm, R. Rivest, Internet Activities Board, Internet Privacy Task Force, April 1992

[7] H. Dobbertin, A. Bosselaers, B. Preneel: RIPEMD-160: A strengthened version of RIPEMD, Fast Software Encryption - Cambridge Workshop 1996, LNCS, Band 1039, S. 71 - 82, Springer-Verlag, 1996. (The final version is to be found via ftp at: ftp.esat.kuleuven.ac.be/pub/COSIC/bosselae/ripemd/)

[8] T. El'gamal: A public key cryptosystem and a signature scheme based on discrete logarithms, Crypto '84, LNCS, Volume 196, pp. 10 - 18, published by Springer-Verlag, 1985

[9] R. Rivest: The MD4 message digest algorithm, Crypto ’90, LNCS, Volume 537, pp. 303 - 311, published by Springer-Verlag, 1991

[10] R. Rivest, A. Shamir, L. Adleman: A method for obtaining digital signatures and public key cryptosystems, Communications of the ACM, vol. 21 no. 2, 1978

## 6.2 Key Generation and Key Certification

To enable participation in the digital signature process a key pair is generated for each user, comprising a private and a corresponding public signature key. Generation of the signature keys must be carried out under particularly secure conditions, as the knowledge of a private signature key enables certificates to be manipulated and misused.

The contents of the certificate belonging to the public user key include an identification characteristic for the user, the public signature key allocated to the user and the validity period of the certificate. The contents of the certificate are authentically combined via the digital signature, which is generated by means of the CA's private key. Generation of the certificate belonging to the public user key must also take place under particularly secure conditions, in order to prevent the generation of false or forged certificates.

The following section summarises the requirements and recommendations which are stipulated in the Act and the Ordinance in order to ensure the secrecy of private signature keys and secure generation of the certificate for the public user key.

### 6.2.1 Requirements stipulated in the Act and the Ordinance

| Reference | Quotation | Interpretation |
|---|---|---|
| **§ 2 (1) SigG** | For the purposes of this Act "digital signature" shall mean a seal affixed to digital data which is generated by a private signature key and establishes the holder 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 of this Act. | Explanation of the procedure employed to generate a digital signature: the digital signature within the meaning of this Act is generated with the aid of the private (secret) signature key and can be verified with the public key. In each case, therefore, a key pair requires to be generated (cf. Section 6.1).<br>Derived requirement REQ-KG 2.1. |
| **§ 2 (3) SigG** | For the purposes of this Act "certification authority" shall mean 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 of this Act. | The public component of the key pair is provided with a digital signature of an appropriately authorised body. This guarantees authentication of the assignment of a public key to a natural person.<br>Derived requirement: REQ-KG 2.2. |

| | | |
|---|---|---|
| **§ 5 (1) SigG** | The certification authority shall reliably establish the identity of persons applying for a certificate. It shall confirm the assignment of a public signature key to an identified person by a signature key certificate which, together with any attribute certificates, shall be kept available for verification and, with the consent of the holder of the signature key, for retrieval at all times and for everyone over publicly available telecommunication links. | The certification authority is responsible for issuing signature key certificates and attribute certificates.<br>Derived requirement: REQ-KG 2.2. |
| **§ 5 (2) SigG** | At an applicant's request the certification authority shall include in the signature key certificate or an attribute certificate information relating to his authority to represent a third party and to his professional admission to practice or other type of admission insofar as reliable proof is furnished of the consent by the third party to the inclusion of the authority of representation or of the admission. | Under the conditions specified here, the certification authority is obliged to include additional information in the certificate or to generate an attribute certificate.<br>Derived requirement: REQ-KG 2.2. |
| **§ 5 (3) SigG** | At an applicant's request the certification authority shall indicate a pseudonym instead of the applicant's name in the certificate. | Derived requirement: REQ-KG 2.2. |
| **§ 5 (4) SigG** | The certification authority shall take safeguards to prevent undetected forgery or manipulation of the data intended for certificates. It shall also take safeguards to ensure confidentiality of private signature keys. Storage of private signature keys by the certification authority shall not be permitted. | Precautions are to be taken at the CA to prevent the undetected forgery or manipulation of data for certificates. It is imperative that the private signature keys be kept secret. The possibility of private signature keys being stored after personalisation is to be eliminated.<br>Derived requirements: REQ-KG 1.1, REQ-KG 1.2, REQ-KG 1.3, REC-KG 2.1. |
| **§ 5 (5) SigG** | The certification authority shall engage reliable staff for the exercise of certification activities. For the provision of signature keys and the issue of certificates it shall use technical components as set out in § 14. This shall also apply to technical components enabling verification of certificates according to § 5 (1) sentence 2 above. | With regard to the use of technical components, reference is made to § 14 SigG.<br>Derived requirement: REQ-KG 1.8. |

| | | |
|---|---|---|
| **§ 7 (1) SigG** | The signature key certificate shall contain the following information:<br>1. name of the holder of the signature key to which additional information must be appended in the event of possible confusion, or a distinctive pseudonym assigned to the holder of the signature key, clearly marked as such,<br>2. public signature key assigned,<br>3. names of the algorithms with which the public key of the holder of the signature key and the public key of the certification authority can be used,<br>4. serial number of the certificate,<br>5. beginning and end of the validity period of the certificate,<br>6. name of the certification authority, and<br>7. an indication as to whether use of the signature key is restricted in type or scope to specific applications. | The elements of a certificate are stipulated here.<br>Derived requirement: REQ-KG 2.3. |
| **§ 7 (2) SigG** | Information relating to the authority to represent a third party and to the professional admission to practice or other type of admission may be included both in the signature key certificate and in an attribute certificate. | The incorporation of attributes into the signature key certificate or into a supplementary attribute certificate is possible.<br>Derived requirement: REQ-KG 2.2. |
| **§ 7 (3) SigG** | Further information shall not be included in the signature key certificate unless the parties concerned give their consent. | When information beyond that specified in § 7 (1) and (2) is to be included in the certificate, the consent of the parties concerned is to be obtained. The unintentional and unauthorised addition of data to the personalisation data record must be prevented.<br>Derived requirement: REQ-KG 2.4 |
| **§ 10 SigG** | The certification authority shall document the security safeguards for compliance with this Act and the ordinance having the force of law pursuant to §16 and the certificates issued in a manner such that the data and their integrity can be verified at all times. | Adequate documentation of the operations of certification authorities is required for verification purposes. In particular, certificates must be documented in a forgREC-Proof manner.<br>Derived requirement: REQ-KG 2.5. |

| | | |
|---|---|---|
| **§ 14 (1) SigG** | Technical components with safeguards are required for the generation and storage of signature keys and for the generation and verification of digital signatures which reliably reveal forged digital signatures and manipulated signed data and provide protection against unauthorised use of private signature keys. | This imposes requirements on the components to be employed for the purposes of key generation and certificate generation (use of evaluated and confirmed components, etc.).<br>Derived requirement: REQ-KG 1.4. |
| **§ 14 (4) SigG** | Technical components according to § 14 (1) to (3) above shall be adequately tested against current engineering standards and their compliance with requirements confirmed by a body recognised by the competent authority. | In order to ensure that the employed components comply with current engineering standards at all times, they should undergo repeat checks (evaluations) in which they will be required to fulfil the latest technical criteria.<br>Derived requirements: REQ-KG 1.4, REQ-KG 1.9, REQ-KG 1.10, REC-KG 1.1. |
| **§ 5 (1) SigV** | If the signature key holder generates signature keys, the certification authority shall reliably establish whether the signature key holder uses suitable technical components, pursuant to the Digital Signature Act and this Ordinance, for storage and use of the private signature key. | The generation of private signature keys by the user must be carried out by means of PSEs, the suitability of which the CA is subsequently able to ascertain.<br>Derived requirement: REQ-KG 1.11. |
| **§ 5 (2) SigV** | If the certification authority provides signature keys, this authority shall take precautions to prevent any disclosure of private keys and any storage of private keys by the certification authority. Similar precautions shall also apply to personal identification numbers and other data used to identify the signature key holder in conjunction with the data storage medium with the private signature key. | Private signature keys must be destroyed at the CA after personalisation.<br>Derived requirement: REQ-KG 1.12. |
| **§ 11 SigV** | The certification authority shall take precautions to protect the following from unauthorised access: private signature keys, and the technical components used to prepare the certificates and time stamps and to ensure that certificates can be checked at any time. | Access to technical components and to data by unauthorised persons must be prevented at the CA. Appropriate technical, material and organisational protection mechanisms are to be applied to this end.<br>Derived requirement: REQ-KG 1.13. |

| | | |
|---|---|---|
| **§ 16 (1) SigV** | The technical components required for generation of signature keys must function in such a manner that it is nearly certain that any given key can occur only once and that a private<br><br>key cannot be derived from the relevant public key. The secrecy of private keys must be assured, and it must not be possible to duplicate keys. Security-relevant changes in technical components must be apparent for the user. | This provision imposes high requirements on the components to be employed for key generation. The mechanisms to be applied for key generation must guarantee that the same private signature key cannot be generated more than once. The mathematical algorithms suitable for use in the generation of digital signatures must guarantee that the private signature key cannot be derived from the public key. The secrecy of the private signature key is to be guaranteed at all times. In order to exclude the possibility of misuse, no duplicates may be made of the secret signature keys.<br><br>Derived requirements: REQ-KG 1.5 to REQ-KG 1.7. |
| **§ 16 (2) SigV** | The technical components required for generation or verification of digital signatures must function in such a manner that the private signature key cannot be derived from the signature and the signature cannot be forged by any other means. Use of the private signature key must be possible only following identification of the holder and must require proper possession and knowledge; the key must not be disclosed during use. Biometrical characteristics may also be used for identification of the signature key holder. The technical components required for collecting identification data must function in such a manner that they do not reveal identification data and that the identification data is stored only on the data storage medium with the private signature key. Security-relevant changes in technical components must be apparent for the user. | The requirements pertaining to the technical components employed at the CA to generate digital signatures apply mutatis mutandis.<br><br>Derived requirement: REQ-KG 1.2. |

| | | |
|---|---|---|
| **§ 17 (1) SigV** | Testing of technical components pursuant to § 14 (4) of the Digital Signature Act must conform to the ";Criteria for assessment of the security of information technology systems"; (GMBl. 1992, S. 545). For technical components for generation of signature keys or for storage or use of private signature keys, and for technical components commercially provided to third parties for use, such tests must conform to the "E4" test standard; otherwise, they must conform to the "E2" test standard. The strength of the security mechanisms must be rated as "high"; and the algorithms and pertinent parameters must be assessed as suitable pursuant to (2). | This provision imposes requirements regarding the standard and depth of evaluation for the technical components to be deployed.<br><br>Derived requirement: REQ-KG 1.9. |
| **Explanatory note on § 17 (1) SigV** | The technical components to be tested and the requirements applying to these components are finalised in § 16.<br><br>The stated criteria ('Information Technology Security Evaluation Criteria - ITSEC') represent an international standard for evaluating the security of information technology components and systems (see also Council Recommendation 95/144/EC of 7th April 1995). These criteria distinguish between the testing and evaluation stage (with a scale ranging from 'E 1' to 'E 6') and the strength of the mechanisms applied to attain the security objectives (differentiated as low, medium and high). They are supplemented by the Information Technology Security Evaluation Manual - ITSEM', which has not been published in the Federal German law gazette, but which is known to the competent experts. Should practically tested new criteria emerge in the future, the Ordinance will be adapted as necessary.<br><br>With regard to the decisive strength of the mechanisms, the Ordinance requires the level 'high' throughout, and with regard to the algorithms and appurtenant parameters in accordance with subsection 2 the Ordinance additionally requires express confirmation of suitability. The preconditions for | The explanatory note on § 17 (1) SigV clearly requires 'E4 high' as the evaluation level for technical components to generate keys, including the loading process.<br><br>Derived requirement: REQ-KG 1.9. |

| | | |
|---|---|---|
| | evaluation of a mechanism as 'high' are described as follows in the ITSEC: 'To enable the minimum strength of a critical mechanism to be classified as high, it must be discernible that the mechanism concerned can only be overcome by aggressors who possess very good specialist knowledge, opportunities and equipment, whereby such a successful attack is assessed as normally unfeasible.'<br><br>Varying requirements are imposed with regard to the test standard, according to the different risks. The high test standard 'E 4' is required for those technical components which serve to maintain the security of the signature keys and the secrecy of the private signature key, and for technical components which are made available for use to third parties on a commercial basis. In both cases, concealed errors / manipulations may have broad-ranging consequences. On the other hand, clearly structured special components are involved here, in view of which the extensive testing (e.g. involving the production of a formal security modal) will entail an acceptable scope of work. Otherwise, the current standard test level 'E 2' (e.g. involving examination of implementation of the mechanisms, a weak-point analysis and fault location tests) appears adequate and acceptable in scope in accordance with current engineering standards. The same also applies to the technical components for checking a digital signature, as only the public key is employed for this purpose.<br><br>A minimum level of security is attained by the confirmation of suitability for the mathematical methods, the required 'high' rating for the strength of the security mechanisms and risk-related tests. These safeguards are supplemented by spot checks and repeat tests carried out in the form of expert opinions when specific circumstances so require, in accordance with subsection 3 sentence 3. The stipulated minimum levels for the test standards may be | |

| | | |
|---|---|---|
| | exceeded in the competitive environment, such as when special components for electronic banking are involved.<br><br>The following requirements thus apply to the individual technical components:<br><br>-Components for generating keys (incl. loading process)<br><br>E4 high<br><br>-Components for storage and application of the private signature key<br><br>E 4 high<br><br>-Other components to generate digital signatures, including<br><br>• recording and verification of identification data<br><br>• display of data to be signed<br><br>-Components to maintain certificates in verifiable form<br><br>E 2 high<br><br>-Components to generate time stamps<br><br>E 2 high<br><br>-Components to generate and verify digital signatures which are offered for use to third parties on a commercial basis<br><br>E 4 high.<br><br>The algorithms and appurtenant parameters must comply with the requirements specified in subsection 2. | |

| | | |
|---|---|---|
| **§ 17 (3) SigV** | Confirmation of fulfilment of requirements for technical components pursuant to § 14(4) of the Digital Signature Act must include mention of the following: for which requirements pursuant to §16 the confirmation applies and within what usage environment; what algorithms and pertinent parameters pursuant to (2) were used and until when, at the least, these algorithms and pertinent parameters will be suitable; the security standard in accordance with which the technical components pursuant to (1) were tested. A copy of the test report and the confirmation shall be submitted to the competent authority. If this authority has reason to suspect there are deficiencies in testing or in confirmed technical components, the authority may obtain an expert opinion from an independent third party to determine if the technical components were tested pursuant to (1) and whether the technical components fulfil the requirements of the Digital Signature Act and this Ordinance; the authority may also obtain such expert opinions as part of spot checks. Affected manufacturers, sellers and testing agencies shall provide necessary support in this connection. If such support is not provided, or if it is revealed that confirmed technical components were not adequately tested or do not fulfil requirements, the competent authority is entitled to rescind the validity of issued confirmations. | When deficiencies in technical components are established or suspected, the components concerned are to undergo renewed testing. The competent authority can and should additionally arrange for spot checks to be carried out. This applies in particular to technical components for generating key material.<br><br>Derived requirements: REQ-KG 1.10, REC-KG 1.1. |

### 6.2.2 Security requirements and recommendations

#### 6.2.2.1 Requirements relating to the key- and certificate-generating system

REQ-KG 1.1 The certification authority is to take precautions to prevent the forgery or manipulation of data.
cf.: § 5 (4) SigG
Safeguards pertaining to this requirement: S-KG 1.1 to S-KG 3.4

REQ-KG 1.2 The certification authority is to take precautions to ensure the secrecy of the private signature keys.
cf.: § 5 (4) SigG, § 16 (2) SigV
Safeguards pertaining to this requirement: S-KG 1.1 to S-KG 1.4, S-KG 1.9, S-KG 2.1 to S-KG 2.3, S-KG 3.1, S-KG 3.3

REQ-KG 1.3 No private signature keys are to be stored at the CA after completion of the personalisation process.
cf.: § 5 (4) SigG
Safeguards pertaining to this requirement: S-KG 1.2, S-KG 1.3, S-KG 2.2, S-KG 2.3

REQ-KG 1.4 For the purposes of generating and storing signature keys and generating and evaluating digital signatures, technical components incorporating security safeguards are required which reliably disclose forgeries of digital signatures and manipulations of signed data and provide protection against the unauthorised use of private signature keys.
cf.: § 14 (1), (4) SigG
Safeguards pertaining to this requirement: S-KG 1.3, S-KG 1.7, S-KG 1.8, S-KG 2.1 to S-KG 2.3

REQ-KG 1.5 The technical components required for the generation of signature keys must be designed in such a manner that a signature key will, with the utmost probability, occur once only (cf. Section 6.1).
cf.: § 16 (1) SigV
Safeguards pertaining to this requirement: S-KG 2.2, S-KG 2.3

REQ-KG 1.6 The secrecy of the private signature keys must be guaranteed, and they must not be duplicated.
cf.: § 16 (1) SigV
Safeguards pertaining to this requirement: S-KG 1.1 to S-KG 1.4, S-KG 1.7, S-KG 1.9, S-KG 2.1 to S-KG 2.3, S-KG 3.1, S-KG 3.3

REQ-KG 1.7 Changes to the technical components which are of relevance to security must be apparent to the user.
cf.: § 16 (1) SigV
Safeguards pertaining to this requirement: S-KG 1.3, S-KG 1.7, S-KG 2.2, S-KG 2.3

REQ-KG 1.8 The certification authority is to deploy technical components pursuant to § 14 SigG for the provision of signature keys and for the generation of certificates.
cf.: § 5 (5) SigG
Safeguards pertaining to this requirement: S-KG 2.2

REQ-KG 1.9 Technical components are to be deployed which have undergone adequate evaluation in accordance with current engineering standards and whose fulfilment of the stipulated requirements (evaluation standard 'E 4 high') has been confirmed by a body which is recognised by the competent authority.
cf.: § 14 (4) SigG, § 17 (1) SigV, explanatory note on § 17 (1) SigV
Safeguards pertaining to this requirement: S-KG 2.2, S-KG 2.3

REQ-KG 1.10 The confirmation of fulfilment of the requirements for technical components is to be reviewed in the event of established or suspected deficiencies in technical components.
cf.: § 17 (3) SigV
Safeguards pertaining to this requirement: S-KG 2.2, S-KG 2.3

REQ-KG 1.11 When signature keys are generated by the signature key holder, the certification authority is to ensure that the key holder employs suitable technical components for this purpose and for storage and application of the private signature key.
cf.: § 5 (1) SigV
Safeguards pertaining to this requirement: S-KG 2.2, S-KG 3.3

REQ-KG 1.12 When signature keys are provided by the certification authority, the latter is to take precautions to prevent the disclosure of private keys and storage at the certification authority. This also applies to personal identification numbers or other data to identify the signature key holder to the data storage medium containing with the private signature key.
cf.: § 5 (2) SigV
Safeguards pertaining to this requirement: S-KG 1.2, S-KG 1.4 to S-KG 3.1

REQ-KG 1.13 The certification authority is to take precautions to protect private signature keys and the technical components employed to generate certificates and time stamps and to keep the certificates available for verification against unauthorised access.
cf.: § 11 SigV
Safeguards pertaining to this requirement: S-KG 1.4 to S-KG 1.7, S-KG 1.9 to S-KG 2.3

REC-KG 1.1 The competent authority should additionally arrange for spot checks to be carried out on the confirmed technical components.
cf.: § 17 (3) SigV
Safeguards pertaining to this requirement: S-KG 2.3

#### 6.2.2.2 Requirements relating to the key- and certificate-generation procedures

REQ-KG 2.1 Key pairs in accordance with Section 6.1 must be generated for the digital signature process.
cf.: § 2 (1) SigG
Safeguards pertaining to this requirement: S-KG 2.2, S-KG 2.3, S-KG 3.3

REQ-KG 2.2 The certification authority is to confirm the assignment of a public signature key to an identified person by means of a signature key certificate and, on request from the applicant, the certification authority is to include additional information in the certificate or in an attribute certificate.
cf.: § 2 (3) SigG, § 5 (1) SigG, § 5 (2) SigG, § 5 (3) SigG, § 7 (2) SigG
Safeguards pertaining to this requirement: S-KG 2.2, S-KG 3.4

REQ-KG 2.3 The signature key certificate must contain the following information at least:
1. name of the holder of the signature key to which additional information must be appended in the event of possible confusion, or a distinctive pseudonym assigned to the holder of the signature key, clearly marked as such,
2. public signature key assigned,
3. names of the algorithms with which the public key of the holder 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.
cf.: § 7 (1) SigG
Safeguards pertaining to this requirement: S-KG 3.4

REQ-KG 2.4 When information beyond the scope of that specified in § 7 (1) and (2) SigG is to be included in the certificate, the consent of the parties concerned is to be obtained. The unintentional or unauthorised addition of data to the personalisation data record must furthermore be prevented.
cf.: § 7 (3) SigG
Safeguards pertaining to this requirement: S-KG 1.3, S-KG 1.4, S-KG 1.7, S-KG 2.1 to S-KG 2.3, S-KG 3.1, S-KG 3.2

REQ-KG 2.5 The certification authority is to document the security safeguards and the issued certificates in such a manner as to ensure that the data themselves can be verified and verification that they have not been manipulated can be obtained at any time.
cf.: § 10 SigG
Safeguards pertaining to this requirement: S-KG 1.1, S-KG 2.2

REC-KG 2.1 The memory areas in which personalisation data are processed are to be erased after the completion of personalisation.
cf.: § 5 (4) SigG
Safeguards pertaining to this requirement: S-KG 1.2

### 6.2.3 Proposed solutions

Key generation can be carried out centrally at the CA and in decentralised mode at the RA or by the user. Certificate generation is always carried out centrally at the CA. Two viable models are considered here:

A) Central key generation and central certificate generation

B) Decentralised key generation and central certificate generation
(cf. example personalisation procedure for a PSE in the model *'Decentralised* key generation in the PSE')

The emphasis falls on different requirements, according to the applied model.

### 6.2.4 Safeguard catalogue

#### 6.2.4.1 Threats

The following enumeration does not draw a strict distinction between threats as defined in ITSEC and any vulnerabilities which may be exploitable as a result of implementation. Equally, the enumeration is certainly not to be regarded as complete or final.

##### 6.2.4.1.1 Threats concerning key generation

1.Use of unsuitable key generators.
Safeguards: S-KG 2.2, S-KG 2.3, S-KG 3.3
2. Generation of unsuitable signature keys.
Safeguards: S-KG 1.1, S-KG 1.3, S-KG 2.2, S-KG 2.3
3. Generation of duplicate signature keys.
Safeguards: S-KG 1.1, S-KG 1.3, S-KG 2.2, S-KG 2.3
4. Compromise of signature key data.
Safeguards: S-KG 1.1 to S-KG 1.4, S-KG 1.7, S-KG 1.9, S-KG 2.1 to S-KG 2.3, S-KG 3.1, S-KG 3.3
5. Duplication of signature key data.
Safeguards: S-KG 1.1, S-KG 1.2, S-KG 1.4, S-KG 1.7, S-KG 1.9, S-KG 2.1 to S-KG 2.3, S-KG 3.1 to S-KG 3.3
6. Theft of signature key data.
Safeguards: S-KG 1.2, S-KG 1.4 to S-KG 1.7, S-KG 2.1 to S-KG 2.3, S-KG 3.1, S-KG 3.3
7. Non-secure handover of signature key data.
Safeguards: S-KG 1.3, S-KG 1.8, S-KG 2.1 to S-KG 2.3, S-KG 3.1, S-KG 3.3
8. Read-out of signature key data.
Safeguards: S-KG 1.2, S-KG 1.4, S-KG 1.7, S-KG 1.9, S-KG 2.1 to S-KG 2.3, S-KG 3.1, S-KG 3.3
9. Non-secure reserves of signature keys.
Safeguards: S-KG 1.2 to S-KG 1.4, S-KG 2.1 to S-KG 2.3, S-KG 3.3
10. Uncontrolled abortion of signature key generation.
Safeguards: S-KG 1.1, S-KG 1.3, S-KG 2.2, S-KG 2.3

11. Any form of uncontrolled signature key generation.
    Safeguards: S-KG 1.1, S-KG 1.3, S-KG 1.5, S-KG 2.2, S-KG 2.3
12. Maloperation of the signature key generating system.
    Safeguards: S-KG 1.3, S-KG 2.2, S-KG 2.3
13. Technical faults during signature key generation.
    Safeguards: S-KG 1.3, S-KG 2.2, S-KG 2.3
14. Manipulation of the key generating system.
    Safeguards: S-KG 1.1 to S-KG 1.3, S-KG 1.5, S-KG 1.6, S-KG 1.7, S-KG 2.1 to S-KG 2.3, S-KG 3.1, S-KG 3.3
15. Unauthorised use of the key generating system.
    Safeguards: S-KG 1.1, S-KG 1.3, S-KG 1.5, S-KG 1.6, S-KG 2.1 to S-KG 2.3
16. Compromising emanation of data relevant to security.
    Safeguards: S-KG 1.9, S-KG 2.2, S-KG 2.3, S-KG 3.1
17. Manipulation of signature key data.
    Safeguards: S-KG 1.4 to S-KG 1.8, S-KG 2.1 to S-KG 2.3, S-KG 3.1 to S-KG 3.4
18. Misuse of signature key data.
    Safeguards: S-KG 1.2, S-KG 1.4, S-KG 1.7, S-KG 2.1 to S-KG 2.3, S-KG 3.1 to S-KG 3.4

#### 6.2.4.1.2 Threats concerning the generation of certificates

1. Use of unsuitable technical components.
   Safeguards: S-KG 2.2, S-KG 2.3, S-KG 3.3
2. Compromise of personalisation data.
   Safeguards: S-KG 1.1 to S-KG 1.9, S-KG 2.1 to S-KG 2.3, S-KG 3.1, S-KG 3.3
3. Duplication of personalisation data.
   Safeguards: S-KG 1.1, S-KG 1.2, S-KG 1.4, S-KG 1.7, S-KG 1.9, S-KG 2.1 to S-KG 2.3, S-KG 3.1 to S-KG 3.3
4. Mix-up of personalisation data.
   Safeguards: S-KG 1.1 to S-KG 1.4, S-KG 1.8, S-KG 2.1 to S-KG 2.3, S-KG 3.1, S-KG 3.3
5. Processing of faulty personalisation data records.
   Safeguards: S-KG 1.1, S-KG 1.3, S-KG 1.8, S-KG 2.2, S-KG 2.3
6. Theft of personalisation data.
   Safeguards: S-KG 1.2, S-KG 1.4 to S-KG 1.7, S-KG 1.9, S-KG 2.1 to S-KG 2.3, S-KG 3.1, S-KG 3.3
7. Non-secure handover of personalisation data.
   Safeguards: S-KG 1.3, S-KG 1.8, S-KG 2.1 to S-KG 2.3, S-KG 3.1, S-KG 3.3
8. Uncontrolled abortion of certificate generation.
   Safeguards: S-KG 1.1, S-KG 1.3, S-KG 2.2, S-KG 2.3
9. Any form of uncontrolled certificate generation.
   Safeguards: S-KG 1.1, S-KG 1.3, S-KG 2.2, S-KG 2.3
10. Maloperation of the certificate generating system.
    Safeguards: S-KG 1.3, S-KG 2.2, S-KG 2.3

11. Technical faults during certificate generation.
    Safeguards: S-KG 1.3, S-KG 2.2, S-KG 2.3
12. Manipulation of the certificate generating system.
    Safeguards: S-KG 1.1 to S-KG 1.7, S-KG 2.1 to S-KG 2.3
13. Unauthorised use of the certificate generating system.
    Safeguards: S-KG 1.1, S-KG 1.3 to S-KG 1.7, S-KG 2.1 to S-KG 2.3
14. Compromising emanation of data relevant to security.
    Safeguards: S-KG 1.9, S-KG 2.2, S-KG 2.3, S-KG 3.1
15. Manipulation of personalisation data.
    Safeguards: S-KG 1.4 to S-KG 1.8, S-KG 2.1 to S-KG 2.3, S-KG 3.1 to S-KG 3.3
16. Misuse of personalisation data.
    Safeguards: S-KG 1.2, S-KG 1.7, S-KG 1.9, S-KG 2.1 to S-KG 2.3, S-KG 3.1, S-KG 3.2, S-KG 3.4

#### 6.2.4.2 Safeguards

##### 6.2.4.2.1 Safeguards relating to the key- and certificate-generating system

**S-KG 1.1 Recording of events**

The deployed technical components are able to record each of the following events together with the specified data:

- Utilisation of the identification and authentication mechanism:
  Required data: Date, time, submitted user ID, indication of the technical component on which identification and authentication were carried out, and success or failure of the attempt.
- Attempted access to an object subject to the administration of rights:
  Required data: Date, time, user ID, name of the object, type of attempted access, success or failure of the attempt.
- Actions by authorised personnel which affect the security of the technical components or of the PSE:
  Required data: Date, time, user ID, type of action (e.g. insertion or deletion of data, insertion or removal of data storage media, etc.) and name of the object to which the action related.

The record data are accessible to the system revisor only (cf. S-KG 1.6) for the purpose of evaluation.

**S-KG 1.2 Erasure of used memory areas**

Memory areas employed during the generation of keys and certificates are erased automatically after the completion of processing in the system in such a manner (e.g. by overwriting the memory contents with a random bit pattern) as to eliminate the possibility of inference of their former contents.

**S-KG 1.3 Signalling of malfunctions**

Malfunctions are indicated to the personnel by clear acoustic and/or optical signals. The mechanisms which are evaluated in the systems for this purpose include:

- failed identification and authentication processes,
- checking of all data storage media for viruses when operating systems are booted,
- integrity tests on employed software,

- integrity tests on stored data,
- failure checking and self-tests of employed hardware,
- evaluation of tamper protection mechanisms, and
- procedural and status assessment of operating activities.

**S-KG 1.4 Encoding of data storage media**

Signature key data or personalisation data on data storage media belonging to the key generation and certificate generation environment are protected against unauthorised disclosure by means of appropriate encoding.

**S-KG 1.5 Identification and authentication**

The personnel must identify and authenticate itself to the key and certificate generating systems by means of possession and knowledge (e.g. chipcard and PIN). Operation of the systems is possible only after successful identification and authentication.

**S-KG 1.6 Access control**

The personnel of the key and certificate generating environment at the CA and the decentralised RA discharges the functions of system administrator, system revisor and operating personnel. The system administrator is responsible for administration of the key and certificate generating system. Only the system administrator is able and authorised to assign the rights of the operating personnel. The revisor is responsible for evaluation of the record data. Only the revisor is able to obtain access to the record data. The operating personnel carries out the tasks which apply during the key and certificate generation process. No individual may be assigned more than one of the stated functions at the same time. The key and certificate generating systems must verify the appropriate rights of the personnel and reject unauthorised attempts to gain access.

**S-KG 1.7 Tamper protection**

The technical components deployed at the CA are secured against manipulations which require the component housing to be opened by means of tamper protection safeguards. Opening the housing interfaces will result, for example, in the automatic erasure of data which are critical to security (e.g. key data) and the output of optical and/or acoustic alarms.

**S-KG 1.8 Integrity of data transport**

All data are signed for the purposes of transportation within the CA (and within decentralised RAs) and their integrity is subsequently checked by the receiving system. When it is not possible to establish the integrity of data, the action concerned is recorded, the data record is rejected, the sender is notified and requested to send the data again. The integrity of data records to be signed is checked directly prior to certificate generation.

**S-KG 1.9 Prevention of compromising emanation**

The technical components employed at the CA are protected against emanation and confirmed accordingly. When systems and components are networked, it is to be ensured that the appurtenant cabling is protected against emanation (shielded cables) and/or the data to be transmitted is to be encoded for the transmission process.

#### 6.2.4.2.2 Safeguards relating to organisation of the key- and certificate-generating environment

**S-KG 2.1 Secure networking of systems**

Within the certification authority, the systems are networked with other areas of the CA in due compliance with strict security requirements. The data lines are to be secured against tapping (e.g. by means of line encoding, protected cabling, etc.). In order to reliably prevent read-out of the personalisation data from CA areas, the lines must not be connected to external networks. Connection to distributed offices (e.g. decentralised RAs) via encoded dedicated lines is possible.

**S-KG 2.2 Deployment of suitable system components**

Only hardware and software components which have been evaluated and found to be suitable by authorised evaluating bodies are employed in the key and certificate generating environment.

**S-KG 2.3 Review of deployed system components**

The deployed system components are subjected to renewed evaluation on a spot-check basis and when deficiencies are suspected. Aspects which arise in the course of technological change are also to be taken into consideration here. The deployed technical components must satisfy all security-related requirements of current engineering standards. Should the requirements not be fulfilled, the issued confirmation will be declared invalid.

#### 6.2.4.2.3 Safeguards relating to key- and certificate-generating procedures

**S-KG 3.1 Transport encoding of key and personalisation data**

All signature keys and personalisation data are transmitted to the personalisation system in transport-encoded form and are not decoded until they reach the PSE.

**S-KG 3.2 Safeguarding of key and personalisation data**

The data records generated in the key and certificate generating systems are secured against manipulation and forgery by means of appropriate methods (e.g. MAC, digital signature).

**S-KG 3.3 Key generation in the PSE**

The key pairs comprising private/public signature keys are generated within the PSE. Only the public key is output from the PSE in authentic, non-corrupted form. The certification authority is able to verify the authentic origin of the generated private signature key (e.g. via an authentication record or a digital signature). The private signature is secured against read-out and is stored in the PSE only.

**S-KG 3.4 Contents of certificates**

The signature key certificate contains the following information at least:

1. name of the holder of the signature key to which additional information must be appended in the event of possible confusion, or a distinctive pseudonym assigned to the holder of the signature key, clearly marked as such,
2. public signature key assigned,
3. names of the algorithms with which the public key of the holder 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.

#### 6.2.4.3 Assignment of the safeguards to solutions

| **Safeguard** | **Counteracts threat** | | **Solution model** | |
|---|---|---|---|---|
| | **Key generation** | **Certificate generation** | **A)** | **A)** |
| S-KG 1.1 | 2-5,10,11,14,15 | 2-5,8,9,12,13 | required | required |
| S-KG 1.2 | 4,5,6,8,9,14,18 | 2,3,4,6,12,16 | required | required |
| S-KG 1.3 | 2,3,4,7,9-15 | 2,4,5,7-13 | required | required |
| S-KG 1.4 | 4,5,6,8,9,17,18 | 2,3,4,6,12,13,15 | recommended | recommended |
| S-KG 1.5 | 6,11,14,15,17 | 2,6,9,12,13,15 | required | required |
| S-KG 1.6 | 6,14,15,17 | 2,6,12,13,15 | required | required |
| S-KG 1.7 | 4,5,6,8,14,17,18 | 2,3,6,12,13,15,16 | required | required |
| S-KG 1.8 | 7,17 | 2,4,5,7,15 | required | required |
| S-KG 1.9 | 4,5,8,16 | 2,3,6,14,16 | required | required |
| S-KG 2.1 | 4-9,14,15,17,18 | 2,3,4,6,7,12,13,15,16 | required | required |
| S-KG 2.2 | 1-18 | 1-16 | required | required |
| S-KG 2.3 | 1-18 | 1-16 | required | required |
| S-KG 3.1 | 4-8,14,16,17,18 | 2-4,6,7,14,15,16 | recommended | recommended |
| S-KG 3.2 | 5,17,18 | 3,15,16 | required | required |
| S-KG 3.3 | 1,4-9,14,17 | 1-4,6,7,15 | recommended | required |
| S-KG 3.4 | 17,18 | 15,16 | required | required |

#### 6.2.4.4 Assignment of the safeguards to the security requirements

| Security requirement/ recommendation | Safeguards |
|---|---|
| REQ-KG 1.1 | S-KG 1.1 to S-KG 3.4 |
| REQ-KG 1.2 | S-KG 1.1 to S-KG 1.4, S-KG 1.9, S-KG 2.1 to S-KG 2.3, S-KG 3.1, S-KG 3.3 |
| REQ-KG 1.3 | S-KG 1.2, S-KG 1.3, S-KG 2.2, S-KG 2.3 |
| REQ-KG 1.4 | S-KG 1.3, S-KG 1.7, S-KG 1.8, S-KG 2.1 to S-KG 2.3 |
| REQ-KG 1.5 | S-KG 2.2, S-KG 2.3 |
| REQ-KG 1.6 | S-KG 1.1 to S-KG 1.4, S-KG 1.7, S-KG 1.9, S-KG 2.1 to S-KG 2.3, S-KG 3.1, S-KG 3.3 |
| REQ-KG 1.7 | S-KG 1.3, S-KG 1.7, S-KG 2.2, S-KG 2.3 |
| REQ-KG 1.8 | S-KG 2.2 |
| REQ-KG 1.9 | S-KG 2.2, S-KG 2.3 |
| REQ-KG 1.10 | S-KG 2.2, S-KG 2.3 |
| REQ-KG 1.11 | S-KG 2.2, S-KG 3.3 |
| REQ-KG 1.12 | S-KG 1.2, S-KG 1.4 to S-KG 3.1 |
| REQ-KG 1.13 | S-KG 1.4 to S-KG 1.7, S-KG 1.9 to S-KG 2.3 |
| REC-KG 1.1 | S-KG 2.3 |
| REQ-KG 2.1 | S-KG 2.2, M.SZ 2.3, S-KG 3.3 |
| REQ-KG 2.2 | S-KG 2.2, S-KG 3.4 |
| REQ-KG 2.3 | S-KG 3.4 |
| REQ-KG 2.4 | S-KG 1.3, S-KG 1.4, S-KG 1.7, S-KG 2.1 to S-KG 2.3, S-KG 3.1, S-KG 3.2 |
| REQ-KG 2.5 | S-KG 1.1, S-KG 2.2 |
| REC-KG 2.1 | S-KG 1.2 |

## 6.3 Personalisation

The term 'personalisation' refers to the process whereby a personalisation data record is transferred to and stored on a suitable PSE (e.g. chipcard). The contents of the personalisation data record include the user data, the certificate for the public signature key, the public signature key of the CA and, where appropriate, the user's private signature key and the PIN.

The following section establishes the requirements and recommendations which are stipulated in the Digital Signature Act and the Digital Signature Ordinance in order to ensure the secrecy of the private signature keys and secure personalisation.

### 6.3.1 Requirements stipulated in the Act and the Ordinance

| Reference | Quotation | Interpretation |
|---|---|---|
| **§ 5 (4) SigG** | The certification authority shall take safeguards to prevent undetected forgery or manipulation of the data intended for certificates. It shall also take safeguards to ensure confidentiality of private signature keys. Storage of private signature keys by the certification authority shall not be permitted. | The dual control principle is to be required for all personalisation actions (exception: decentralised key generation by the user); it must be ensured that no private signature keys remain in the personalisation environment. Security safeguards are also to be undertaken to ensure the secure transmission of initialised and prREC-Personalised PSEs.<br>Derived requirements: REQ-P 1, REQ-P 2, REQ-P 3. |
| **§ 5 (5) SigG** | The certification authority shall engage reliable staff for the exercise of certification activities. For the provision of signature keys and the issue of certificates it shall use technical components as set out in § 14. This shall also apply to technical components enabling verification of certificates according to § 5 (1) sentence 2 above. | Technical components in accordance with § 14 SigG are to be used.<br>Derived requirement: REQ-P 4. |
| **§ 10 SigG** | The certification authority shall document the security safeguards for compliance with this Act and the ordinance having the force f law pursuant to §16 and the certificates issued in a manner such that the data and their integrity can be verified at all times. | Adequate documentation of the operations of certification authorities is required for verification purposes. In particular, certificates must be documented in such a manner that their contents and integrity can be verified at all times.<br>Derived requirements: REQ-P 7, REC-P 1. |

| | | |
|---|---|---|
| **§ 14 (1) SigG** | Technical components with safeguards are required for the generation and storage of signature keys and for the generation and verification of digital signatures which reliably reveal forged digital signatures and manipulated signed data and provide protection against unauthorised use of private signature keys. | This imposes requirements on the components to be deployed for personalisation (use of evaluated and confirmed components, etc.).<br>Derived requirements: REQ-P 4, REQ-P 5. |
| **§ 14 (4) SigG** | Technical components according to § 14 (1) to (3) above shall be adequately tested against current engineering standards and their compliance with requirements confirmed by a body recognised by the competent authority. | In order to ensure that the deployed components comply with 'current engineering standards' at all times, they should be tested not once only, but subjected to repeat tests (evaluations) in accordance with the prevailing technical requirements.<br>Derived requirements: REQ-P 4, REQ-P 5, REQ-P 9, REC-P 5. |
| **§ 5 (2) SigV** | If the certification authority provides signature keys, this authority shall take precautions to prevent any disclosure of private keys and any storage of private keys by the certification authority. Similar precautions shall also apply to personal identification numbers and other data used to identify the signature key holder in conjunction with the data storage medium with the private signature key. | After completion of the personalisation process, private keys must be destroyed at the CA.<br>Derived requirements: REQ-P 2, REQ-P 3. |
| **§ 11 SigV** | The certification authority shall take precautions to protect the following from unauthorised access: private signature keys, and the technical components used to prepare the certificates and time stamps and to ensure that certificates can be checked at any time. | Access to technical components and data by unauthorised persons must be prevented at the CA. Appropriate technical, material and organisational protection mechanisms are to be applied to this end.<br>Derived requirement: REQ-P 6. |

| | | |
|---|---|---|
| **§ 16 (1) SigV** | The technical components required for generation of signature keys must function in such a manner that it is nearly certain that any given key can occur only once and that a private key cannot be derived from the relevant public key. The secrecy of private keys must be assured, and it must not be possible to duplicate keys. Security-relevant changes in technical components must be apparent for the user. | It must also be ensured that the operating personnel in the personalisation environment obtain no knowledge of the private keys.<br><br>Manipulations must be detectable and duplication of the PSEs or personalisation data must be prevented (protection of the signature key: e.g. by the use of cryptological methods or generation and storage of the private signature key in the PSE in a manner which provides security against read-out).<br><br>Derived requirements: REQ-P 1, REQ-P 6. |
| **§ 16 (2) SigV** | The technical components required for generation or verification of digital signatures must function in such a manner that the private signature key cannot be derived from the signature and the signature cannot be forged by any other means. Use of the private signature key must be possible only following identification of the holder and must require proper possession and knowledge; the key must not be disclosed during use. Biometrical characteristics may also be used for identification of the signature key holder. The technical components required for collecting identification data must function in such a manner that they do not reveal identification data and that the identification data is stored only on the data storage medium with the private signature key. Security-relevant changes in technical components must be apparent for the user. | Only PSEs which are approved by the certification authority should be used.<br><br>Application of the private signature key must take place in the PSE and must require proof of proper possession and knowledge (PSE and PIN).<br><br>Additional personalisation of the PSE with biometric characteristics is possible.<br><br>Derived requirement: REQ-P 8. |

| | | |
|---|---|---|
| **§ 17 (1) SigV** | Testing of technical components pursuant to § 4 (4) of the Digital Signature Act must conform to the "Criteria for assessment of the security of information technology systems" (GMBl. 1992, S. 545). For technical components for generation of signature keys or for storage or use of private signature keys, and for technical components commercially provided to third parties for use, such tests must conform to the ";E4"; test standard; otherwise, they must conform to the ";E2"; test standard. The strength of the security mechanisms must be rated as ";high"; and the algorithms and pertinent parameters must be assessed as suitable pursuant to (2). | These provisions impose requirements on the evaluation standards for the technical components to be employed:<br>PSE → E4 high,<br>technical components in the personalisation environment → E4 high, (cf. explanatory note on SigV) when the personalisation data is not encoded for transmission purposes.<br>Derived requirement: REQ-P 4. |
| **Explanatory note on § 17 (1) SigV** | The technical components to be tested and the requirements applying to these components are finalised in § 16.<br>The stated criteria ('Information Technology Security Evaluation Criteria - ITSEC') represent an international standard for evaluating the security of information technology components and systems (see also Council Recommendation 95/144/EC of 7th April 1995). These criteria distinguish between the testing and evaluation stage (with a scale ranging from 'E 1' to 'E 6') and the strength of the mechanisms applied to attain the security objectives (differentiated as low, medium and high). They are supplemented by the Information Technology Security Evaluation Manual - ITSEM', which has not been published in the Federal German law gazette, but which is known to the competent experts. Should practically tested new criteria emerge in the future, the Ordinance will be adapted as necessary.<br>With regard to the decisive strength of the mechanisms, the Ordinance requires the level 'high' throughout, and with regard to the algorithms and appurtenant parameters in accordance with subsection 2 the Ordinance additionally | The explanatory note stipulates the evaluation standard 'E4 high' for technical components employed in key generation, including the loading process.<br>Derived requirement: REQ-P 4. |

| | | |
|---|---|---|
| | requires express confirmation of suitability. The preconditions for evaluation of a mechanism as 'high' are described as follows in the ITSEC: 'To enable the minimum strength of a critical mechanism to be classified as high, it must be discernible that the mechanism concerned can only be overcome by aggressors who possess very good specialist knowledge, opportunities and equipment, whereby such a successful attack is assessed as normally unfeasible.'<br><br>Varying requirements are imposed with regard to the test standard, according to the different risks. The high test standard 'E 4' is required for those technical components which serve to maintain the security of the signature keys and the secrecy of the private signature key, and for technical components which are made available for use to third parties on a commercial basis. In both cases, concealed errors / manipulations may have broad-ranging consequences. On the other hand, clearly structured special components are involved here, in view of which the extensive testing (e.g. involving the production of a formal security modal) will entail an acceptable scope of work. Otherwise, the current standard test level 'E 2' (e.g. involving examination of implementation of the mechanisms, a weak-point analysis and fault location tests) appears adequate and acceptable in scope in accordance with current engineering standards. The same also applies to the technical components for checking a digital signature, as only the public key is employed for this purpose.<br><br>A minimum level of security is attained by the confirmation of suitability for the mathematical methods, the required 'high' rating for the strength of the security mechanisms and risk-related tests. These safeguards are supplemented by spot checks and repeat tests carried out in the form of expert opinions when specific circumstances so require, in accordance with subsection 3 sentence 3. | |

| | | |
|---|---|---|
| | The stipulated minimum levels for the test standards may be exceeded in the competitive environment, such as when special components for electronic banking are involved.<br><br>The following requirements thus apply to the individual technical components:<br><br>-Components for generating keys (incl. loading process)<br><br>E4 high<br><br>-Components for storage and application of the private signature key<br><br>E 4 high<br><br>-Other components to generate digital signatures, including<br><br>• recording and verification of identification data<br><br>• display of data to be signed<br><br>-Components to maintain certificates in verifiable form<br><br>E 2 high<br><br>-Components to generate time stamps<br><br>E 2 high<br><br>-Components to generate and verify digital signatures which are offered for use to third parties on a commercial basis<br><br>E 4 high.<br><br>The algorithms and appurtenant parameters must comply with the requirements specified in subsection 2. | |

| | | |
|---|---|---|
| **§ 17 (3) SigV** | Confirmation of fulfilment of requirements for technical components pursuant to § 14(4) of the Digital Signature Act must include mention of the following: for which requirements pursuant to §16 the confirmation applies and within what usage environment; what algorithms and pertinent parameters pursuant to (2) were used and until when, at the least, these algorithms and pertinent parameters will be suitable; the security standard in accordance with which the technical components pursuant to (1) were tested. A copy of the test report and the confirmation shall be submitted to the competent authority. If this authority has reason to suspect there are deficiencies in testing or in confirmed technical components, the authority may obtain an expert opinion from an independent third party to determine if the technical components were tested pursuant to (1) and whether the technical components fulfil the requirements of the Digital Signature Act and this Ordinance; the authority may also obtain such expert opinions as part of spot checks. Affected manufacturers, sellers and testing agencies shall provide necessary support in this connection. If such support is not provided, or if it is revealed that confirmed technical components were not adequately tested or do not fulfil requirements, the competent authority is entitled to rescind the validity of issued confirmations. | When deficiencies in technical components are established or suspected, the components concerned are to undergo renewed testing. The competent authority can and should additionally arrange to have spot checks carried out. This applies in particular to technical components for generating key material.<br><br>Derived requirements: REQ-P 4, REQ-P 5, REQ-P 9, REC-P 5. |

### 6.3.2 Security requirements and recommendations

REQ-P 1 It must be ensured in the personalisation environment that personalisation data cannot be forged, altered, duplicated or misused in any other manner.
cf.: § 5 (4) SigG, § 16 (1) SigV
Safeguards pertaining to this requirement: S-P 1.1 to S-P 3.8

REQ-P 2 Private signature keys must not be stored in the personalisation environment for longer than is necessary for processing.
cf.: § 5 (4) SigG, § 5 (2) SigV
Safeguards pertaining to this requirement: S-P 1.5, S-P 2.2, S-P 2.3, S-P 3.1, S-P 3.8

REQ-P 3 The secrecy of the private signature keys must be guaranteed within the personalisation environment.
cf.: § 5 (4) SigG, § 5 (2) SigV
Safeguards pertaining to this requirement: S-P 1.5, S-P 1.7, S-P 1.8, S-P 2.1, S-P 2.2, S-P 2.3, S-P 3.1, S-P 3.2, S-P 3.4

REQ-P 4 Technical components which have undergone adequate testing in accordance with current engineering standards and received due confirmation are to be employed for the purposes of processing and storing the personalisation data.
cf.: § 14 (1) SigG, (4), § 17 (1), (3) SigV, explanatory note on § 17 (1) SigV
Safeguards pertaining to this requirement: S-P 2.2, S-P 2.3, S-P 3.1, S-P 3.7

REQ-P 5 The personalisation system must accept suitable and confirmed PSEs only.
cf.: § 14 SigG
Safeguards pertaining to this requirement: S-P 2.2, S-P 2.3, S-P 3.1, S-P 3.2, S-P 3.4

REQ-P 6 Deployed technical components are to be protected against unauthorised access, both to the physical hardware and the incorporated software. Changes relating to security must be apparent to the personnel.
cf.: § 11 SigV, § 16 (1) SigV
Safeguards pertaining to this requirement: S-P 1.1 to S-P 1.4, S-P 1.7, S-P 2.1, S-P 2.2, S-P 3.5 to S-P 3.8

REQ-P 7 The certification authority is to document the security safeguards and the issued certificates in such a manner as to ensure that the data and their integrity can be verified at any time.
cf.: § 10 SigG
Safeguards pertaining to this requirement: S-P 1.3, S-P 3.3, S-P 3.8

REQ-P 8 The technical components which are required for recording identification and authentication data, such as biometric characteristics, must be designed in such a manner as to ensure that the identification and authentication data are not disclosed and are stored on the data storage medium with the private signature key only. Security-related modifications to the technical components must be apparent to the user.
cf.: § 16 (2) SigV
Safeguards pertaining to this requirement: S-P 1.3 to S-P 1.8, S-P 2.1, S-P 2.2, S-P 2.3, S-P 3.1, S-P 3.2, S-P 3.4

REQ-P 9 The confirmation of fulfilment of the requirements for technical components is to be reviewed in the event of deficiencies being established or suspected in technical components.
cf.: § 14 (4) SigG, § 17 (3) SigV
Safeguard pertaining to this requirement: S-P 2.3

REC-P 1 Detailed records are to be kept specifying the whereabouts of all PSEs. The appurtenant information includes the receipt of initialised and, where appropriate, prepersonalised PSEs, the issuance of personalised PSEs and defective PSEs (rejected items).
cf.: § 10 SigG
Safeguards pertaining to this recommendation: S-P 1.3, S-P 3.3, S-P 3.8

REC-P 2 On completing personalisation, the personalisation facility must be deactivated.
cf.: § 5 (4) SigG
Safeguard pertaining to this recommendation: S-P 3.5

REC-P 3 The memory areas in which personalisation data are processed are to be erased after completing personalisation in such a manner as to exclude the possibility of inference of their former contents.
cf.: § 5 (4) SigG
Safeguards pertaining to this recommendation: S-P 1.5, S-P 1.7, S-P 2.2, S-P 2.3

REC-P 4 PSEs may be provided with additional identification characteristics (photograph of the user, biometric characteristics, etc.).
cf.: § 16 (2) SigV
Safeguard pertaining to this recommendation: S-P 3.1

REC-P 5 The competent authority should additionally arrange for spot checks to be carried out on the confirmed technical components.
cf.: § 17 (3) SigV
Safeguard pertaining to this recommendation: S-P 2.3

### 6.3.3 Proposed solutions

**Personalisation of the PSE**

In principle, personalisation of the PSE can be carried out centrally at the CA or on a decentralised basis at distributed RAs with a personalisation system (cf. Section 2.3). Three viable models apply in conjunction with key generation:

A) central key generation and central personalisation,

B) central key generation and decentralised personalisation,

C) decentralised key generation and decentralised personalisation.

The emphasis falls on different requirements, according to the selected model.

### 6.3.4 Safeguard catalogue

#### 6.3.4.1 Threats

The following enumeration does not draw a strict distinction between threats as defined in ITSEC and any vulnerabilities which may be exploitable as a result of implementation. Equally, the enumeration is certainly not to be regarded as complete or final.

1. Personalisation of unsuitable PSEs.
   Safeguards: S-P 1.3, S-P 1.4, S-P 2.2, S-P 2.3, S-P 3.1, S-P 3.2, S-P 3.4, S-P 3.5
2. Compromise of the transport key.
   Safeguards: S-P 1.5, S-P 1.7, S-P 1.8, S-P 2.2, S-P 2.3
3. Compromise of personalisation data.
   Safeguards: S-P 1.1, S-P 1.2, S-P 1.5, S-P 1.7, S-P 1.8, S-P 2.1, S-P 2.2, S-P 2.3, S-P 3.1, S-P 3.4, S-P 3.8
4. Duplication of personalised PSEs.
   Safeguards: S-P 1.1, S-P 1.2, S-P 1.5, S-P 1.7, S-P 2.1, S-P 2.2, S-P 2.3, S-P 3.1, S-P 3.6, S-P 3.8
5. Non-secure handover of personalisation data.
   Safeguards: S-P 1.5, S-P 1.6, S-P 1.8, S-P 2.1, S-P 2.2, S-P 2.3, S-P 3.4
6. Uncontrolled abortion of the personalisation process.
   Safeguards: S-P 1.3, S-P 1.4, S-P 1.6, S-P 2.2, S-P 2.3, S-P 3.2, S-P 3.3
7. Any form of uncontrolled personalisation.
   Safeguards: S-P 1.1, S-P 1.3, S-P 1.4, S-P 1.6, S-P 2.2, S-P 2.3, S-P 3.2, S-P 3.3
8. Maloperation of the personalisation system.
   Safeguards: S-P 1.1, S-P 1.4, S-P 2.2, S-P 2.3, S-P 3.5
9. Theft of personalised PSEs.
   Safeguards: S-P 3.3, S-P 3.6, S-P 3.8
10. Theft of unusable PSEs (rejected items).
    Safeguards: S-P 3.3, S-P 3.5, S-P 3.6, S-P 3.8
11. Technical faults during personalisation.
    Safeguards: S-P 1.4, S-P 1.6, S-P 2.2, S-P 2.3, S-P 3.1, S-P 3.2
12. Interception of PIN letters.
    Safeguards: S-P 3.7
13. Manipulation of the personalisation system.
    Safeguards: S-P 1.1 to S-P 1.4, S-P 1.6, S-P 1.7, S-P 2.1, S-P 2.2, S-P 2.3
14. Compromising emanation of data relevant to security.
    Safeguards: S-P 1.8, S-P 2.1, S-P 2.2, S-P 2.3, S-P 3.4

#### 6.3.4.2 Safeguards

##### 6.3.4.2.1 Safeguards relating to the personalisation system

**S-P 1.1 Access control**

The personnel of the key- and certificate-generating environment at the CA and the decentralised RA discharges the functions of system administrator, system revisor and operating personnel. The system administrator is responsible for administration of the key and certificate generating system. Only the system administrator is able and authorised to assign the rights of the operating personnel. The revisor is responsible for evaluation of the record data.

Only the revisor is able to obtain access to the record data. The operating personnel carries out the tasks which apply during the key and certificate generation process. No individual may be assigned more than one of the stated functions at the same time. The key and certificate generating systems must verify the appropriate rights of the personnel and reject unauthorised attempts to gain access.

**S-P 1.2 Identification and authentication**

The personnel must identify and authenticate itself to the personalisation system by means of possession and knowledge (e.g. chipcard and PIN). Operation of the systems is possible only after successful identification and authentication.

**S-P 1.3 Recording of events**

All personalisation actions are recorded. The record data are clearly assigned to the individually specified PSEs. The record data are accessible to the system revisor only, for the purpose of evaluation (cf. S-P 1.1). The deployed technical components are able to record each of the following events together with the specified data:
Utilisation of the identification and authentication mechanism:

- Required data: Date, time, submitted user ID, indication of the technical component on which identification and authentication were carried out, and success or failure of the attempt.
- Attempted access to an object subject to the administration of rights:
  Required data: Date, time, user ID, name of the object, type of attempted access, success or failure of the attempt.
- Actions by authorised personnel which affect the security of the technical components or of the PSE:
  Required data: Date, time, user ID, type of action (e.g. insertion or deletion of data, insertion or removal of data storage media, etc.) and name of the object to which the action related.

**S-P 1.4 Signalling of malfunctions**

Malfunctions are indicated to the personnel by clear acoustic and/or optical signals. The mechanisms which are evaluated in the systems for this purpose include:

- failed identification and authentication processes,
- checking of all data storage media for viruses when operating systems are booted,
- integrity tests on employed software,
- integrity tests on stored data,
- failure checking and self-tests of employed hardware,
- evaluation of tamper protection mechanisms, and
- procedural and status assessment of operating activities.

**S-P 1.5 Erasure of used memory areas**

Memory areas employed during the generation of keys and certificates are erased automatically after the completion of processing in the system in such a manner (e.g. by overwriting the memory contents with a random bit pattern) as to eliminate the possibility of inference of their former contents.

**S-P 1.6 Integrity of data transport**

All data are signed for the purposes of transportation within the CA (and within decentralised RAs) and their integrity is subsequently checked by the receiving system. When it is not possible to establish the integrity of data, the action concerned is recorded, the data record is rejected, the sender is notified and requested to send the data again. The integrity of personalisation data records is checked directly after personalisation in the PSE.

**S-P 1.7 Tamper protection**

The technical components deployed at the CA are secured against manipulations which require the component housing to be opened by means of tamper protection safeguards. Opening the housing interfaces will result, for example, in the automatic erasure of data which are critical to security (e.g. key data) and the output of optical and/or acoustic alarms.

**S-P 1.8 Prevention of compromising emanation**

The technical components employed at the CA are protected against emanation and confirmed accordingly. When systems and components are networked, it is to be ensured that the appurtenant cabling is protected against emanation (shielded cables) and/or the data to be transmitted is to be encoded for the transmission process.

**6.3.4.2.2 Safeguards relating to organisation of the personalisation environment**

**S-P 2.1 Secure networking of the personalisation system**

Within the certification authority, the systems are networked with other areas of the CA in due compliance with strict security requirements. The data lines are to be secured against tapping (e.g. by means of line encoding, protected cabling, etc.). In order to reliably prevent read-out of the personalisation data from CA areas, the lines must not be connected to external networks. Connection to distributed offices (e.g. decentralised RAs) via encoded dedicated lines is possible.

**S-P 2.2 Deployment of suitable system components**

Only hardware and software components which have been evaluated and found to be suitable by authorised evaluating bodies are employed in the personalisation environment.

**S-P 2.3 Review of deployed system components**

The deployed system components are subjected to renewed evaluation on a spot-check basis and when deficiencies are suspected. Aspects which arise in the course of technological change are also to be taken into consideration here. The deployed technical components must satisfy all security-related requirements of current engineering standards. Should the requirements not be fulfilled, the issued confirmation will be declared invalid.

**6.3.4.2.4 Safeguards relating to the personalisation process**

**S-P 3.1 Use of suitable PSEs**

The personalisation department ensures that only suitable and appropriately evaluated and confirmed PSEs are personalised. Suitable PSEs can, for example, be provided with an individual and unambiguous indicator during the initialisation phase at the manufacturer's premises, and this indicator can then be verified at the beginning of the personalisation process. PSEs without a verifiable indicator are rejected by the personalisation system.

**S-P 3.2 System authentication**

Mutual authentication of personalisation system and PSE is carried out. This results in verification not only of the PSE´s suitability, but also of the personalisation system's legitimacy (cf. Section 6.3.5).

**S-P 3.3 PSE records**

A detailed record is kept specifying the whereabouts of each individual PSE. The information to be kept in these records includes the receipt of initialised and, where applicable, prepersonalised PSEs, the issuance of personalised PSEs and defective PSEs (rejected items). Personalised PSEs are provided with a personalisation indicator, consisting of the certificate of the personalisation system, the time stamp and the serial number of the personalisation process (e.g. counter number in the personalisation system). The identifier of the PSE is recorded in accordance with S-P 1.3.

**S-P 3.4 Secure transport of personalisation data**

All personalisation data are transmitted to the personalisation system in transport-encoded mode and are not decoded until they are located in the PSE.

**S-P 3.5 Deactivation of the personalisation facility**

On completion of the personalisation process, the personalisation facility of the PSE is deactivated. This renders the application of further or new personalisation data impossible (cf. Section 6.3.5).

**S-P 3.6 Activation of password protection/PIN**

After completing the personalisation process, the password protection/PIN of the PSE is activated and the start password/PIN is transmitted to the PIN-letter printer (cf. Section 6.3.5).

**S-P 3.7 Application of suitable mechanisms for PIN handover**

Only suitable mechanisms are employed for PIN handover, e.g. handover via PIN letter. Only specially protected printers and special PIN-letter forms are employed for print-out of the PIN letters.

**S-P 3.8 Destruction of defective PSEs (rejected items)**

When a defect is identified on a PSE in the course of the personalisation process, the PSE concerned is checked and physically destroyed. This action is documented.

#### 6.3.4.3 Assignment of the safeguards to solutions

| Safeguard | Counteracts threat | Solution model | | |
|---|---|---|---|---|
| | | A) | B) | C) |
| S-P 1.1 | 3,4,7,8,13 | required | required | required |
| S-P 1.2 | 3,4,13 | required | required | required |
| S-P 1.3 | 1,6,7,13 | required | required | required |
| S-P 1.4 | 1,6,7,8,11,13 | required | required | required |
| S-P 1.5 | 2,3,4,5 | required | required | required |
| S-P 1.6 | 5,6,7,11,13 | required | required | required |
| S-P 1.7 | 2,3,4,13 | required | required | required |
| S-P 1.8 | 2,3,5,14 | required | required | required |
| S-P 2.1 | 3,4,5,13,14 | required | required | required |
| S-P 2.2 | 1,2,3,4,5,6,7,8,11,13, 14 | required | required | required |
| S-P 2.3 | 1,2,3,4,5,6,7,8,11,13, 14 | required | required | required |
| S-P 3.1 | 1,3,4,11 | required | required | required |
| S-P 3.2 | 1,6,7,11 | recommended | recommended | recommended |
| S-P 3.3 | 6,7,9,10 | required | required | required |
| S-P 3.4 | 1,3,5,14 | recommended | recommended | not required |
| S-P 3.5 | 1,7,8,10 | recommended | recommended | recommended |
| S-P 3.6 | 4,9,10 | required | required | required |
| S-P 3.7 | 12 | required | required | required |
| S-P 3.8 | 3,4,9,10 | required | required | required |

#### 6.3.4.4 Assignment of the safeguards to the security requirements

| Security requirement/ Recommendation | Safeguards |
|---|---|
| REQ-P 1 | S-P 1.1 to S-P 3.8 |
| REQ-P 2 | S-P 1.5, S-P 2.2, S-P 2.3, S-P 3.1, S-P 3.8 |
| REQ-P 3 | S-P 1.5, S-P 1.7, S-P 1.8, S-P 2.1, S-P 2.2, S-P 2.3, S-P 3.1, S-P 3.2, S-P 3.4 |
| REQ-P 4 | S-P 2.2, S-P 2.3, S-P 3.1, S-P 3.7 |
| REQ-P 5 | S-P 2.2, S-P 2.3, S-P 3.1, S-P 3.2, S-P 3.4 |
| REQ-P 6 | S-P 1.1 to S-P 1.4, S-P 1.7, S-P 2.1, S-P 2.2, S-P 3.5 to S-P 3.8 |
| REQ-P 7 | S-P 1.3, S-P 3.3, S-P 3.8 |
| REQ-P 8 | S-P 1.3 to S-P 1.8, S-P 2.1, S-P 2.2, S-P 2.3, S-P 3.1, S-P 3.2, S-P 3.4 |
| REQ-P 9 | S-P 2.3 |
| REC-P 1 | S-P 1.3, S-P 3.3, S-P 3.8 |
| REC-P 2 | S-P 3.5 |
| REC-P 3 | S-P 1.5, S-P 1.7, S-P 2.2, S-P 2.3 |
| REC-P 4 | S-P 3.1 |
| REC-P 5 | S-P 2.3 |

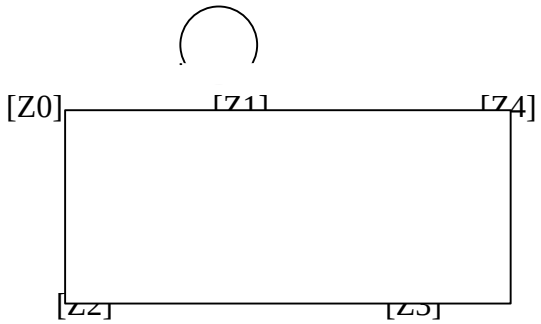
### 6.3.5 Example procedure for personalisation of a PSE in accordance with the model

**Decentralised key generation in the PSE**

This proposed solution provides an example of a possible form of organisation for the entire personalisation process, including key generation and key changing. The CA is able to verify the integrity of the PSE. In this example, generation of the user keys is carried out in the PSE itself and initiated by the user after the PSE has been handed over by the issuing office. The CA is able to ascertain whether the PSE assigned to the user has actually generated the key pair itself, by reference to the submitted public key but without requiring submission of the PSE. This proposal employs only digital signature methods as security safeguards.

**Prerequisites:**

1. Generation of a CA public key pair ($s_{Auth,CA}$, $v_{Auth,CA}$)[15] at the CA
2. Authentic transportation of the CA public key $v_{Auth,CA}$ to the production plant with guaranteed integrity.
3. Life-cycle incorporated in the operating system of the PSE, with the following state diagram and the valid command sets for the respective states.




STATE DIAGRAM

[15] Note: The abbreviation s stands for sign, v for verify

**Procedure:**

## State [Z0]

**(Initialisation state)**

**Explanation:**

During this life-cycle state an authentication mechanism is established which permits mutual authentication between CA and PSE. This enables the CA to verify that only PSEs which it has approved enter into the personalisation process. The PSE can only be personalised by the authorised CA.

**Exclusively valid command set during [Z0]:**

1. Generate Authentication-Keys ($s_{Auth,PSE}$, $v_{Auth,PSE}$)
2. Load $v_{Auth,CA}$

**Description of procedure:**

1. Generation of a public key pair ($s_{Auth,PSE}$, $v_{Auth,PSE}$) in the PSE and the production plant
2. Loading of $v_{Auth,CA}$ into the PSE at the production plant
3. Authentic transportation of the PSE public key $v_{Auth,PSE}$ with guaranteed integrity from the production plant to the CA
4. Transportation of the PSE to the CA

## State [Z1]

**(Prepersonalisation state)**

**Explanation:**

During this life-cycle state, assignment between PSE and user is carried out and the authentication mechanism between user and PSE is established.

**Exclusively valid command set during [Z1]:**

1. Execute Authenticate
2. Load personalisation after 1. only
3. Create PIN system after 2. only
4. Reset to state Z1: Clear personalisation data (incl. PIN)

**Description of procedure:**

1. Identification of the PSE at the CA by means of $v_{Auth,PSE}$
2. Mutual authentication of PSE and CA (abortion of the personalisation process in the event of an error)
3. Loading of the personalisation data into the PSE, apart from $s_{User}$, $v_{User}$ and certificate
4. Registration of the assignment (PSE / User) by means of ($v_{Auth,PSE}$ / $Name_{User}$) at the CA

5. Activation of the PIN system (or equivalent method)
6. Transportation of the PSE to the user with guaranteed integrity (e.g. via PSE output)
7. Confidential transportation of the PIN to the user (e.g. PIN letter)

## State [Z2]

**(Key generating state)**

**Explanation:**

During this life-cycle state the signature keys are generated by the authorised user. The user's public verification key is signed by the PSE. On the basis of this signed data record, the CA is able to verify that the user's signature key pair has been generated in the PSE assigned to the user.

**Exclusively valid command set during [Z2]:**

1. Verify PIN
2. Change PIN only after 1. (optional)
3. KeyGen only after 1. or 2., if previous state was [Z1]
4. Sign $v_{User}$

***Important:*** In this state, signature generation is permissible with $s_{Auth,PSE}$ only

5. Reset to state Z1: Clear $s_{User}$, $v_{User}$, personalisation data (incl. PIN)

**Description of procedure:**

1. Authentication of the user to the PSE via PIN
2. Generation of the public key pair ($s_{User}$, $v_{User}$) in the PSE
3. Generation of a signature via $v_{User}$ enable $s_{Auth,PSE}$

## State [Z3]

**(Personalisation state)**

**Explanation:**

During this life-cycle state, the control state is enabled via loading of the certificate into the PSE.

**Exclusively valid command set during [Z3]:**

1. Verify PIN
2. Change PIN after 1. (optional)
3. Load certificate after 1.
4. Check certificate after 1.

5. Verify certificate after 1.
6. Reset to state Z1: Clear certificate, $s_{User}$, $v_{User}$, Personalisation data (incl. PIN)

**Description of procedure:**

1. Transportation of the signed $v_{User}$ to the CA
2. Verification of the signature generated via $v_{User}$ by means of $v_{Auth,PSE}$ at the CA (this verification ensures that the $v_{User}$ has been generated in the PSE assigned to the user)
3. Generation of the certificate $Cert_{User}$ via $v_{User}$
4. Transportation of certificate $Cert_{User}$ to the user
5. Authentication of the user to the PSE via PIN
6. Loading of certificate $Cert_{User}$ into the PSE
7. Consistency check on the certificate by reference to the data already contained in the PSE
8. Verification of the certificate by means of the verification key (public certification key) of the CA, where appropriate including the complete certificate path

## State [Z4]

**(Control state)**

**Explanation:**

During this life-cycle state, the generation and verification of signatures for the authorised user is possible.

**Exclusively valid command set during [Z4]:**

1. Verify PIN
2. Change PIN after 1. (optional)
3. Sign by means of $s_{User}$
4. Verify signature
5. Verify certificate
6. Reset to state Z2: Clear certificate, $s_{User}$, $v_{User}$
7. Reset to state Z1: Clear certificate, $s_{User}$, $v_{User}$, Personalisation data (incl. PIN)

**Description of procedure:**

1. Authentication of the user to the PSE
2. Signature generation and/or signature verification (incl. certificates)

## 6.4 Directory Service

The directory service provides the facility required by the Digital Signature Act to enable the verification and, subject to the consent of the signature key holder, retrieval of the signature key certificates and attribute certificates at the certification authorities by any person at any time.

### 6.4.1 Requirements stipulated in the Act and the Ordinance

| Reference | Quotation | Interpretation |
|---|---|---|
| **§ 5 (1) sentence 2 SigG** | It *(the certification authority)* shall confirm the assignment of a public signature key to an identified person by a signature key certificate which, together with any attribute certificates, shall be kept available for verification and, with the consent of the holder of the signature key, for retrieval at all times and for everyone over publicly available telecommunication links. | In order to enable verification of a document, the certificate should either be delivered together with the document or identification parameters should be incorporated automatically in the course of a signature process.<br>'At all times': The maximum response time for the directory service should be one minute.<br>'Over publicly available tele-communication links': e.g. via access to the Internet. The protocols and methods to be employed must be published and available to everyone.<br>The minimum scope of data to be contained in a certificate is stipulated in § 7.<br>Derived requirements: REQ-DIR 1.1, REQ-DIR 1.2, REQ-DIR 1.3. |
| **Explanatory note on § 5 (1) Sentence 2 SigG** | Sentence 2 provides the necessary basis to ensure that the authenticity and validity of an existing certificate can be verified at any time (i.e. within the period stipulated in the Digital Signature Ordinance). Public disclosure of the certificate shall, however, be possible only with the express consent of the signature key holder. Irrespective of whether public disclosure takes place, the certificate may be attached to signed data, in order to enable the recipient to verify the signature. The scope of any services offered beyond this (e.g. with all the certificates and revocation lists of the licensed certification authorities and of the competent authority)shall be left to market forces. | Derived requirements: REQ-DIR 1.1, REQ-DIR 1.2, REQ-DIR 1.3. |

| | | |
|---|---|---|
| **§ 5 (5) sentence 2 SigG** | For the provision of signature keys and the issue of certificates it (*the certification authority)* shall use technical components as set out in § 14. This shall also apply to technical components enabling verification of certificates according to § 5 (1) sentence 2 above. | Components which enable the verification or retrieval of certificates must be tested, as they are specified in § 14 (4) SigG.<br>Derived requirement: REQ-DIR 2.7. |
| **§ 7 SigG** | The signature key certificate shall contain the following information:<br>1. name of the holder of the signature key to which additional information must be appended in the event of possible confusion, or a distinctive pseudonym assigned to the holder of the signature key, clearly marked as such,<br>2. public signature key assigned,<br>3. names of the algorithms with which the public key of the holder of the signature key and the public key of the certification authority can be used,<br>4. serial number of the certificate,<br>5. beginning and end of the validity period of the certificate,<br>6. name of the certification authority, and<br>7. an indication as to whether use of the signature key is restricted in type or scope to specific applications.<br><br>(2) Information relating to the authority to represent a third party and to the professional admission to practice or other type of admission may be included both in the signature key certificate and in an attribute certificate. | This must be taken into account with regard to the dimensioning of the directory service data structure.<br>Derived requirements: REQ-DIR 2.1, REC-DIR 2.1. |
| **§ 8 (1) sentence 2 and 3 SigG** | The revocation *(of a certificate)* shall indicate the time at which it enters into effect. Retrospective revocation shall not be permitted. | § 16 (5) SigV stipulates that the valid official time must be employed to indicate the time of revocation.<br>Derived requirements: REQ-DIR 3.1, REQ-DIR 3.2. |

| | | |
|---|---|---|
| **Explanatory note on § 8 (1) sentence 2 SigG** | When a signature key certificate is revoked, all appurtenant attribute certificates are revoked accordingly. Attribute certificates can be revoked separately. [...]<br><br>In cases of doubt, a time stamp provides definite confirmation as to whether a signature was generated before or after the revocation. The time of revocation includes the date and the time of day. | Derived requirements: REQ-DIR 3.1, REQ-DIR 3.2, REQ-DIR 3.3. |
| **§ 14 (3) SigG** | Technical components enabling signature key certificates to be kept available for verification or retrieval in accordance with §5(1) sentence 2 require safeguards to protect the lists of certificates against unauthorised alteration and retrieval. | Certificate lists and revocation lists must be protected against unauthorised alteration.<br><br>The process which comes into contact with the outside world must be evaluated in accordance with standard 'E 2'. This also applies to all components of the operating system which are used by this process.<br><br>A knowledge of the inquiry protocol is necessary in order to verify which data constitute inquiries and which data constitute attacks. The computer on which the directory service is operated must not have any further external network connections. Otherwise, these must also be confirmed in accordance with 'E 2 high'. Administration is to be possible only after adequate identification and authentication. ITSEC F-C2 is appropriate here.<br><br>Derived requirements: REQ-DIR 2.3, REQ-DIR 2.4, REC-DIR 2.2, REC-DIR 2.3. |
| **Explanatory note on § 14 (3) SigG** | The certificate directories must be protected above all from the unauthorised revocation of certificates and the removal of revocations. If the holder of the signature key has not consented to his certificate being available for retrieval via public networks (cf. § 5 (1)), it must also be protected against unauthorised retrieval (authorised retrieval for internal purposes of the certification authority remains unaffected). | Derived requirements: REQ-DIR 2.3, REQ-DIR 2.4, REC-DIR 2.2,<br><br>REC-DIR-2.3. |

| | | |
|---|---|---|
| **§ 14 (4) SigG** | Technical components according to § 14 (1) to (3) above shall be adequately tested against current engineering standards and their compliance with requirements confirmed by a body recognised by the competent authority. | Derived requirements: REQ-DIR 2.7, REQ-DIR 2.8. |
| **§ 8 (1) SigV** | (1) The certification authority shall keep certificates issued by it within a register, pursuant to the provisions of § 5 (1) Sentence 2 of the Digital Signature Act; a certificate shall be kept in such directory for at least as long as the algorithm listed in the certificate and its pertinent parameters are considered suitable pursuant to § 17 (2). | A retrieval facility for the certificates may result in very large revocation lists and certificate lists, as no certificates or revocation entries can be deleted. This may pose problems for the requirements 'at any time' and 'protection against unauthorised alteration'. A facility should thus be provided for retrieving individual revocation entries.<br>Derived requirement: REQ-DIR 1.4. |
| **Explanatory note on § 8 (1) SigV** | Digital signatures must be available for verification within the specified period.<br>In order to organise the verification of digital signature in the most practical manner possible, particularly when large-scale applications are involved (e.g. at banks or department stores), the certification authorities can keep all relevant certificates (including those of the competent authority and any foreign bodies)available for verification on a centralised basis, by means of an integrated network of its registers of certificates. In order to avoid repeated on-line inquiries, revocation lists and new revocations can be transmitted automatically to major users, who will then require only to check this information against the data in their own computers. The certification authorities are free to draft corresponding commercial offers.<br>A certification may offer the verification of digital signatures generated with different algorithms or parameters as an additional service. | Derived requirement: REQ-DIR 1.4. |

| | | |
|---|---|---|
| **§ 9 (3) SigV** | Revocation of certificates must be clearly indicated, with inclusion of the relevant date and time, in the directory pursuant to § 8 of the Digital Signature Act, and may not be rescinded. | The revocation list is to be protected against unauthorised alterations. After adding new entries, the revocation lists are signed with a private key of the user 'Directory service'. A secure procedure is to oblige the CA to send the revocation lists to all or at least several other CAs or the competent authority after each alteration (= expansion). This would also accelerate the availability of certificates for verification (see also explanatory note on § 8 (1) SigV).<br><br>Copies of the revocation lists and the protocol information should be stored on a medium which permits writing once only.<br><br>Derived requirements: REQ-DIR 2.2, REQ-DIR 2.3, REC-DIR 2.3. |
| **Explanatory note on § 9 (3) SigV** | In order to avoid any doubt as to when a certificate was revoked, a revocation must be final. If necessary, a new certificate is to be issued. The possible confirmation of revocation to the signature key holder falls within the scope of contractual agreements. Retroactive revocation is precluded by § 8 (1) Sentence 3 of the Digital Signature Act. | Derived requirements: REQ-DIR 2.2, REQ-DIR 2.3. |
| **§ 11 SigV** | The certification authority shall take precautions to protect the following from unauthorised access: private signature keys, and the technical components used to prepare the certificates and time stamps and to ensure that certificates can be checked at any time. | The data of the directory service are to be protected against unauthorised access. In particular, this concerns the certificate lists and revocation lists.<br><br>Derived requirements: REQ-DIR 2.3, REC-DIR 2.2, REC-DIR 2.3. |
| **Explanatory note on § 11 Sentence 1 and 2 SigV** | Protection of the technical components against unauthorised access is intended to prevent possible technical manipulations. Unauthorised access (in either physical or logical form, e.g. via communications networks) must at least be detected prior to renewed use, so as to enable replacement or checking of the technical components. | The data of the directory service are to be protected against undetected access.<br><br>Derived requirement: REQ-DIR 2.3. |

| | | |
|---|---|---|
| **§ 16 (4) SigV** | The technical components used to store certificates in verifiable form, pursuant to §4 (5) Sentence3 or §5 (1) Sentence2 of the Digital Signature Act, must function in such a manner that only authorised persons can make entries and changes; that the revocation of a certificate cannot be undetectably rescinded; and that information can be checked for genuineness. The information must include mention of whether the verified certificates were present at the given time, without having been revoked, in the directory of certificates.<br><br>Only certificates kept available for verification purposes must not be publicly available for retrieval. Security-relevant changes in technical components must be apparent for the user. | The certificate lists and revocation lists must be protected against unauthorised alterations.<br><br>Additions to the lists of the directory service may only be carried out with the aid of special programmes which are certified in accordance with 'E2 high'. These programmes must not enable the deletion or alteration of entries. Alternatively, this can be ensured by organisational safeguards ('reliable staff'). The information on the validity of a certificate is contained in the certificate (§ 7 SigG). The directory service must be able to receive not only of the serial number of the certificate to be verified, but also the time to be verified.<br><br>Derived requirements: REQ-DIR 1.5, REQ-DIR 2.3, REQ-DIR 2.5, REQ-DIR 2.6, REC-DIR 2.3. |
| **Explanatory note on § 16 (4) SigV** | As a supplement to § 14 Sentence 3 of the Digital Signature Act, this regulation is intended to protect the mandatory directories of certificates against the insertion of forged certificates and against unauthorised alterations (e.g. removal of revoked certificates) and to protect the certificates which are not kept available for retrieval (e.g. attribute certificates on rights of representation) against unauthorised access. If the rescission of revocations by persons authorised to access the system (cf. § 9 (3) cannot be precluded by technical means, any such rescissions must at least be detected.<br><br>Reliable verification of the authenticity of the information must also be possible, to eliminate the possibility of fake directories being use (so-called 'masquerade').<br><br>In order to prevent complete forgeries and to enable the identification of such at least, in addition to providing a statement concerning revocation the information should also specify whether the certificate exists in the public directory of certificates. When this procedure is implemented, anyone | The reply from the directory service must specify whether a certificate exists and whether it had been revoked at the time of signature generation. In the case of revoked certificates, the date and time of revocation must also be furnished. Consequently, the directory service must be able to receive the serial number and, where applicable, a date and time.<br><br>Derived requirements: REQ-DIR 1.5,REQ-DIR 2.3, REQ-DIR 2.5, REQ-DIR 2.6, REC-DIR 2.3. |

| | | |
|---|---|---|
| | wishing to put a complete forgery into circulation would not only have to generate a false certificate, but would also have to place this certificate in the directory and, with regard to possible checks, insert a forged application for a certificate in the documentation (which would subsequent provide evidence of the forgery). In the course of subsequent verification of a certificate, the user will then at least be able to ascertain whether the certificate exists in the directory (yes/no) and whether it had been revoked at the stated time (of signature generation) (yes/no). With regard to revoked certificates, information on the date and time of revocation is also required.<br><br>Certificates which are kept available for public retrieval on the basis of the signature key holder's consent may be kept in separate directories which are not subject to the provisions of the law, in addition to being kept in the mandatory directory. This also applies to revocation lists (cf. Explanatory note on § 9 (3).The certificates themselves are already protected against forgery and undetected manipulation by their digital signatures. Directories of certificates and revocation lists can similarly be protected against undetected manipulation by means of digital signatures. | |

| | | |
|---|---|---|
| **§ 17 (1) SigV** | Testing of technical components pursuant to § 14 (4) of the Digital Signature Act must conform to the ";Criteria for assessment of the security of information technology systems"; (GMBl. 1992, S. 545). For technical components for generation of signature keys or for storage or use of private signature keys, and for technical components commercially provided to third parties for use, such tests must conform to the "E4" test standard; otherwise, they must conform to the "E2" test standard. The strength of the security mechanisms must be rated as "high"; and the algorithms and pertinent parameters must be assessed as suitable pursuant to (2). | The components in which the certificate list and the revocation list are kept available for verification or retrieval must be evaluated in accordance with standard 'E2 high'.<br>The components which are employed to sign the certificate list and revocation list are components on which private signature keys are used. They must therefore be evaluated in accordance with standard 'E 4 high'.<br>Derived requirements: REQ-DIR 2.7, REQ-DIR 2.8. |
| **Explanatory note on § 17 (1) SigV** | [...]<br>The following requirements thus apply to the individual technical components:<br>[...]<br>-Components for storage and application of the private signature key<br>'E 4 high'<br>[...]<br>-Components to maintain certificates in verifiable form<br>'E 2 high' | Derived requirements: REQ-DIR 2.7, REQ-DIR 2.8. |

### 6.4.2 Security requirements

#### 6.4.2.1 Security requirements and recommendations regarding provision of data from the directory service for users

REQ-DIR 1.1 All certificates must be available for verification and, with the consent of the holder of the signature key, for retrieval at all times and for everyone over publicly available telecommunication links. (Availability).
Cf. § 5 (1) Sentence 2 SigG
Safeguards pertaining to this requirement: S-DIR 3.1, S-DIR 3.2, S-DIR 3.10, S-DIR 4.1, S-DIR 4.2, S-DIR 4.5

REQ-DIR 1.2 All certificates must be available for verification and, with the consent of the holder of the signature key, for retrieval at all times and for everyone over publicly available telecommunication links. (Availability).
Cf. § 5 (1) Sentence 2 SigG
Safeguards pertaining to this requirement: S-DIR 3.1, S-DIR 3.2, S-DIR 3.10, S-DIR 4.1, S-DIR 4.2, S-DIR 4.5

REQ-DIR 1.3 Certificates may be retrievable only with the consent of the signature key holder. (Confidentiality).
Cf. § 5 (1) Sentence 2 SigG
Safeguards pertaining to this requirement: S-DIR 2.1, S-DIR 2.2, S-DIR 3.4, S-DIR 4.3

REQ-DIR 1.4 Certificates must be kept in the directory for 35 years.
Cf. § 8 (1) SigV, § 13 (2) SigV
Safeguards pertaining to this requirement: S-DIR 2.3

REQ-DIR 1.5 The information provided by the directory service must specify whether the verified certificates existed in the certificate directory at the specified time and whether they had been revoked. In the case of revoked certificates, information on the date and time of revocation is also required.
Cf. § 16 (4) Sentence 2 SigV and explanatory note on § 16 (4) Sentence 2 SigV
Safeguard pertaining to this requirement: S-DIR 4.5

#### 6.4.2.2 Security requirements and recommendations relating to operation of the directory service

REQ-DIR 2.1 The directory system must be capable of storing certificates containing the scope of information stipulated in § 7 SigG at least.
cf. § 5 (2) SigG, § 5 (3) SigG, § 7 SigG
Safeguards pertaining to this requirement: S-DIR 2.1, S-DIR 2.2, S-DIR 2.3

REC-DIR 2.1 Certificates should be generated and stored in the format X.509v3.
cf. § 7 SigG
Safeguards pertaining to this recommendation: S-DIR 2.3

REQ-DIR 2.2 The directory system must be capable of storing revocation entries together with the time of revocation and clear identification of the revoked certificate.
cf. § 9 (3) SigV and explanatory note on § 9 (3) SigV
Safeguards pertaining to this requirement: S-DIR 1.1

REQ-DIR 2.3 Certificate lists and revocation lists must be protected against unauthorised and undetected alterations.
cf. § 14 (3) SigG, § 9 (3) SigV, § 16 (4) SigV and explanatory note on § 16 (4) SigV
Safeguards pertaining to this requirement: S-DIR 1.3, S-DIR 2.4, S-DIR 3.4, S-DIR 3.5, S-DIR 3.6, S-DIR 3.7, S-DIR 3.9, S-DIR 4.3

REC-DIR 2.2 New entries in the list of certificates or the revocation list are possible only after identification and authentication of the user. The revocations are provided with a time stamp.
cf. § 14 (4) SigG, § 9 (3) SigV
Safeguards pertaining to this recommendation: S-DIR 1.3, S-DIR 3.5, S-DIR 4.5

REC-DIR 2.3 Each activity on the directory system is recorded on a medium which permits writing once only.
cf. § 14 (3) SigG, § 9 (3) SigV and § 16 (4) SigV
Safeguard pertaining to this recommendation: S-DIR 3.6

REQ-DIR 2.4 Certificates which have not been approved for retrieval must be protected against unauthorised retrieval.
cf. § 14 (3) SigG
Safeguards pertaining to this requirement: S-DIR 2.2, S-DIR 3.3, S-DIR 3.4, S-DIR 3.5, S-DIR 4.3

REQ-DIR 2.5 The information furnished by the directory service must be checked to verify it authenticity.
cf. § 16 (4) SigV
Safeguards pertaining to this requirement: S-DIR 1.2, S-DIR 1.3, S-DIR 4.2, S-DIR 4.3, S-DIR 4.4, S-DIR 4.5

REQ-DIR 2.6 Alterations to the directory system which are of relevance to security must be apparent to the user.
cf. § 16 (3) SigV
Safeguards pertaining to this requirement: S-DIR 3.8

REQ-DIR 2.7 The components which are employed to sign the certificate list and revocation list are components on which private signature keys are used. They must therefore be evaluated and confirmed in accordance with standard 'E 4 high'.
cf. § 5 (5) Sentence 2 SigG, § 14 (4) SigG, § 17 (1) SigV and explanatory note on § 17 (1) SigV
Safeguards pertaining to this requirement: S-DIR 5.1

REQ-DIR 2.8 All components of the directory service, with the exception of the components on which the private signature key of the directory service is used, must be evaluated and confirmed in accordance with ITSEC 'E2 high'.
cf. § 5 (5) Sentence 2 SigG, § 14 (4) SigG, § 17 (1) SigV and explanatory note on § 17 (1) SigV
Safeguards pertaining to this requirement: S-DIR 5.2

#### 6.4.2.3.1 Security requirements and recommendations relating to the generation of revocation entries

REQ-DIR 3.1 The retroactive revocation of certificates must not be possible.
cf. § 8 (1) SigG
Safeguards pertaining to this requirement: S-DIR 1.1, S-DIR 1.3, S-DIR 3.5

REQ-DIR 3.2: The revocation entries must be provided with a time stamp stipulating the time from which the revocation applies. The valid official time in accordance with § 1 (4) of the Time Act must be employed for this purpose.
cf. § 8 (1) SigG and explanatory note on § 8 (1) SigG, § 16 (5) SigV
Safeguards pertaining to this requirement: S-DIR 1.1, S-DIR 1.3, S-DIR 3.5

REQ-DIR 3.3 When a certificate is revoked, all appurtenant attribute certificates must be revoked automatically.
cf. explanatory note on § 8 (1) Sentence 2 SigG
Safeguards pertaining to this requirement: S-DIR 1.4

### 6.4.3 Proposed solutions

In all the solutions, a revocation list is used to store the revoked certificates. This lists contains only an unambiguous identifier for the revoked certificates, with a time stamp. In addition to a serial number and a reference to the CA, the unambiguous identifier must also contain the signature for the certificate. After identification and authentication of the person applying for revocation, revocation entries are effected by an employee of the CA as follows: the unambiguous identifier of the certificate to be revoked is provided with a time stamp and appended to the revocation list. The revocation is valid from this point in time. After one or more additions effected at the same time, the revocation list is provided with a time stamp. The revocation list also contains an entry specifying its maximum duration of validity. It is then signed with a special signature key. For this purpose, a signature key (directory service key) certified by the competent authority is used for each CA, whereby this key may be used by the CA solely for signing revocation lists and replies from the directory service. In order to reduce the scope for manipulation of the revocation list and to increase availability, revocation lists should be sent to as many authorities as possible after adding an additional entry. A network of all certification authorities would thus be expedient for the purpose of exchanging all revocation lists, for example. This would require the serial numbers of the certificates to be unambiguous, which means that they must contain an identifier for the issuing certification authority at least.

As the directory service is required in accordance with § 16 (4) to furnish information as to whether a certificate existed and had been revoked at a given time and it must be possible to verify the authenticity of this information, all information furnished by the directory service must be digitally signed with the directory service key. Use of the CA's signature key is not permissible for this purpose.

Inquiries to the directory service must unambiguously identify the certificate to which the inquiry relates and, where appropriate, must contain a time specification. When no time is specified, the current time will be used automatically. The following will then be returned by way of reply:

- If the certificate is currently retrievable and has not been revoked, it will be sent back to the inquirer together with the statement 'Certificate with identifier ... not revoked on ... at ... '
- If the certificate is currently retrievable and has been revoked, the revocation entry will be sent back to the inquiry together with the statement 'The certificate with the identifier ... exists and has been revoked since ... at ... '. This reply is also output when the time for which information is requested lies before the time of revocation.
- If the certificate is not currently retrievable and has not been revoked, the statement 'The certificate with the identifier ... exists but is not retrievable. It was not revoked on ... at ...' will be sent back together with the signature for the certificate.
- If the certificate is not currently retrievable and has been revoked, the statement 'The certificate with the identifier ... exists but is not retrievable. It has been revoked since ... at ...'. This reply is also output when the time for which information is requested lies before the time of revocation.
- When the certificate does not currently exist in the directory, the statement 'The certificate with the identifier ... does not exist' is sent back, together with the signature for the certificate.

All information statements must be provided with a time stamp and signed with the directory service key. The time stamp contains the time of the inquiry.

The reply time for an inquiry submitted to the directory service should not exceed one minute and the response time which is required to put a revocation entry into effect should not exceed 10 minutes. The maximum down time should be 180 minutes.

Combinations of the following solutions are also possible.

#### 6.4.3.1 Solution 1: Communications computer and certificate computer are interlinked

The data in the directory system are stored separately in three lists. All certificates which are retrievable are stored in a public certificate list, all certificates are stored in a complete certificate list and the unambiguous identifiers of the revoked certificates are stored in a revocation list with the time stamp for the time of revocation.

The directory system consists of two computers. The revocation list, the public certificate list and a list of the existing identifiers together with the signatures for the certificates are stored on a communications computer. These data are located on a writREC-Protected medium and can be retrieved via HTTP. The user sends a serial number for a certificate and, if appropriate a time, and is able to view a revocation note or the contents of a certificate in non-secure mode or to request an information statement. The communications computer is simultaneously connected to one network only. This may be the public network, for example. All actions, with the exception of simple inquiries, are recorded on a medium which permits writing once only (printer, WORM). A security box in accordance with Section 6.7 is employed to sign the information statements.

Additions are inserted in the complete certificate list and the revocation list and the public certificate list is generated on a second computer which is not connected to the communications computer. This computer is subject to precisely the same security

requirements as apply to the computer on which the certificates are generated. Under certain circumstances, it may be identical to this computer. All actions are recorded on a medium which permits writing once only (printer, WORM). After alterations, the revocation list is signed with the private key of the user 'directory service', using a security box. See Section 6.7 with regard to safeguards for the security box.

The data are transferred between the computers by hand, using diskettes.

Access to both computers is possible for authorised personnel after due identification and authentication.

This solution offers the advantage that non-retrievable certificates do not require to be stored on the less protected communications computer.

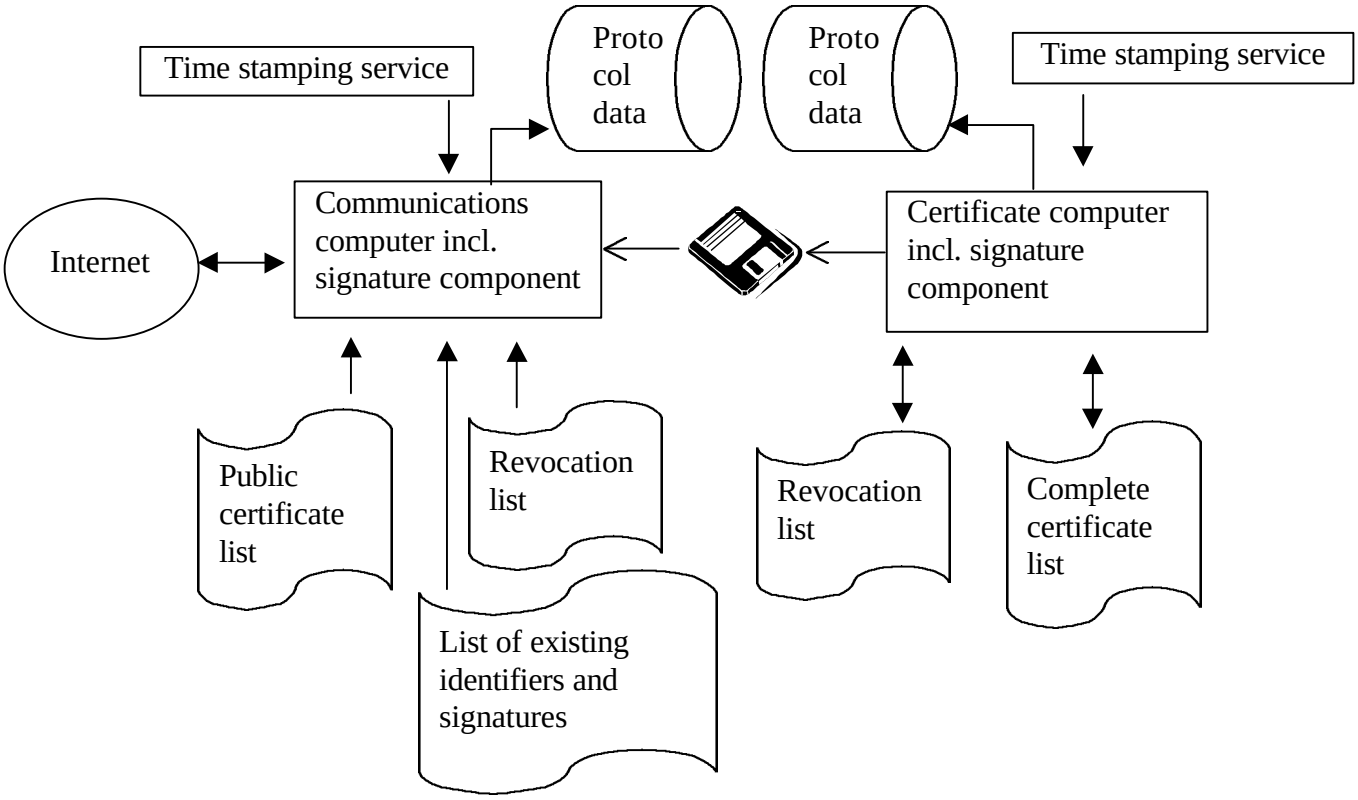



Fig.: Directory service with non-interlinked computers

#### 6.4.3.2 Solution 2: Communications computer and certificate computer are interlinked

The data in the directory system are stored on a certificate computer. The system consists of a list of all issued certificates and the revocation list.

The certificate list contains additional entries providing information on the retrievability of the certificate.

Inquiries and verifications are received by a communications computer with one or more telecommunications links and are transferred via a client to be evaluated to a server process to be evaluated on the certificate computer. The protocol employed between these processes must be designed so that only the identification parameters of the certificate to which the inquiry relates can be transmitted to the certificate computer and only the replies generated by

the certificate computer can be received by the communications computer. This may be achieved by means of a store-and-forward method, for example, whereby the communications computer stores the received data on a hard disk, from which it is collected at regular intervals by the certificate computer. Transmission of the reply data to the inquirer is then effected via the reverse procedure.

The information statements are digitally signed on the certificate computer using the private signature key of the user 'directory service'. This computer should not be used to generate certificates. Alterations to the revocation list are effected on the certificate computer.

Access to both computers is possible for authorised personnel after due identification and authorisation. All actions are recorded on a medium which permits writing once only (printer, WORM.

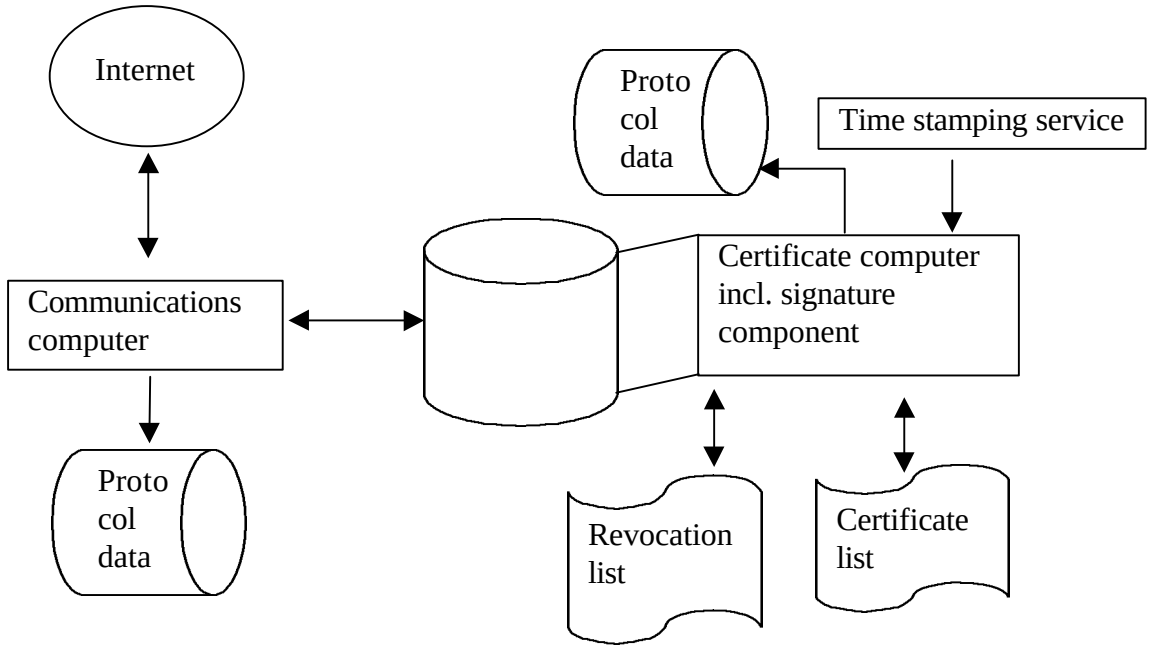



Fig.: Directory service with interlinked computers

#### 6.4.3.3 Solution 3: Several communications computers are linked with one certificate computer by means of a one-way communication configuration

The data in the directory system are stored separately in three lists. All retrievable certificates, the identifiers and the signatures for all certificates are stored in a public certificate list, all certificates are stored in a complete certificate list and the identifiers of the revoked certificates are stored in a revocation list with the time stamp for the time of revocation.

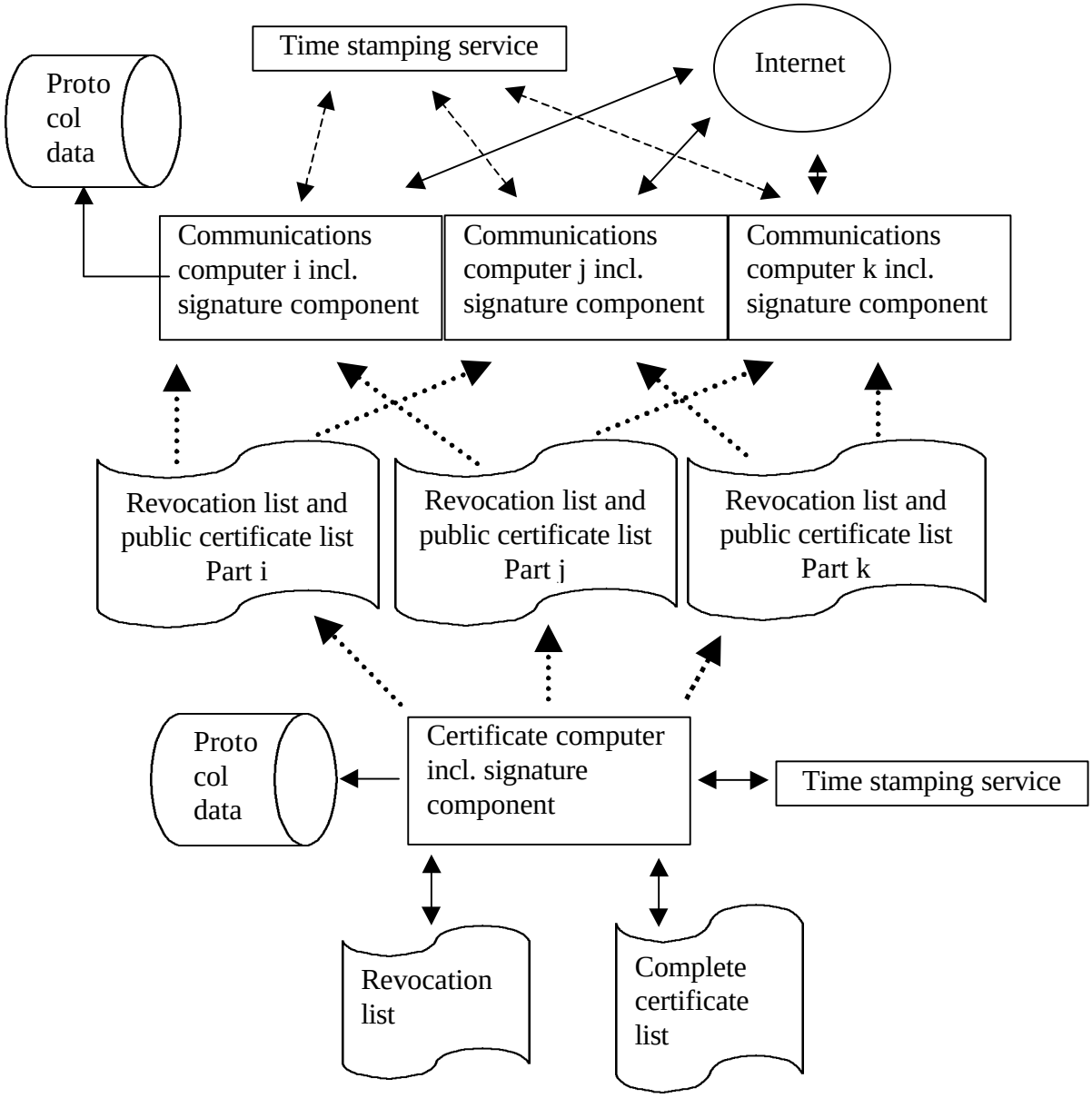



Fig.: Directory service with several communications computers

The directory system consists of one certificate computer and several communications computers. The revocation list and the public certificate list are stored on the communications computers. This public complete certificate list can be divided into several non-overlapping parts and stored on various communications computers. As the volume of data increases, further subdivisions can be carried out. Each part of the list is transferred to several communications computers. This ensures the redundancy of both the access channels and the storage media. A security box in accordance with Section 6.7 is employed for the purpose of signing the information statements with the directory service key.

Additions are inserted in the complete certificate list and the revocation list and the public certificate list is generated on the certificate computer. This computer is subject to precisely the same security requirements as apply to the computer on which the certificates are generated. All actions on the certificate computer and the communications computers, with the exception of simple inquiries, are recorded on a medium which permits writing once only (printer, WORM).

Data transfer between the certificate computer and the communications computers is effected via a secure network link. The processes employed for this purpose must ensure that data transport is possible only from the certificate computer to the communications computers (one-way link). The integrity and confidentiality of the data during data transmission should be ensured by appropriate cryptographic methods. The time stamp which is appended to the revocation list after effecting an addition to the list ensures that no outdated revocation lists are transmitted. A time stamp must additionally be appended to the certificate list prior to transmission, in order to detect input of an outdated certificate list.

### 6.4.4 Safeguard catalogue

#### 6.4.4.1 Threats

The following enumeration does not draw a strict distinction between threats as defined in ITSEC and any vulnerabilities which may be exploitable as a result of implementation. Equally, the enumeration is certainly not to be regarded as complete or final.

1. Illegal revocation of certificates.
   Safeguards: S-DIR 3.2, S-DIR 3.4, S-DIR 3.5, S-DIR 3.8, S-DIR 3.9, S-DIR 4.3, S-DIR 5.1, S-DIR 5.2
2. Rescission of a revocation via the removal or alteration of an entry in the revocation list with record.
   Safeguards: S-DIR 1.1, S-DIR 3.2, S-DIR 3.3, S-DIR 3.4, S-DIR 3.5, S-DIR 3.9, S-DIR 4.3, S-DIR 5.1, S-DIR 5.2
3. Undetected rescission of a revocation via removal or alteration of an entry in the revocation list without record.
   Safeguards: S-DIR 1.1, S-DIR 3.2, S-DIR 3.3, S-DIR 3.4, S-DIR 3.5, S-DIR 3.6, S-DIR 3.7, S-DIR 3.9, S-DIR 4.3, S-DIR 5.1, S-DIR 5.2
4. Reading of certificates which have not been approved for retrieval.
   Safeguards: S-DIR 2.1, S-DIR 2.2, S-DIR 3.2, S-DIR 3.3, S-DIR 3.4, S-DIR 3.5, S-DIR 3.9, S-DIR 4.3, S-DIR 5.1, S-DIR 5.2
5. Deletion of certificates from the certificate list via access to the certificate server.
   Safeguards: S-DIR 3.2, S-DIR 3.3, S-DIR 3.4, S-DIR 3.5, S-DIR 3.9, S-DIR 4.3, S-DIR 5.1, S-DIR 5.2
6. Transmission of a forged revocation list.
   Safeguards: S-DIR 1.3, S-DIR 3.2, S-DIR 3.3, S-DIR 3.4, S-DIR 3.5, S-DIR 3.9, S-DIR 4.5, S-DIR 5.1, S-DIR 5.2
7. Transmission of an outdated revocation list.
   Safeguards: S-DIR 1.2, S-DIR 1.3, S-DIR 4.5, S-DIR 5.1, S-DIR 5.2
8. Transmission of a forged certificate.
   Safeguards: S-DIR 3.2, S-DIR 3.3, S-DIR 3.4, S-DIR 3.5, S-DIR 3.9, S-DIR 4.5, S-DIR 5.1, S-DIR 5.2
9. Prevention of verification for certificates.
   Safeguards: S-DIR 2.3, S-DIR 3.1, S-DIR 4.1, S-DIR 4.2, S-DIR 4.4, S-DIR 5.1, S-DIR 5.2
10. Prevention of retrieval for certificates.
    Safeguards: S-DIR 2.3, S-DIR 3.1, S-DIR 4.1, S-DIR 4.2, S-DIR 4.4, S-DIR 5.1, S-DIR 5.2
11. Loss of the certificate list due to data loss on the certificate server.

Safeguards: S-DIR 3.10, S-DIR 5.1, S-DIR 5.2

12. Loss of the revocation list.

Safeguards: S-DIR 3.10, S-DIR 5.1, S-DIR 5.2

13. Failure of the recording process.

Safeguards: S-DIR 3.6, S-DIR 3.7, S-DIR 3.10, S-DIR 5.1, S-DIR 5.2

14. Misuse via alteration of records.

Safeguards: S-DIR 3.6, S-DIR 3.7, S-DIR 3.9, S-DIR 5.1, S-DIR 5.2

15. Misuse via alteration of the security-related components.

Safeguards: S-DIR 3.2, S-DIR 3.3, S-DIR 3.4, S-DIR 3.5, S-DIR 3.6, S-DIR 3.7, S-DIR 3.8, S-DIR 3.9, S-DIR 4.3, S-DIR 5.1, S-DIR 5.2

16. Unauthorised access to the directory system.

Safeguards: S-DIR 3.2, S-DIR 3.3, S-DIR 3.4, S-DIR 3.5, S-DIR 3.9, S-DIR 4.3, S-DIR 5.1, S-DIR 5.2

17. Operation of a directory service with forged or outdated entries after compromise of the directory service key.

Safeguards: S-DIR 2.4, S-DIR 4.4, S-DIR 5.1, S-DIR 5.2

18. Generation of a forged certificate with a serial number which has been assigned for a genuine certificate.

Safeguards: S-DIR 1.1, S-DIR 4.2, S-DIR 4.5

#### 6.4.4.2 Safeguards

##### 6.4.4.2.1 Safeguards relating to the revocation list

**S-DIR 1.1 Use of a revocation list**

The revocation list stores the unambiguous identifiers of revoked certificates. Each unambiguous identifier must document the time of revocation by means of a time stamp. In addition to a serial number and reference to the CA, the unambiguous identifier must also contain the signature for the certificate. All certificates must be identifiable via their serial number at the issuing CA at least.

**S-DIR 1.2 Integration of a maximum validity period into the revocation list**

This enables outdated revocation lists to be detected. It may be necessary to generate new revocation lists prior to expiry of the validity period.

**S-DIR 1.3 Use of a time stamp after effecting additions to the revocation list**

This safeguard ensures that the current revocation list can be transmitted. The time of enlargement of the revocation list provides an indication of the validity in conjunction with the time of signature generation for a document. In order to confirm the correctness of a signature, users must first provide their data with a time stamp and then verify the revocation list.

**S-DIR 1.4 Revocation of attribute certificates**

When a certificate is revoked, all appurtenant attribute certificates must be revoked automatically.

#### 6.4.4.2.2 Safeguards relating to certificate lists

**S-DIR 2.1 Use of a certificate list containing all the certificates of a CA**

In addition to the data stipulated in § 7 SigG, there must be at least one entry for each stored certificate to indicate whether the certificate concerned may be retrieved. This list is required for administration of the generated certificates. The additional data on the permissibility of retrieval should be stored at a central location.

**S-DIR 2.2 Use of a certificate list containing retrievable certificates only**

This list must be treated confidentially and is easy to extract from the central certificate list. Copies of the public certificate list may also be made available on a decentralised basis.

**S-DIR 2.3 Use of an adequately dimensioned data structure**

The employed data structure must be capable of storing the certificates in the form of the structure defined by the CA and must permit random access. Due consideration should also be given here to the possible size of the lists after 35 years. Random access via the serial number or the identification parameters must also be possible for certificates of variable length (e.g. [X.509]. The following enumeration does not draw a strict distinction between threats as defined in ITSEC and any vulnerabilities which may be exploitable as a result of implementation. Equally, the enumeration is certainly not to be regarded as complete or final.

**S-DIR 2.4 Use of a time stamp prior to transmission of a certificate list to a communications computer**

To prevent input of an outdated list containing retrieval certificates, the certificate list is provided with a time stamp prior to transmission.

#### 6.4.4.2.3 Safeguards relating to operation of the certificate computer

**S-DIR 3.1 Use of a publicly accessible communications computer**

The communications computer must be accessible via public telecommunications facilities and must contain the revocation list and the public certificate list. Two independent systems enable the operation of two certificate lists with different protection requirements.

**S-DIR 3.2 Secure communications between communications computer and certificate computer**

The communications computer which is accessible via public telecommunications facilities relays inquiries and verifications to a certificate computer and, where applicable, receives replies from the latter by means of a secure protocol.

**S-DIR 3.3 Off-line transmission**

Transfer of the updated revocation lists and the public certificate list is effected off-line. This can be carried out by means of diskettes, for example.

**S-DIR 3.4 Use of a special protocol**

A special protocol is employed for the transmission of data between the communications computer and the certificate computer. This protocol and the necessary software implementation must be assessed at all levels to verify that no other functions, such as a remote log-in, can be executed on the certificate server. The testing in accordance with § 14 SigG must cover the software implementation for all involved network layers.

**S-DIR 3.5 Use of secure operating systems**

Operating systems of functionality standard ITSEC F-C2 are employed; the certificate servers furthermore fulfil requirements ITSEC A.38 and ITSEC A.39 of F-B2. This regulates identification and authentication, maintenance of records, reprocessing, separation of posts, etc.

**S-DIR 3.6 Use of a medium which permits writing once only for the purpose of generating records**

Records are stored on WORM systems, for example.

**S-DIR 3.7 Automatic shut-down**

After transmitting a warning to the systems involved, an automatic warning is output in the event of failure of the recording component. In case of failure of the recording component (e.g. overflow), the system is switched to a state in which access to the components to which the administration of rights applies is possible for specially authorised persons only (e.g. revisor).

**S-DIR 3.8 Detectability of security-related alterations**

Alterations to the software components or files of the involved systems are evaluated by means of integrity tests. When a violation of integrity is established, the system is switched to a state in which access to the components to which the administration of rights applies is possible for specially authorised persons only (e.g. revisor).

**M.DIR 3.9 Use of a minimal system**

All systems must incorporate only components critical to and of relevance to security within the meaning of ITSEC.

**S-DIR 3.10 Use of a back-up process for the certificate lists and the revocation list**

Back-ups of the central certificate list and the revocation list are to be generated automatically on a regular basis.

**6.4.4.2.4 Safeguards relating to the transmission of data to the inquirer**

**S-DIR 4.1 Redundancy of the access channels**

The use of several different publicly accessible telecommunications facilities will counteract attacks on availability. When a decentralised directory system is operated, the branch offices can be connected via channels other than those for the central office, for example.

**S-DIR 4.2 Use of a special protocol**

A special protocol is used to receive the identification data for the certificate which is to be verified or retrieved. This protocol and the necessary software implementation must be checked at all levels to verify that no other functions (e.g. remote log-in) can be executed on the communications server. An HTTP proxy with highly restricted functionality may be used here, for example. The employed protocol stack must then be provided with appropriate packet filter characteristics which do not permit any additional form of use. The testing in accordance with § 14 SigG must cover the software implementation of all involved network layers. A secure network link must exist between the communications server and the certificate server. The protocol must be capable of processing inquiries which contain the unambiguous identifier of the certificate to be verified and/or retrieved and, where appropriate, a date and time for verification.

**S-DIR 4.3 Operation of a telephone inquiry service provided by an employee of the CA**

**S-DIR 4.4 Security safeguards for the replies from the directory service**

The use of an automatic time key and a signature with a signature key which is to be used for this purpose only (directory service key) for a reply from the directory service prevents the transmission of outdated or manipulated replies concerning a revocation entry. The use of this signature key, which is certified by the competent authority, also prevents the operation of a false directory service, should the certification key of the CA be compromised.

**S-DIR 4.5 Reply from the directory service in case of non-retrievable certificates**

The serial number of the certificate and a time must be transmitted to the directory service with the inquiry. In the case of a non-retrievable and non-revoked certificate, the directory service must send back the reply 'The certificate with the identifier ... exists but is not retrievable. It has not been revoked on ... at ...', together with the signature for the certificate.

If the certificate is non-retrievable and has been revoked, the revocation entry will be sent back together with the statement 'The certificate with the identifier ... exists but is not retrievable and has been revoked since ... at ...'. This replay is also output when the time for which information is requested lies before the time of revocation.

If the serial number does not exist, the statement 'The certificate with the identifier ... does not exist' will be sent back together with the signature for the certificate.

**S-DIR 4.6 Reply from the directory service in case of retrievable certificates**

The serial number of the certificate and a time must be transmitted to the directory service together with an inquiry. In the case of a retrievable and non-revoked directory service, the directory service must send back the identified certificate together with the statement 'Certificate with the identifier ... not revoked on ... at ...'.

If the certificate is retrievable and has been revoked, the revocation entry will be sent back together with the statement 'The certificate with the identifier ... exists and has been revoked since ... at ...'. This reply is also output when the time for which information is requested lies before the time of revocation.

**6.4.4.2.5 General safeguards**

**S-DIR 5.1 Testing and evaluation of components to expand the data at the directory service**

The components of the directory service which are employed to sign the certificate lists and revocations lists are components for application of the directory service's private signature key. Consequently, they must be evaluated and confirmed in accordance with ITSEC standard 'E4 high'.

**S-DIR 5.2 Testing and evaluation of components for evaluating and retrieving the data at the directory service**

All components of the directory service, with the exception of those components on which the directory service's private signature key is used, must be evaluated and confirmed in accordance with ITSEC standard 'E2 high'.

#### 6.4.4.3 Assignment of safeguards to solutions

| Safeguard | Counteracts threat | Solution models | | |
|---|---|---|---|---|
| | | **Solution 1** | **Solution 2** | **Solution 3** |
| S-DIR 1.1 | 2,3,18 | required | required | required |
| S-DIR 1.2 | 7 | recommended | recommended | recommended |
| S-DIR 1.3 | 6 | required | required | required |
| S-DIR 1.4 | 2 | required | required | required |
| S-DIR 2.1 | 4 | required | required | required |
| S-DIR 2.2 | 4 | required | not required | required |
| S-DIR 2.3 | 9,10 | required | required | required |
| S-DIR 2.4 | 17 | recommended | recommended | required |
| S-DIR 3.1 | 8,9,10 | required | required | required |
| S-DIR 3.2 | 1 to 6,8,15,16 | not required | required | required |
| S-DIR 3.3 | 2,3,4,5,6,8,15,16 | required | not required | not required |
| S-DIR 3.4 | 1 to 6,8,15,16 | not required | required | required |
| S-DIR 3.5 | 1 to 6,8,15,16 | required | required | required |
| S-DIR 3.6 | 3,13,14,15 | required | required | required |
| S-DIR 3.7 | 3,13,14,15 | required | required | required |
| S-DIR 3.8 | 1,15 | required | required | required |
| S-DIR 3.9 | 1 to 6,14, 15,16 | required | required | required |
| S-DIR 3.10 | 11,12,13 | required | required | required |
| S-DIR 4.1 | 9,10 | required | required | required |
| S-DIR 4.2 | 9,10,18 | required | required | required |
| S-DIR 4.3 | 1,2,3,4,5,15,16 | recommended | recommended | recommended |
| S-DIR 4.4 | 9,10,17 | required | required | required |
| S-DIR 4.5 | 7,8,9,10,18 | required | required | required |
| S-DIR 5.1 | all | required | required | required |
| S-DIR 5.2 | all | required | required | required |

#### 6.4.4.4 Assignment of safeguards to the security requirements

| Security requirements/ Recommendation | Safeguards |
|---|---|
| REQ-DIR 1.1 | S-DIR 3.1, S-DIR 3.2, S-DIR 3.10, S-DIR 4.1, S-DIR 4.2, S-DIR 4.5 |
| REQ-DIR 1.2 | S-DIR 3.1, S-DIR 3.2, S-DIR 3.10, S-DIR 4.1, S-DIR 4.2, S-DIR 4.5 |
| REQ-DIR 1.3 | S-DIR 2.1, S-DIR 2.2, S-DIR 3.4, S-DIR 4.3 |
| REQ-DIR 1.4 | S-DIR 2.3 |
| REQ-DIR 1.5 | S-DIR 4.5 |
| REQ-DIR 2.1 | S-DIR 2.1, S-DIR 2.2, S-DIR 2.3 |
| REQ-DIR 2.2 | S-DIR 1.1 |
| REQ-DIR 2.3 | S-DIR 1.3, S-DIR 2.4, S-DIR 3.4, S-DIR 3.5, S-DIR 3.6, S-DIR 3.7, S-DIR 3.9, S-DIR 4.3 |
| REQ-DIR 2.4 | S-DIR 2.2, S-DIR 3.3, S-DIR 3.4, S-DIR 3.5, S-DIR 4.3 |
| REQ-DIR 2.5 | S-DIR 1.2, S-DIR 1.3, S-DIR 4.2, S-DIR 4.3, S-DIR 4.4, S-DIR 4.5 |
| REQ-DIR 2.6 | S-DIR 3.8 |
| REQ-DIR 2.7 | S-DIR 5.1 |
| REQ-DIR 2.8 | S-DIR 5.2 |
| REQ-DIR 3.1 | S-DIR 1.1, S-DIR 1.3, S-DIR 3.5 |
| REQ-DIR 3.2 | S-DIR 1.1, S-DIR 1.3, S-DIR 3.5 |
| REQ-DIR 3.3 | S-DIR 1.4 |
| REC-DIR 2.1 | S-DIR 2.3 |
| REC-DIR 2.2 | S-DIR 1.3, S-DIR 3.5, S-DIR 4.5 |
| REC-DIR 2.3 | S-DIR 3.6 |

## Literature

[X.509] ITU-T Recommendation X.509 (1993), Information technology - Open Systems Interconnection - The directory: authentication framework

## 6.5 Time stamping service

The time stamping service provides the facility required by the Digital Signature Act to enable any digital data of a certification authority to be provided with a date and time and digitally signed.

As loss or compromise of the time stamp signature key will render all time stamps generated with this key irreversibly invalid, independent mechanisms must exist to control the generated time stamps.

### 6.5.1 Requirements stipulated by the Act and the Ordinance

| Reference | Quotation | Interpretation |
|---|---|---|
| **§ 2 (4) SigG** | For the purposes of this Act "time stamp" shall mean a digital declaration bearing a digital signature and issued by a certification authority confirming that specific digital data were presented to it at a particular point in time. | A time source which is difficult to manipulate must be used and an unambiguous time zone must be applied.<br>Derived requirements: REQ-TSS 1, REQ-TSS 2. |
| **Explanatory note on § 2 (4) SigG** | Time stamps prevent the pre- or back-dating of 'digital documents'. In the case of signed data, it is sufficient to affix a time stamp to the digital signature, as the signature contains a 'digital fingerprint' for the signed data. | The current time must be used. The user must be aware of the format and, in particular, of the time zone.<br>Derived requirement: REC-TSS 1. |
| **Explanatory note on § 4 (5) SigG** | [...]<br>The signature keys certified by the competent authority are intended exclusively for signing certificates and, where necessary, for signing time stamps. Other certified signature keys may also be used for time stamps.<br>[...] | Each time stamping service is a user of a CA. The CA issues a different signature key for each time stamping service.<br>Derived requirement: REQ-TSS 8. |
| **§ 5 (4) SigG** | The certification authority shall take safeguards to prevent undetected forgery or manipulation of the data intended for certificates.<br>It shall also take safeguards to ensure confidentiality of private signature keys. Storage of private signature keys by the certification authority shall not be permitted. | When the same key is used to sign certificates and to sign time stamps, there is a risk that any data can be made into signed certificates by attaching a time stamp. Consequently, the signature keys employed for certification must not be used for time stamps. A separate time stamp signature key must be used, and must be clearly identifiable as such. This key is issued by the CA for each time stamping service.<br>Derived requirement: REQ-TSS 8. |
| **§ 5 (5) Sentence 2 SigG** | For the provision of signature keys and the issue of certificates it *(the certification authority)* shall use technical components as set out in § 14. | In accordance with § 9 SigG, this applies accordingly to the time stamp.<br>Derived requirement: REQ-TSS 4. |

| | | |
|---|---|---|
| **§ 9 SigG** | Upon request, the certification authority shall affix a time stamp to digital data.<br><br>§ 5 (5) sentences 1 and 2 shall apply mutatis mutandis. | A certification authority is obliged to offer a time stamping service.<br><br>Derived requirement: REQ-TSS 3. |
| **Explanatory note on § 9 SigG** | A time stamp may be requested by anyone who generates data or is in possession of data from third parties and who is interested in a time stamp for reasons of evidence in connection with such data. A time stamp may be requested by anyone who generates data or is in possession of data from third parties and who is interested in a time stamp for reasons of evidence in connection with such data. In the case of signed data it is sufficient to obtain a time stamp for the digital signature, as this signature represents the entire signed data.<br><br>The provision in sentence 2 is intended to establish the same personnel and technical security for the generation of time stamps as applies to the generation of certificates | As evidentiary data may occur at any time, e.g. when contracts are concluded abroad in different time zone, the time stamping service must be available for use at all times.<br><br>The directory service also requires a time stamping service which is available at all times.<br><br>The time-stamped data must be returned to the user promptly.<br><br>Derived requirement: REC-TSS 2. |
| **§ 14 (1) SigG** | Technical components with safeguards are required for the generation and storage of signature keys and for the generation and verification of digital signatures which reliably reveal forged digital signatures and manipulated signed data and provide protection against unauthorised use of private signature keys. | Upon generation of time stamps, a digital signature is generated with the time stamp signature key.<br><br>Derived requirement: REQ-TSS 4. |
| **§ 14 (4) SigG** | Technical components according to § 14 (1) to (3) above shall be adequately tested against current engineering standards and their compliance with requirements confirmed by a body recognised by the competent authority. | Upon generation of time stamps, a digital signature is generated with the time stamp signature key.<br><br>Derived requirement: REQ-TSS 5. |
| **Explanatory note on § 14 (2) SigG** | § 5 (5) sentence 2 and § 9 require the certification authorities to deploy appropriate technical components for the generation of signature key certificates and time stamps, and subjects the certification authorities to control by the competent authority pursuant to § 13 in this respect. | Derived requirement: REQ-TSS 5. |

| | | |
|---|---|---|
| **§ 11 SigV** | The certification authority shall take precautions to protect the following from unauthorised access: private signature keys, and the technical components used to prepare the certificates and time stamps and to ensure that certificates can be checked at any time. | Derived requirement: REQ-TSS 6. |
| **Explanatory note on § 11 SigV** | Protection of the technical components against unauthorised access is intended to prevent possible technical manipulations. Unauthorised access (in either physical or logical form, e.g. via communications networks) must at least be detected prior to renewed use, so as to enable replacement or checking of the technical components.<br><br>The data storage media containing private signature keys which are used to sign certificates or time stamps must also be protected against misappropriation, in order to prevent possible misuse. | The time stamping service must be protected against manipulations by employees of the certification authority and from outside.<br><br>Derived requirement: REQ-TSS 6. |
| **§ 16 (2) SigV** | The technical components required for generation or verification of digital signatures must function in such a manner that the private signature key cannot be derived from the signature and the signature cannot be forged by any other means. Use of the private signature key must be possible only following identification of the holder and must require proper possession and knowledge; the key must not be disclosed during use. Biometrical characteristics may also be used for identification of the signature key holder. The technical components required for collecting identification data must function in such a manner that they do not reveal identification data and that the identification data is stored only on the data storage medium with the private signature key. Security-relevant changes in technical components must be apparent for the user. | A digital signature is necessary for generation of a time stamp.<br><br>Alterations to the components which are of relevance to security must be apparent to the user.<br><br>Derived requirement: REQ-TSS 7. |

| | | |
|---|---|---|
| **§ 16 (5) SigV** | The technical components with which time stamps pursuant to § 9 of the Digital Signature Act are generated must function in such a manner that the valid official time, without any distortion, is added to the time stamp when it is generated. Security-relevant changes in technical components must be apparent for the user. | Derived requirements: REQ-TSS 2, REC-TSS 1. |
| **Explanatory note on § 16 (5) SigV** | § 1 (1) of the Time Act of 25th July, 1978 (Federal German law gazette I S 1110, 1262; amended by Act of 13th September, 1994, Federal German law gazette I S 2322) requires the date and time to be employed in accordance with the valid official time in official and commercial communications. The term 'valid official time' is defined in § 1 (4) of the Time Act as Central European Time, and includes summer time. | Derived requirements: REQ-TSS 2, REC-TSS 1. |
| **§ 17 (1) SigV** | Testing of technical components pursuant to § 14 (4) of the Digital Signature Act must conform to the ";Criteria for assessment of the security of information technology systems"; (GMBl. 1992, S. 545). For technical components for generation of signature keys or for storage or use of private signature keys, and for technical components commercially provided to third parties for use, such tests must conform to the "E4" test standard; otherwise, they must conform to the "E2" test standard. The strength of the security mechanisms must be rated as "high"; and the algorithms and pertinent parameters must be assessed as suitable pursuant to (2). | The components which are employed to sign time stamps are components for application of the private signature key. Consequently, they must be evaluated in accordance with standard 'E4 high'. All other components of the time stamping service must be evaluated in accordance with standard 'E2 high'.<br>Derived requirement: REQ-TSS 5, REQ-TSS 9. |

| | | |
|---|---|---|
| **Explanatory note on § 17 (1) SigV** | [...]<br>The following requirements thus apply to the individual technical components:<br>[...]<br>-Components for storage and application of the private signature key<br>'E 4 high'<br>[...]<br>-Components to generate time stamps<br>'E 2 high' | Derived requirements: REQ-TSS 5, REQ-TSS 9. |

### 6.5.2 Security requirements and recommendations

REQ-TSS 1 With the aid of a digital signature within the meaning of the Digital Signature Act, a time stamp must certify that digital data existed at a certification authority at a specific point in time.
cf. § 2 (4) SigG
Safeguards pertaining to this requirement: S-TSS 6, S-TSS 7, S-TSS 11

REQ-TSS 2 The valid official time must be used for a time stamp.
cf. explanatory note on § 2 (4) SigG, § 16 (5) SigV
Safeguards pertaining to this requirement: S-TSS 6

REC-TSS 1 The standard time published by the PTB should be used for the time stamping service.
cf. § 16 (5) SigV
Safeguards pertaining to this recommendation: S-TSS 6

REQ-TSS 3 On request, the certification authority is to provide digital data with a time stamp (availability).
cf. § 9 SigG
Safeguards pertaining to this requirement: S-TSS 1, S-TSS 2

REC-TSS 2 In order to enable a time stamp to be obtained promptly and at any time, the time stamping service should be automatically retrievable.
cf. explanatory note on § 9 SigG
Safeguards pertaining to this recommendation: S-TSS 1, S-TSS 3, S-TSS 5, S-TSS 11

REQ-TSS 4 For the generation of time stamps, i.e. in particular the provision of a correct time and generation of the necessary digital signature, technical components are required which incorporate security safeguards to reliably detect forgeries of the digital signature and the use of a false time.
cf. § 9 (1) Sentence 2 SigG in conjunction with § 5 (5) Sentence 1 and 2 SigG and with § 14 (1) SigG, and explanatory note on § 9 SigG and § 14 (4) SigG
Safeguards pertaining to this requirement: S-TSS 7, S-TSS 8, S-TSS 9, S-TSS 11

REQ-TSS 5 The components of the time stamping service in which the required signature for the time stamp is generated must be evaluated and confirmed in accordance with standard E4 high.
cf. § 17 (1) SigV
Safeguards pertaining to this requirement: S-TSS 12

REQ-TSS 6 The certification authority is to take precautions to protect the technical components and private signature key which are used to generate the time stamp against unauthorised physical or logical access.
cf. § 11 SigV and explanatory note on § 11 SigV
Safeguards pertaining to this requirement: S-TSS 3, S-TSS 4, S-TSS 5

REQ-TSS 7 Security-related alterations to the technical components must be apparent to the user.
cf. § 16 (2) SigV
Safeguard pertaining to this requirement: S-TSS 10

REQ-TSS 8 For the digital signature in the area of the time stamping service a special signature key certified by the CA must be used which is automatically identifiable as a time stamp signature key. This is necessary, as when the same key is employed to sign both certificates and time stamps there is a risk that any data can be made into signed certificates by affixing a time stamp.
cf. § 4 (5) SigG
Safeguard pertaining to this requirement: S-TSS 8

REQ-TSS 9 The components of the time stamping service in which the time is ascertained and affixed to the data to be stamped must be evaluated and confirmed in accordance with standard 'E2'.
cf. § 17 (1) SigV
Safeguard pertaining to this requirement: S-TSS 13

### 6.5.3 Proposed solutions

The time (data, hour, minute, seconds where applicable and time zone) is ascertained by a radio receiver (DCF77, 77 kHz) and signed automatically together with the data to be signed. The form of data is irrelevant for the time stamping service. The data concerned may be signatures, hashed values or complete files. In parallel with this process, the correctness of the received time is verified by a local IT-supported reference clock. Alternatively, a GPS receiver or similar may also be used to determine the reference time. If a discrepancy is established

between the radio clock and the reference clock, the time stamping service will be shut down and a warning signal generated.

The use of a second-accurate time stamp is only possible when the discrepancies between the radio receiver and the reference clock resulting from technical aspects are within the milliseconds range. As a general principle, the permissible discrepancy between the clocks must not exceed half the response time guaranteed by the operator of the time stamping service. This response time should not exceed one minute.

The time stamping service is a user of the CA to which it is assigned. This limits the damage in the event of compromise of the time stamp key signature to one CA. The certificate of the time stamping service is kept available for retrieval in the directory service. Even when it belongs to the CA at an organisational level only (as part of the obligatory scope of services), the time stamping service nevertheless uses a signature key of its own, which is certified by the appurtenant CA.

In order to obtain a time stamp, the user sends his data via a publicly accessible telecommunications facility to a communications computer at the location of the operator offering the time service. An HTTP proxy with highly restricted functionality may be employed here, for example. The telecommunications access must be secured in such a manner as to preclude any attacks on the communications computer. The employed protocol stack must then be provided with appropriate packet filters which do not permit any additional form of use.

The communications computer is additionally linked via a secure protocol to a special security box. A store-and-forward process may be employed here, for example, whereby the communications computer stores the received data on a hard disk, from which they are collected at regular intervals by the time stamp security box. This security box is to be subject to the requirements specified in Section 6.7. Beyond this, the security box is also able to ascertain the current time and to compare this with the reference time. Alterations to the radio receiver or the reference clock are interpreted as manipulations of the security box. This time is signed in the box, together with the transmitted data and a serial number. The result is then sent back to the user via the communications computer. The user must verify whether the data provided with a time stamp correspond to the transmitted data, whether the time stamp is correct and whether the time used by the time stamping service is plausible.

To enable verification of a time stamp in suspected or actual cases of manipulation, each utilisation of the time stamping service is recorded on a medium which permits writing once only, in addition to which interlinked lists of generated time stamps can be employed. The time stamp signature key must be changed once annually at least.

Access to the time stamp computer is possible for trustworthy personnel only, after due identification and authentication.

In the course of verifying a time stamp it must be ascertained whether the employed time stamp signature key is revoked at the time of verification.

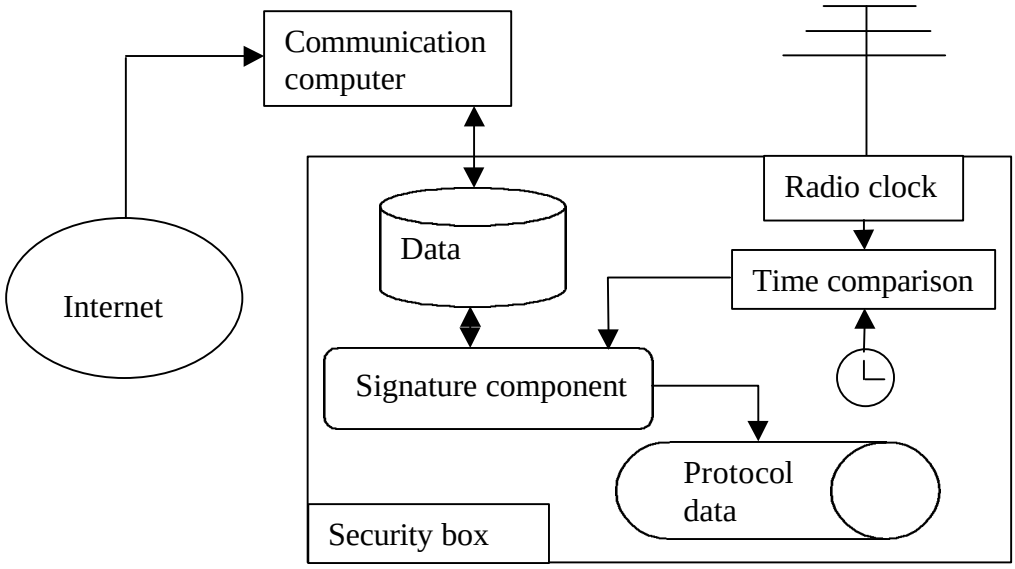



Fig.: Time stamping service

### 6.5.4 Safeguard catalogue

#### 6.5.4.1 Threats

The following enumeration does not draw a strict distinction between threats as defined in ITSEC and any vulnerabilities which may be exploitable as a result of implementation. Equally, the enumeration is certainly not to be regarded as complete or final.

1. Unauthorised access to the communications computer.
   Safeguards: S-TSS 3, S-TSS 4, S-TSS 12
2. Unauthorised access to the time stamp security box from the communications computer.
   Safeguards: S-TSS 5, S-TSS 12
3. Prevention of obtainment of a time stamp.
   Safeguards: S-TSS 1, S-TSS 2, S-TSS 12
4. Generation of a time stamp with a false time. This may occur via the transmission of a forged radio signal with a false time, for example.
   Safeguards: S-TSS 5, S-TSS 6, S-TSS 7, S-TSS 11, S-TSS 12
5. Generation of a time stamp with a false signature key.
   Safeguards: S-TSS 5, S-TSS 8, S-TSS 9, S-TSS 10, S-TSS 11, S-TSS 12
6. Generation of a time stamp without generation of an appurtenant record.
   Safeguards: S-TSS 9, S-TSS 11, S-TSS 12
7. Manipulation of data to be time-stamped before and during time-stamping.
   Safeguards: S-TSS 3, S-TSS 10, S-TSS 11, S-TSS 12
8. Misuse via loss or compromise of the time stamp signature key.
   Safeguards: S-TSS 8, S-TSS 10, S-TSS 11, S-TSS 12
9. Unauthorised alterations to the radio clock or the reference clock.
   Safeguards: S-TSS 9, S-TSS 10, S-TSS 11, S-TSS 12
10. Unauthorised generation of a certificate via the use of an identical secret key to generate certificates and time stamp signatures.
    Safeguards: S-TSS 8, S-TSS 12

Threats for the security box are dealt with in Section 6.7.

#### 6.5.4.2 Safeguards

##### 6.5.4.2.1 Safeguards to protect access

**S-TSS 1 Use of a communications server**

The server receives data via publicly accessible communications links.

**S-TSS 2 Redundancy of access channels**

The use of several different publicly accessible telecommunications links protects the availability of the time stamping service.

**S-TSS 3 Use of a special protocol to receive data which are to be provided with a time stamp**

This protocol and the necessary software implementation must be assessed at all levels to verify that no other functions, such as a remote log-in, can be executed on the communications computer. The testing in accordance with § 14 SigG must cover the software implementation for all involved network layers.

**S-TSS 4 Use of a secure operating system**

An operating system with functionality ITSEC F-C2 is employed for the communications computer, in addition to which requirements ITSEC A.38 and ITSEC A.39 of F.B2 are applied.

**S-TSS 5 Use of a special protocol for the transmission of data**

A special protocol is used for the transmission of data between the communications computer and the time stamp security box. This protocol and the necessary software implementation must be assessed at all levels to verify that no other functions, such as a remote log-in, can be executed on the time stamp security box. The testing in accordance with § 14 SigG must cover the software implementation for all involved network layers.

##### 6.5.4.2.2 Safeguards to protect the time

**S-TSS 6 Use of an IT-supported radio clock**

An IT-supported clock enables ascertainment of the current time published by the PTB and the date at the location of the time stamping service.

**S-TSS 7 Use of an IT-supported reference clock**

An IT-supported reference clock enables the discrepancies in relation to the radio clock to be ascertained independently of external influences. When discrepancies are established, the time stamp security box is shut down and a warning signal is generated.

##### 6.5.4.2.3 Safeguards relating to the security of time stamps

**S-TSS 8 Use of a special signature key**

The use of a special signature key makes the time service a user at a certification authority with a retrievable certificate. The employed signature key must be restricted to the exclusive use as a time stamp signature key by means of an attribute in accordance with § 7 (1) no. 7 SigG. Each time stamping service must use its own signature key. The public time stamp signature key must be retrievable in the directory service of the CA.

**S-TSS 9 Use of a recording component which permits writing once only**

Within the time stamp security box a recording component which permits writing once only is used, enabling all generated time stamps to be traced and identified. In the event of failure of the recording component, e.g. due to overflow of the storage medium, the time stamp security box must shut down operations automatically. Random access to any record entry must be possible. The following items of information at least must be recorded: $Signature_{TSS}$ (hash (data, time to be stamped)), time, serial number of the time stamp.

**S-TSS 10 Detectability of security-related alterations**

Alterations to the software components or files of the involved systems are evaluated by means of integrity tests. When a violation of integrity is established, the system is switched to a state in which access to the components to which the administration of rights applies is possible for specially authorised persons only (e.g. revisor).

**S-TSS 11 Use of a security box**

The security box automatically adds the current time (day, month, year, hour, seconds if applicable and time zone) and a serial number to the received data and subsequently signs the data with the time stamp signature key. This security box must fulfil all the requirements specified in Section 6.7.

**S-TSS 12 Testing and evaluation of components employed to generate signatures for time stamps**

The components of the time stamping service which are used to apply the private time stamp signature key must be evaluated and confirmed in accordance with ITSEC standard 'E4 high'.

**S-TSS 13 Testing and evaluation of components to ascertain the time and to combine the time with the data to be stamped**

All components of the time stamping service, with the exception of the components used to apply the private time stamp signature key, must be evaluated and confirmed in accordance with ITSEC standard 'E2 high'.

**S-TSS 14 Guaranteed times in connection with use of the time stamping service**

The guaranteed response time for the time stamping service should be in the range of one minute. The maximum down time should not exceed 180 minutes.

Further safeguards, in particular of an organisational nature, are to be found in Chapter 5 of this safeguard catalogue.

#### 6.5.4.3 Assignment of safeguards to solutions

| Safeguard | Counteracts threat | Solution |
|---|---|---|
| S-TSS 1 | 3 | required |
| S-TSS 2 | 3 | required |
| S-TSS 3 | 1, 7 | required |
| S-TSS 4 | 1 | required |
| S-TSS 5 | 2, 4, 5 | required |
| S-TSS 6 | 4 | required |
| S-TSS 7 | 4 | required |
| S-TSS 8 | 5, 8 | required |
| S-TSS 9 | 6 | required |
| S-TSS 10 | 5, 7, 8, 9 | required |
| S-TSS 11 | 4, 5, 6, 7, 8, 9 | required |
| S-TSS 12 | all | required |
| S-TSS 13 | all | required |
| S-TSS 14 | 3 | recommended |

#### 6.5.4.4 Assignment of the safeguards to the security requirements

| **Security requirements/ Recommendation** | **Safeguards** |
|---|---|
| REQ-TSS 1 | S-TSS 6, S-TSS 7, S-TSS 11 |
| REQ-TSS 2 | S-TSS 6 |
| REQ-TSS 3 | S-TSS 1, S-TSS 2 |
| REQ-TSS 4 | S-TSS 7, S-TSS 8, S-TSS 9, S-TSS 11 |
| REQ-TSS 5 | S-TSS 12 |
| REQ-TSS 6 | S-TSS 3, S-TSS 4, S-TSS 5 |
| REQ-TSS 7 | S-TSS 10 |
| REQ-TSS 8 | S-TSS 8 |
| REQ-TSS 9 | S-TSS 13 |
| REC-TSS 1 | S-TSS 6 |
| REC-TSS 2 | S-TSS 1, S-TSS 3, S-TSS 5, S-TSS 11 |

## 6.6 Operational environment

The following sections specify safeguards for the technical operational environment to generate and verify digital signatures.

The object of the security safeguards is to provide appropriate means to counter the threats in the operational environment in an effective manner. The specification is restricted to security safeguards for the operational environment in relation to the digital signature process. General security safeguards (such as virus protection, etc.) are implicitly assumed and not dealt with explicitly in this catalogue. The safeguard catalogue is open-ended. There are no restrictions to specific platforms (hardware, operating system). The safeguards are not restricted to hardware or software.

The safeguards apply irrespective of any special configurations of the operational environment. The safeguards take due account of all components of the operational environment for the signing and the verifying party which may have a direct or indirect influence on the trustworthiness of the digital signature. Depending on the configuration of the operational environment, such components will include, for example, input devices, output devices, chipcard reading devices, input devices for PIN or biometric characteristics, document selection mechanisms, signing components, verification components, access components for time stamping, certificate directory and revocation list services, mechanisms for data transmission to the chipcard, etc. The safeguards are to be implemented in these components in accordance with the specific configuration concerned. This is to be specified in the future by reference to example configurations in accordance with the course of technological development, and provided as an appendix to the catalogue.

### 6.6.1 Requirements stipulated in the Act and the Ordinance

| Reference | Quotation | Interpretation |
|---|---|---|
| **§ 14 (2) SigG** | Technical components with safeguards are required for the presentation of data to be signed which clearly indicate in advance the generation of a digital signature and enable identification of the data to which the digital signature applies. Technical components with safeguards are required for the verification of signed data which allow the integrity of the signed data, the data to which the digital signature applies and the holder of the signature key to whom the digital signature belongs to be established. | The technical operational environment must carry out authentic visualisation of the individual activities in the signing process, including the verification process, with guaranteed integrity. The clear visualisation process must guarantee that the signing process is carried out in full accordance with the user's wishes. The signature must be assignable to the data to be signed without any doubt.<br>The following must be visualised in the operational environment:<br>- the fact that a digital signature is generated prior to carrying out the signing process;<br>- the relationship of the signature to the digital data which are signed in the course of the signing and verification process;<br>- verification of the integrity and authenticity of the signed data at the recipient's location;<br>- assignment of the digital signature to the signature key holder.<br>Derived requirements: REQ-SHIF 1, REQ-SHIF 3, REQ-SHIF 4, REQ-SHIF 5. |

| | | |
|---|---|---|
| **Explanatory note on § 14 (2) SigG** | The processing of data for purposes relating to the digital signature must be effected in such a manner that the user can be adequately assured, for example, that the data displayed on the screen correspond to the signed data. This requires supplementary components to the standard scope of information technology equipment or special technical components.<br><br>With regard to the (automatic) verification of a digital signature, in addition to correct presentation of the signed data it must also be guaranteed that no false confirmation of correctness is output for the digital signature. No confirmation of correctness is to be output in the event of forgery of the signature or manipulation of the signed document. Also, the holder of the signature key with which the signature has been generated must be identifiable (directly via the certified public key).<br><br>Any person using technical components without appropriate security safeguards to process data to be signed or to verify signed data shall bear the risk for any incorrect results. The certification authorities are obliged in accordance with § 5 (5) Sentence 2 and § 9 to use appropriate technical components to generate signature key certificates and time stamps, and are furthermore subject to official control pursuant to § 13 in this respect. | See above. |
| **§ 4 (1) No. 2 SigV** | Personal identification numbers or other data used for identification in conjunction with the data storage medium with the private signature key must be kept secret. If such identification data is disclosed, or if there are grounds to assume it has been disclosed, the data must be changed without delay. | Identification data must be protected against unauthorised access and be changeable in the event of compromise.<br><br>Derived requirements: REQ-SHIF2, REQ-SHIF3. |
| **Explanatory note on § 4 (1) No. 2 SigV** | Modern processes enable the user himself to change the personal identification number or other data (e.g. the password) in the event of disclosure, in accordance with Number 2. | Alteration mechanisms can be provided both via the signing component and via the technical operational environment.<br><br>Derived requirement: REQ-SHIF 6. |

| | | |
|---|---|---|
| **§ 4 (1) No. 3 SigV** | For generation and verification of digital signatures, and for display of data that must be signed or of signed data that must be verified, technical components shall be used that fulfil the requirements of the Digital Signature Act and of this Ordinance and whose security pursuant to the Digital Signature Act and this Ordinance has been confirmed. Such components shall be protected from unauthorised access. | The technical operational environment must be evaluated and confirmed accordingly.<br>Derived requirements: REQ-SHIF 1, REQ-SHIF 2, REQ-SHIF 3, REQ-SHIF 4, REQ-SHIF 5. |
| **Explanatory note on § 4 (1) No. 3 SigV** | In accordance with No. 3 the applicant is to be notified of the need to use suitable technical components and informed as to which technical components fulfil the statutory requirements. | A list of evaluated and approved technical components must be provided by the regulatory authority. |
| **§ 4 (1) No. 5 SigV** | If a particular time can be of considerable significance with regard to use of signed data, a time stamp shall be appended. | The technical operational environment must provide a link to the time stamping service for such cases.<br>Derived requirement: REQ-SHIF 6. |
| **Explanatory note on § 4 (1) No. 5 SigV** | The question as to whether a particular time is of 'considerable significance' with regard to the use of signed data (no. 5) must be examined in each individual case. A time stamp is necessary for new digital signatures, for example (cf. § 18). | See above. |
| **§ 4 (1) No. 7 SigV** | In verification of digital signatures, it shall be determined whether the signature key certificate and attribute certificates were valid at the time the signature was generated, whether the signature key certificate contains restrictions pursuant to § 7 (1) No.7 of the Digital Signature Act and whether Numbers 4 and 5 were complied with, if applicable. | The technical operational environment must guarantee a link to the directory service and analysis of the certificates.<br>Derived requirement: REQ-SHIF 6. |

| | | |
|---|---|---|
| **Explanatory note on § 4 (1) No. 7 SigV** | Verification of the validity of certificates in accordance with Number 7 includes checking the digital signatures which belong to the certificates. It is left to the discretion of the person verifying the signature to decide whether the certificates should additionally be verified via the appropriate public directory of certificates (whether they are registered there and were valid at the time of generation of the signature). | See above. |
| **§ 5 (1) SigV** | If the signature key holder generates signature keys, the certification authority shall reliably establish whether the signature key holder uses suitable technical components, pursuant to the Digital Signature Act and this Ordinance, for storage and use of the private key signature. | When key generation and key management are carried out by the user, the technical operational environment must keep the necessary security mechanisms available for verification.<br>Derived requirements: REQ-SHIF 1, REQ-SHIF 2, REQ-SHIF 3. |
| **§ 16 (1) SigV** | The technical components required for generation of signature keys must function in such a manner that it is nearly certain that any given key can occur only once and that a private key cannot be derived from the relevant public key. The secrecy of private keys must be assured, and it must not be possible to duplicate keys. Security-relevant changes in technical components must be apparent for the user. | When key generation and key management are carried out by the user, the technical operational environment must provide the basic supporting framework to enable generation and management of the signature keys on the signing component.<br>Derived requirements: REQ-SHIF 1, REQ-SHIF 2, REQ-SHIF 3. |

| | | |
|---|---|---|
| **§ 16 (2) SigV** | The technical components required for generation or verification of digital signatures must function in such a manner that the private signature key cannot be derived from the signature and the signature cannot be forged by any other means. Use of the private signature key must be possible only following identification of the holder and must require proper possession and knowledge; the key must not be disclosed during use. Biometrical characteristics may also be used for identification of the signature key holder. The technical components required for collecting identification data must function in such a manner that they do not reveal identification data and that the identification data is stored only on the data storage medium with the private signature key. Security-relevant changes in technical components must be apparent for the user. | The identification and authentication mechanisms of the operational infrastructure must ensure that the user authentifies himself to the signature component prior to signature generation. Suitable measures must be provided to display security-related changes to these components.<br><br>Derived requirements: REQ-SHIF 1, REQ-SHIF 2, REQ-SHIF 3. |

| | | |
|---|---|---|
| **Explanatory note on § 16 (2) SigV** | The signing technology is generally implemented on a chipcard or a comparable data-carrier (e.g. PCMCIA card). Biometric characteristics (e.g. face, personal signature or finger structure) may be used in order to establish a link between card and owner beyond possession (card) and knowledge (PIN or password).<br><br>The technical components may be designed so as to require renewed input of the identification data, either prior to each digital signature or after the elapse of a certain period during which the signing technology is not used. The procedure to be adopted by the user remains at his discretion - with due regard to the specific application environment.<br><br>The identifiability of security-relevant changes required in Sentence 6 is intended to protect the user from changes of relevance to security, which in this context may in particular be aimed at disclosing the private signature key or the identification data. cf. also explanatory note on subsection 1. | See above. |

| | | |
|---|---|---|
| **§ 16 (3) SigV** | The technical components required for display of data for signing must function in such a manner that the person signing can reliably determine what data is to receive the signature; that a digital signature is provided only at the initiation of the person signing; and that such initiation is clearly indicated in advance. The technical components required for verifying signed data must function in such a manner that the person verifying can reliably establish what data has received the digital signature; that the person verifying can reliably establish the identity of the signature key holder; and that the correctness of the digital signature is reliably verified and appropriately displayed. The technical components for verifying certificates must permit clear, reliable determination of whether verified certificates were present, without having been invalidated, in the register. The technical components must permit adequate determination, as necessary, of the contents of signed data or of data that is to be signed. If technical components pursuant to Sentences 1 to 4 are commercially provided to third parties for use, clear, reliable interpretation of the relevant data must be assured, and the technical components must automatically be checked for genuineness when used. Security-relevant changes in technical components must be apparent for the user. | The technical components for the signing process must visualise the fact that a signature has been generated and the contents of the data to be signed in a form which enables authentic interpretation by the signing party, with guaranteed integrity.<br><br>The technical components for the verification process must visualise the contents of the data to be signed and the appropriate confirmation of correctness of the digital signature in a form which enables authentic interpretation by the party verifying and guaranteed integrity.<br><br>The technical operational environment must ensure a link to the directory service and enable analysis of the certificates.<br><br>Appropriate measures must be implemented to display changes to the technical operational environment which are of relevance to security.<br><br>Derived requirements: REQ-SHIF 1, REQ-SHIF 2, REQ-SHIF 3, REQ-SHIF 4, REQ-SHIF 5, REQ-SHIF7. |
| **Explanatory note on § 16 (3) SigV** | A person generating a digital signature must be able to rely on the fact that displayed and signed data (e.g. requested data) correspond, and that he has not been 'duped' into signing different data (Sentence 1). With regard to the verification of a digital signature, he must be able to rely on the fact that the signature of the displayed data has been verified and on the confirmation of correctness (Sentence 2).<br><br>With regard to the verification of certificates (cf. § 4 (5) Sentence 3 and § 5 (1) Sentence 2, Digital Signature Act) | See above. |

| | | |
|---|---|---|
| | the party verifying must be able to rely on the correctness of the information specified in Sentence 3. This provision is supplemented by appropriate procedures for the technical components used to store and maintain the directories of certificates in accordance with (4) Sentence 2. The following means are available to the user for the purpose of verifying the validity of certificates:<br><br>- By means of an internal check using the public key of the regulatory authority, he can ascertain whether the certificate originates from an officially approved certification authority and, on the basis of the entries in the certificate, whether the certificate was valid at the (stated or assumed) time of generation of the digital signature which is to be verified.<br><br>- Additionally, he can transmit an on-line request for verification in the regulatory authority's directory of certificates, to establish whether the certificate is registered in this directory and was valid at the time of generation of the digital signature. Alternatively, he may also obtain information from a current internal revocation list (cf. explanatory note on § 8 (1) and § 9 (3)).<br><br>- In the case of foreign certificates, he may also submit an on-line request for verification in the regulatory authority's directory of certificates, in order to establish whether the certificate of the foreign root authority is registered in this directory (cf. § 8 (2) Sentence 2 and 3).<br><br>In accordance with § 14 (2) of the Digital Signature Act, the digital signature relates solely to the digital data and is independent of the interpretation of these data (e.g. text, language, music, software). However, where necessary (particularly in the case of texts), a person generating or verifying a signature must also be able to identify the contents of the signed data or the data to be signed "to an | |

| | | |
|---|---|---|
| | adequate extent" (Sentence 4). Special formats and application programmes may be used for certain applications (e.g. home banking).<br><br>When technical components are provided for use to third parties on a commercial basis, the users are to be enabled to verify the authenticity of these components at the beginning of use (Sentence 5), in order to prevent "duping" with false data via manipulated technical components. The authenticity and security status of the technical components can be ascertained, for example, via automatic authentication to the user's chipcard.<br><br>The requirement for changes of relevance to security to be identifiable in accordance with Sentence 6 also applies to privately used technical components. cf. also explanatory note on (1). | |

| | | |
|---|---|---|
| **§ 17 (1) SigV** | Testing of technical components pursuant to § 14 (4) of the Digital Signature Act must conform to the ";Criteria for assessment of the security of information technology systems";<br><br>(GMBl. 1992, S. 545). For technical components for generation of signature keys or for storage or use of private signature keys, and for technical components commercially provided to third parties for use, such tests must conform to the "E4" test standard; otherwise, they must conform to the "E2" test standard. The strength of the security mechanisms must be rated as "high"; and the algorithms and pertinent parameters must be assessed as suitable pursuant to (2). | The components of the technical operational environment must be tested and assessed in accordance with the appropriate ITSEC test standard, prior to being employed for the generation and verification of digital data.<br><br>On the basis of the individual scenarios for the technical operational environment, this results in the following test standards:<br><br>Components for generating digital signatures, including:<br><br>• recording and verification of identification data<br><br>• display of data to be signed<br><br>E 2 high<br><br>Components for verifying digital data, including<br><br>• display of signed data<br><br>• verification of certificates<br><br>E 2 high<br><br>Components for generating and verifying digital signatures which are offered for use to third parties on a commercial basis:<br><br>E 4 high<br><br>Derived requirements: REQ-SHIF 1, REQ-SHIF 2, REQ-SHIF 3, REQ-SHIF 4, REQ-SHIF 5. |

### 6.6.2 Security requirements and recommendations

REQ-SHIF 1 The operational environment must sign the data which are displayed to the party signing in a reliable, unambiguous and non-forgeable manner.
cf.: § 14 (2) SigG, § 4 (1) No. 3 SigV, § 5 (1) SigV, § 16 (1), (2) and (3) SigV, Explanatory note on § 16 (2) and (3) SigV, § 17 (1) SigV
Safeguards pertaining to this requirement: S-SHIF 1.3, S-SHIF 2.1, S-SHIF 2.2, S-SHIF 3.1, S-SHIF 3.2, S-SHIF 6.1, S-SHIF 7.1 to S-SHIF 7.4

REQ-SHIF 2 The operational environment must only sign when the signature-key holder expressly wishes a signature to be effected.
cf.: § 4 (1) No. 2 and No. 3 SigV, § 5 (1) SigV, § 16 (1), (2) and (3) SigV, Explanatory note on § 16 (2) and (3) SigV, § 17 (1) SigV
Safeguards pertaining to this requirement: S-SHIF 1.1 to S-SHIF 1.4, S-SHIF 4.1, S-SHIF 4.2, S-SHIF 7.1 to S-SHIF 7.4

REQ-SHIF 3 The operational environment must only sign those data which have been displayed to the signature key holder and which have actually been released for signing by the latter.
cf.: § 14 (2) SigG, § 4 (1) No. 2 and No. 3 SigV, § 5 (1) SigV, § 16 (1), (2) and (3) SigV, Explanatory note on § 16 (2) and (3) SigV, § 17 (1) SigV
Safeguards pertaining to this requirement: S-SHIF 1.1 to S-SHIF 1.4, S-SHIF 7.1 to S-SHIF 7.3

REQ-SHIF 4 The operational environment must verify the data which are displayed to the verifying party in a reliable, unambiguous and non-manipulable manner.
cf.: § 14 (2) SigG, § 4 (1) No. 3 SigV, § 16 (3) SigV, § 17 (1) SigV
Safeguards pertaining to this requirement: S-SHIF 3.1, S-SHIF 3.3, S-SHIF 5.1, S-SHIF 5.2, S-SHIF 7.1 to S-SHIF 7.5

REQ-SHIF 5 The operational environment must provide the result of the verification process in unambiguous and non-manipulable form.
cf.: § 14 (2) SigG, § 4 (1) No. 3 SigV, § 16 (3) SigV, § 17 (1) SigV
Safeguards pertaining to this requirement: S-SHIF 3.3, S-SHIF 7.1 to S-SHIF 7.4

REQ-SHIF 6 The operational environment must provide the general conditions for application of the signing process. This involves auxiliary safeguards:

- for retrieving and assessing the directory authority's certificate lists,
- for obtaining a time stamp from the time stamping service,
- for altering authentication data of the signing component and of the technical operational environment,
- for key generation on the signing component.

cf.: § 4 (1) No. 2, No. 5 and No. 7 SigV, § 17 (1) SigV
Safeguards pertaining to this requirement: S-SHIF 1.1, S-SHIF 1.2, S-SHIF 5.1, S-SHIF 5.2, S-SHIF 6.1

REQ-SHIF 7 In cases of commercial use by third parties, the operational environment must verify the authenticity of the technical components automatically and render any technical changes apparent to the user.
cf.: § 16 (3) SigV, § 17 (1) SigV
Safeguards pertaining to this requirement: S-SHIF 7.2

### 6.6.3 Proposed solutions

The requirements imposed on the technical operational environment can be implemented in various scenarios. These scenarios are outlined below. Special architectures for individual scenarios are discussed in Appendix A. The list of architectures is not to be regarded as complete, and is to undergo continual updating in accordance with technical developments in the area of digital signatures. The generic safeguards pertaining to the respective scenarios are then to be specified by reference to implemented architectures. In accordance with § 17 (1) SigV, a distinction is drawn between applications in the private sphere, which require ITSEC test standard 'E2 high', and applications concerning commercial use by third parties, which require evaluation in accordance with ITSEC test standard 'E4 high'.

#### 6.6.3.1 Single-user PC in the private sphere

The single-user PC in the private sphere is characterised by the fact that only the role of the user exists for the PC. Apart from the signing process, other applications may also be installed on the PC. Operation in the private sphere requires evaluation in accordance with ITSEC test standard 'E2 high'. The classical area of use is in the home and the normal office environment.

#### 6.6.3.2 Multi-user PC in the private sphere

The multi-user PC in the private sphere is characterised by the fact that various roles exist for the PC, such as user, administrator, revisor, maintenance technician, etc. Apart from the signing process, other applications may also be installed on the PC. Operation in the private sphere requires evaluation in accordance with ITSEC test standard 'E2 high'. The classical area of use is in the home and in the normal office environment.

#### 6.6.3.3 Single-user PC for commercial use by third parties

The single-user PC for commercial use by third parties is characterised by the fact that only the role of user exists for the PC. Apart from the signing process, other applications may also be installed on the PC. Operation for commercial use by third parties requires evaluation in accordance with ITSEC test standard 'E4 high'. The classical area of use is in the external service sector.

#### 6.6.3.4 Multi-user PC for commercial use by third parties

The multi-user PC for commercial use by third parties is characterised by the fact that various roles exist for the PC, such as user, administrator, revisor, maintenance technician, etc. Apart from the signing process, other applications may also be installed on the PC. Operation for commercial use by third parties requires evaluation in accordance with ITSEC test standard 'E4 high'. The classical area of use is in the external service sector..

#### 6.6.3.5 Monofunctional signing device for commercial use by third parties

The monofunctional signing device is characterised by the fact that only the role of user exists for the PC, and that no other applications are installed apart from the signing process. The classical area of application is in the public service sector for commercial use by third parties, which requires evaluation in accordance with ITSEC test standard 'E4 high'. Application as a self-contained signing station in the private office environment is also possible, in which case evaluation in accordance with ITSEC test standard 'E2 high' is required.

#### 6.6.3.6 Signing computer for the automatic processing of signing jobs

The signing computer for the automatic processing of signing jobs is characterised by the fact that various roles exist, such as user, administrator, revisor, maintenance technician, etc., and that no other applications are installed apart from the signing process. Application may take place in the private sphere within companies or in the public service sector for commercial use by third parties. Operation in the private sphere requires evaluation in accordance with ITSEC test standard 'E2 high'. Operation in the public sector for commercial use by third parties requires evaluation in accordance with ITSEC test standard 'E4 high'.

### 6.6.4 Safeguard catalogue

#### 6.6.4.1 Threats

The following enumeration does not draw a strict distinction between threats as defined in ITSEC and any vulnerabilities which may be exploitable as a result of implementation. Equally, the enumeration is certainly not to be regarded as complete or final.

1. Data other than those which are displayed to the user and which the user wishes to sign are signed.
   Safeguards: S-SHIF 1.3, S-SHIF 2.1, S-SHIF 2.2, S-SHIF 3.1, S-SHIF 3.2, S-SHIF 6.1, S-SHIF 7.1 to S-SHIF 7.4
2. Data are signed, although the user does not wish to sign them.
   Safeguards: S-SHIF 1.1 to S-SHIF 1.4, S-SHIF 4.1, S-SHIF 4.2, S-SHIF 7.1 to S-SHIF 7.4
3. Data which do not constitute the actually verified data are displayed as having been positively verified.
   Safeguards: S-SHIF 3.1, S-SHIF 3.3, S-SHIF 5.1, S-SHIF 7.1 to S-SHIF 7.5
4. A verification result is displayed which does not correspond to the actual result of the verification process.
   Safeguards: S-SHIF 3.3, S-SHIF 7.1 to S-SHIF 7.4
5. A signing party is identified and displayed who has not actually generated the signature.
   Safeguards: S-SHIF 1.1, S-SHIF 1.2, S-SHIF 1.4, S-SHIF 3.3, S-SHIF 5.1, S-SHIF 7.1 to S-SHIF 7.4
6. Signing is effected using a private key of the user in an unauthorised manner.
   Safeguards: S-SHIF 2.1, S-SHIF 2.2, S-SHIF 5.2

7. Signing is effected via the improper use of a private key of another user.
   Safeguards: S-SHIF 1.1, S-SHIF 1.2, S-SHIF 1.4, S-SHIF 2.1, S-SHIF 2.2, S-SHIF 6.1
8. Signing or verification is effected with a non-secure technical operational environment.
   Safeguards: S-SHIF 1.3, S-SHIF 7.1 to S-SHIF 7.5

#### 6.6.4.2 Generic safeguards

##### 6.6.4.2.1 Identification and authentication

**S-SHIF 1.1 Identification and authentication of the user to the signing component**

Prior to generating signatures, the user must identify and authenticate himself to the signing component which contains the signature key, in accordance with S-CHIP 7.1 and S-SBOX 1.1-1.5. For this purpose, the technical operational environment receives the input data from the user, passes them on to the signing component and displays the reply. Identification and authentication are effected via a reliable channel between user and operational environment, and are initiated by the user. The possibility of undetected tapping of the identification and authentication data along the transmission channel is excluded. Further interaction is possible only after successful identification and authentication. After successful authentication, the signing component is enabled for a specified period or a specified number of signatures. This can be preset on the signing component or defined individually by the user. In the latter case input of the period or the number of signatures to be effected in connection with the authentication is combined directly with the input of the authentication data.

**S-SHIF 1.2 Identification and authentication of the user to the technical operational environment**

When various roles (user, administrator, revisor, maintenance technician, ...) are defined in the operational environment, the activities relating to which may influence the reliability and integrity of the signing and verification process, the user must identify and authenticate himself to the technical operational environment. Authentication may be effected on the basis of possession and knowledge, for example. Further interaction is possible only after successful authentication. The number of unsuccessful attempts is limited, e.g. to 3 successive attempts, after which access is blocked for this user. The authentication information is protected against unauthorised access. Any suspected compromising of this information is displayed directly to the user. Activation of the signing process is then possible only after authorised alteration of the authentication data. Authentication data may take the form of passwords, PINs or biometric reference data, for example. The operational environment provides functions for the input, storage and verification of these authentication data. The authentication data are copied in encoded form into a hidden file to which no direct access is possible

In the case of authentication by means of knowledge-based authentication data (e.g. password, PIN), each user can alter the authentication data after successful identification and authentication. After identification and authentication of the user for the first time, the user is compelled to alter preset authentication data. The authentication data must possess a minimum length - e.g. 6 characters. Prior to accepting authentication data which are to be altered, a check is carried out to avoid trivial data. The period of validity of authentication data is limited.

**S-SHIF 1.3 Use of signing components after due authentication of the technical operational environment**

When a user employs his signing component in a technical operational environment for use on a commercial basis by third parties, identification and authentication of the operational environment must be carried out in accordance with S-CHIP 7.2 and S-SBOX 1.6.

**S-SHIF 1.4 Log-out on completion of the signing process**

The signing process may comprise several signing operations in batch mode. After completion of the signing process and/or the period of enablement in accordance with S-SHIF 1.1, log-out of the user in relation to the signing component and in relation to the technical operational environment is effected automatically, whereby this log-out function cannot be deactivated. When a chipcard is used as the signing component, the signing party is requested beforehand to remove his chipcard from the terminal. The withdrawal of the chipcard is recorded. The log-out process is effected in its entirety and cannot be aborted. An automatic log-out is effected after a signing process has been inactive for a defined period without being terminated. Further interaction with the operational environment is then possible only after renewed identification and authentication. During brief periods of inactivity, a screen blocking function is activated and cannot be deactivated. When the screen blocking function is active, the halted signing process cannot be resumed prior to verification of the user's indicator.

#### 6.6.4.2.2 Access control

**S-SHIF 2.1 Administration of rights**

When various roles are defined in the operational environment in accordance with S-SHIF 1.2, these roles are subject to administration of the appurtenant rights. The roles in the technical operational environment are clearly defined together with the appurtenant rights. Each registered user is assigned a role together with his specific rights in unambiguous and non-manipulable form.

**S-SHIF 2.2 Verification of rights**

All identification and authentication information in accordance with S-SHIF 1.2 and all data, software components and memory areas which are used directly for the generation and verification of signatures are subject to access control, so as to ensure that only authorised persons and processes have access. Prior to granting access, the authorisation of the identified and authenticated user is verified in accordance with the administration of rights. The desired access is possible only after successful verification. Unauthorised attempts to access data and components are recorded with the user ID, object ID, type and time of access.

#### 6.6.4.2.3 Secure display

**S-SHIF 3.1 Use of a secure selection component**

The data to be signed and/or verified are selected by the party signing by means of an unambiguous selection mechanism. The selection criterion must be unambiguous in the operational environment. The number of data to be signed is checked to verify that it does not conflict with the enablement period or the number of signatures specified during the authentication process in accordance with S-SHIF 1.1. The signing process is activated only after positive verification that no such conflicts apply.

All information required for the signing process must be unambiguous and must furthermore be linked to the data and displayable in a manner which excludes the possibility of manipulation.

**S-SHIF 3.2 Use of a secure visualisation component for the signing process**

In the course of the signing process the secure display shows the user the selected data to which the digital signature will apply if the user decides that he wishes to sign these data. The act of generation of a digital signature is displayed to the user beforehand, whereby this display function cannot be deactivated.

The data and the appurtenant signing information are displayed clearly and in their entirety, thus enabling the signing party to identify beyond doubt which items of data he is signing. When the data cannot be shown in its entirety with an adequate degree of accuracy, the user is provided with a function (zoom, scroll) which enables him to select all parts of the display and to view the data with the necessary degree of accuracy. He is furthermore provided with an overview showing him which part he is presently viewing and which parts make up the rest of the overall display.

The display component is designed in such a manner as to ensure that signatures, certificates, etc. pertaining to the signed data cannot be confused with the contents of documents displayed by the visualisation component.

**S-SHIF 3.3 Use of a secure visualisation component for the verification process**

In the course of the verification process the secure display shows the user which data the digital signature applies to, whether the data remain unchanged and which signature key holder the digital signature is to be attributed to. Secure display of the data which are linked to the signature, of the verification result (verification OK) and of the identity of the signature key holder is always effected in direct combination, thus ensuring the integrity of the attribution of data, verification OK and identity. The identity of the signature key holder is established via interpretation of the signature certificate. Whenever verification is not possible in this connection, e.g. due to the absence of a verification key, this fact is always displayed. 'Always' means that this display function cannot be deactivated.

#### 6.6.4.2.4 Signing process dependent on the user's consent

**S-SHIF 4.1 Provision of a signing process which is dependent on the user's consent**

After the user has been shown the data to be signed by means of the secure display, a decision is received from the user in the form of an input. His decision may relate to individual items of data or to a sequence of data selected in accordance with S-SHIF 3.1. Only when the user's input signifies his decision to generate the signature are the signed data transferred directly to the cryptographic signing function. The dialogue leading to the decision is unambiguous. The data to be signed are forwarded directly to the signing process - where appropriate after undergoing the hashing process - and are protected from manipulation throughout the entire hashing and signing process. This protection is ensured by the operating system or by supplementary security components in the operational environment.

The result of the signature generation process is shown directly on the secure display by means of a message stating 'Signing of data ... by user ... successfully completed', whereby this display function cannot be deactivated and requires no action on the part of the user. In the event of failure of the signing process, a appropriate error message is displayed.

**S-SHIF 4.2 Unambiguous user prompting during the signing process**

The technical operational environment incorporates an unambiguous user prompting system. If possible, the operational environment should incorporate a user interface with an integrated user prompting system, in order to avoid wrong decisions by the user during the signing and verification process. At each point in the process, the user is shown which component of the

signing and verification process will be started upon selecting a specific function. Critical decisions are highlighted and safeguarded by means of an additional confirmation. Wherever possible, an on-line help function should be available for each decision required by the user prompting system.

#### 6.6.4.2.5 Connection to the directory and time stamping services

**S-SHIF 5.1 Reliable link from the operational environment to the directory service of the certification authority**

The validity of the signing party's certificate, including any appurtenant restrictions, can be verified using the directory service of the competent certification authority. The link from the operational environment of the verifying party to the directory service of the certification authority is established in an unambiguous and verifiable manner. Communications are effected in authentic mode. Inquiries to the directory service must identify the certificate to which the inquiry relates, that is, they must contain the identification of the certificate in accordance with S-DIR 4.5 and S-DIR 4.6 (e.g. the serial number). The time to which the inquiry relates can be specified explicitly. Otherwise, the inquiry relates to the current time. Retrievable certificates are then returned to the inquirer together with a statement in accordance with Section 6.4.3, while in the case of non-retrievable certificates or an incorrect serial number the inquirer receives only a reply as specified in Section 6.4.3. The supplied result is provided with a time stamp and signed with the signature key of the directory service. The public key and the certificate of the directory service are used to carry out a check in the operational environment in order to verify whether the information originates from a current, non-manipulated certificate directory. The result of this verification is displayed to the user directly and in non-manipulable form. After successful retrieval and verification of the certificate, the operational environment extracts the data required for verification in accordance with § 7 (1) SigG in non-manipulable mode guaranteeing integrity and displays these data to the user, together with the reply from the directory service in accordance with Section 6.4.3. On receipt of a negative reply from the directory service, the user is shown only the statement from the directory service in accordance with Section 6.4.3.

The course of the inquiry is recorded in the operational environment in non-manipulable form, including the ID of the certification authority, the ID of the verified signing party and the result of the inquiry.

**S-SHIF 5.2 Reliable link from the operational environment to the time stamping service of the certification authority**

For the purpose of generating time stamps to provide an authenticate point in time, e.g. for the effected digital signature, the link from the operational environment to the time stamping service of the certification authority is established in unambiguous and verifiable form. Communications are effected in authentic mode.

The data are transmitted to the time stamping service. The latter appends the authentic time, signs the data with the time stamp signature key and returns everything to the operational environment. Confidential or comprehensive volumes of data can be hashed by the user beforehand, using a hashing function which has been proclaimed valid. In this case, the hashing value is transmitted to the time stamping service.

The public key and the certificate of the time stamping service are used in the operational environment to verify whether the signature is provided with a current and non-manipulable time stamp of the service. The result of this verification and the signature with appended time stamp are displayed to the user directly and in non-manipulable form.

The course of the time stamping process is recorded in the operational environment in non-manipulable form, covering the ID of the certification authority, the ID of the signature or of the data belonging to the signature, the time of stamping and the result of the subsequent verification.

#### 6.6.4.2.6. Supporting safeguards for key generation

**S-SHIF 6.1 Safeguards to support secure key generation**

When key pairs for digital signatures are generated by the user himself, the operational environment must provide the interface between user and signing component to activate the process of key generation on the signing component. The key generation process is activated via the entry of an unambiguous command by the user, after successful identification and authentication of the user in accordance with S-SHIF 1.1 and S-SHIF 1.2.

#### 6.6.4.2.7 Reliability of the operational environment

**S-SHIF 7.1 Security features of the operating system**

The reliability of the signing process is based on the security of the operating system in the technical operational environment. Standard operating systems deployed in multi-user mode in accordance with S-SHIF 1.2 must be proven to provide security functionality of standard F-C2 at least (ITSEC functionality class, see Appendix B). Alternatively, the security functionality may be achieved by means of supplementary components, provided that these are proven to provide the required security functionality.

**S-SHIF 7.2 Verification of integrity of the technical operational environment**

The technical operational environment for the signing and verification process must be protected against undetected manipulation. The integrity of the technical operational environment must be verified after each signing and verification process. The result of the integrity check is displayed to the user in non-manipulable form in the operational environment and recorded together with the time. The record can only be deleted after being displayed in clear form and subject to an explicit decision on the part of the revisor. Should a breach of integrity be established, the operational environment will be blocked for all signing and verification activities. After maintenance work, it must be released for operation again by means of an explicit command input in an authorised manner.

**S-SHIF 7.3 Maintenance of the operational environment in a manner guaranteeing integrity**

The technical operational environment for the signing and verification process must be protected against undetected manipulation during repair and maintenance work on the hardware and software components. The effects on the signing process are examined and disclosed. After the completion of maintenance work, the reference value for the integrity checks in the signing process are updated. Each maintenance activity is recorded, specifying the cause, IDs and version numbers of the components concerned, IDs and version numbers of the new components, the person responsible for the maintenance work and the time. Every maintenance activity is traceable and reversible. Every configuration of the operational environment is restorable. Only replacement components which have been approved (certified, confirmed) for the operational environment in the signing process are used in maintenance work.

### S-SHIF 7.4 Records

The technical operational environment records all actions which are of relevance or critical to the security of the signing and verification process for the purposes of analysis and the preservation of evidence. The record data can be evaluated by the revisor in a manner which precludes manipulation. The protocol data are protected against unauthorised alteration.

### S-SHIF 7.5 Use of certified operational environments

In order to support the verification of an effected digital signature it may be important to establish that a user has generated the signature in a reliable and approved operational environment of guaranteed integrity.

For this purpose, operational environments may possess a signing component of their own, containing a public and private key and the appurtenant certificate. Such data requiring protection are stored in areas which possess special protection against unauthorised access (e.g. security modules). Processing of these data takes place in these areas only. Any attempt to manipulate the data will result in automatic deletion of the private key.

After due authentication of the operational environment to the signing component in accordance with S-SHIF 1.3, an unambiguous indicator (e.g. the indicator of the technical operational environment or an arbitrary, but well defined, character string) can be generated on the signing component, for example. This indicator records whether the signature is generated in a reliable, approved operational environment of guaranteed integrity. The indicator is evaluated in the course of the verification process. The result is displayed in non-manipulable form, thus enabling the verifying party to establish whether the signature has been generated in an approved, non-manipulated operational environment.

### 6.6.4.3 Assignment of safeguards to solutions

| Safeguard | Counteracts threat | Solution model | | | | | |
|---|---|---|---|---|---|---|---|
| | | 6.6.3.1 Single-user PC E2 | 6.6.3.2 Multi-user PC E2 | 6.6.3.3 Single-user PC E4 | 6.6.3.4 Multi-user PC E4 | 6.6.3.5 Mono-functional signing device E2 \| E4 | 6.6.3.6 Signing computer E2 \| E4 |
| S-SHIF 1.1 | 2, 5, 7 | req | req | req | req | req | req |
| S-SHIF 1.2 | 2, 5, 7 | nr | req | nr | req | nr | req |
| S-SHIF 1.3 | 1, 2, 8 | nr | nr | req | req | rec \| req | rec \| req |
| S-SHIF 1.4 | 2, 5, 7 | req | req | req | req | req | req |
| S-SHIF 2.1 | 1, 6, 7 | nr | req | nr | req | nr | req |
| S-SHIF 2.2 | 1, 6, 7 | nr | req | nr | req | nr | req |
| S-SHIF 3.1 | 1, 3 | req | req | req | req | req | req |
| S-SHIF 3.2 | 1 | req | req | req | req | req | req |
| S-SHIF 3.3 | 3, 4, 5 | req | req | req | req | req | req |
| S-SHIF 4.1 | 2 | req | req | req | req | req | req |
| S-SHIF 4.2 | 2 | req | req | req | req | req | req |
| S-SHIF 5.1 | 3, 5 | req | req | req | req | req | req |
| S-SHIF 5.2 | 6 | req | req | req | req | req | req |
| S-SHIF 6.1 | 7 | req | req | req | req | req | req |
| S-SHIF 7.1 | 1, 2, 3, 4, 5, 8 | nr | req | nr | req | nr | req |
| S-SHIF 7.2 | 1, 2, 3, 4, 5, 8 | req | req | req | req | req | req |
| S-SHIF 7.3 | 1, 2, 3, 4, 5, 8 | rec | rec | req | req | req | req |
| S-SHIF 7.4 | 1, 2, 3, 4, 5, 8 | rec | rec | req | req | req | req |
| S-SHIF 7.5 | 3, 8 | rec | rec | rec | rec | rec | rec |

req = required, rec = recommended, nr = not required

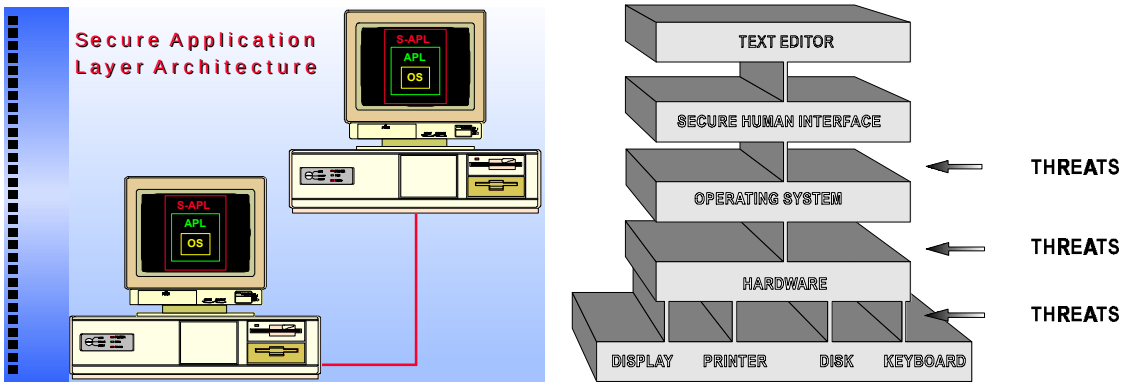
#### 6.6.4.4 Assignment of safeguards to security requirements

| Security requirement/ Recommendation | Measures |
|---|---|
| REQ-SHIF 1 | S-SHIF 1.3, 2.1, 2.2, 3.1, 3.2, 6.1, 7.1-7.4 |
| REQ-SHIF 2 | S-SHIF 1.1 - 1.4, 4.1, 4.2, 7.1-7.4 |
| REQ-SHIF 3 | S-SHIF 1.1-1.4,7.1-7.3 |
| REQ-SHIF 4 | S-SHIF 3.1, 3.3, 5.1, 5.2, 7.1-7.5 |
| REQ-SHIF 5 | S-SHIF 3.3, 7.1-7.4 |
| REQ-SHIF 6 | S-SHIF 1.1, 1.2, 5.1, 5.2, 6.1 |
| REQ-SHIF 7 | S-SHIF 7.2 |

# A. Example scenarios for the technical operational environment

This appendix discusses special architectures for individual scenarios of the operational environment by reference to examples. The list of architectures is not to be regarded as complete, and is to undergo continual updating in accordance with technical developments in the area of digital signatures. The generic safeguards for the respective examples contained in this catalogue are then to be defined in more specific terms by reference to implemented architectures.

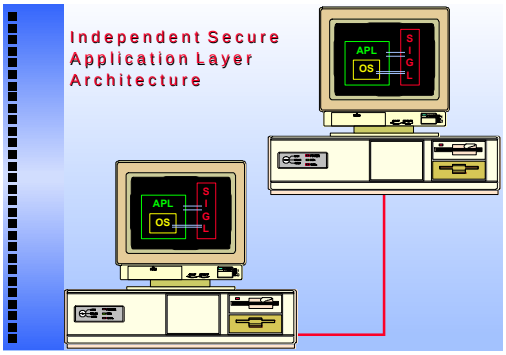
## A.1 PC with standard operating system and standard hardware

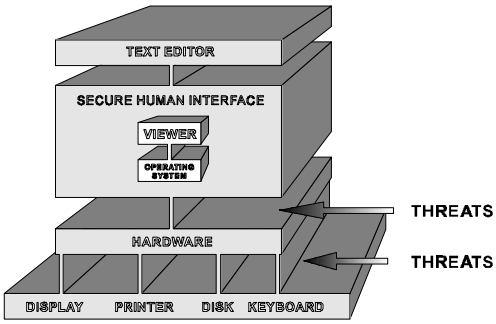



[Glossary: APL - Application Layer; OS - Operating System; S-APL - Signature Application Layer]

The standard PC architecture is characterised by activation of the signing process from a standard application on a standard computer with a standard operating system. The reliability of the signing process is directly dependent on the reliability of the employed standard applications, operating system functions and hardware utilities. This architecture represents a possible embodiment of solution proposals 6.6.3.1 and 6.6.3.2.

## A.2 PC with independent operating system for the signing process on standard hardware

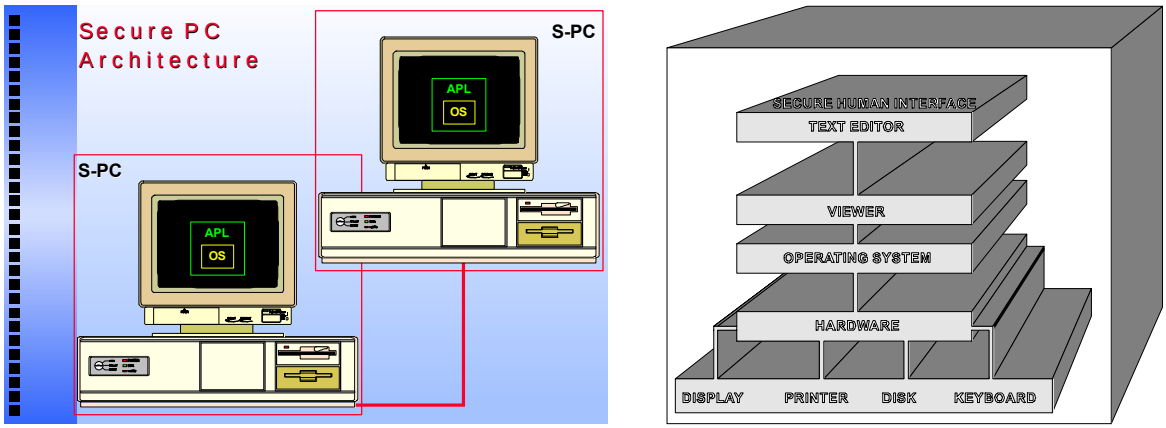



[Glossary: APL - Application Layer; OS - Operating System; SIGL - Signature Layer]

This PC architecture is characterised by activation of the signing process from an independent signing application on a computer with an independent, reliable operating system for the signing process. The reliability of the signing process is directly dependent on the reliability of the employed hardware utilities of the standard PC and on the reliability of any utilities of the standard applications and standard operating system functions which may be used. This architecture represents a possible embodiment of solution proposals 6.6.3.1 to 6.6.3.4.

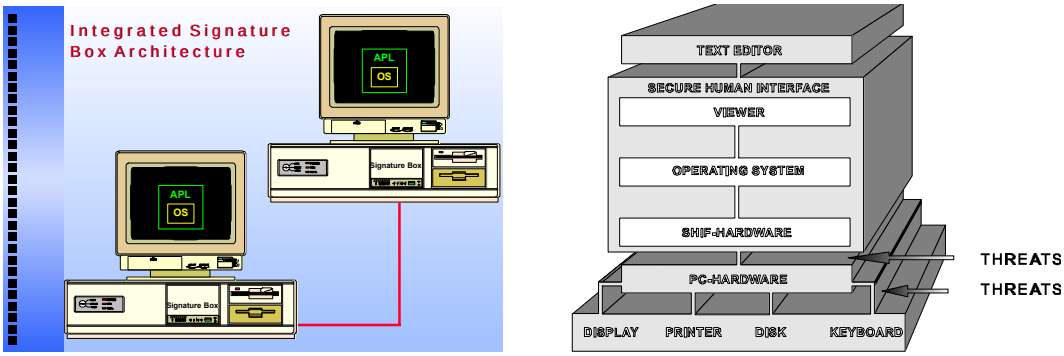
## A.3 Reliable signing computer




[Glossary: APL - Application Layer; OS - Operating System; S-PC - Secure PC]

This architecture is characterised by activation of the signing process on a reliable signing computer with a reliable signing application, reliable operating system and reliable hardware. No other applications can be activated on the signing computer at the same time as the signing process. This architecture represents a possible embodiment of solution proposals 6.6.3.5 and 6.6.3.6.

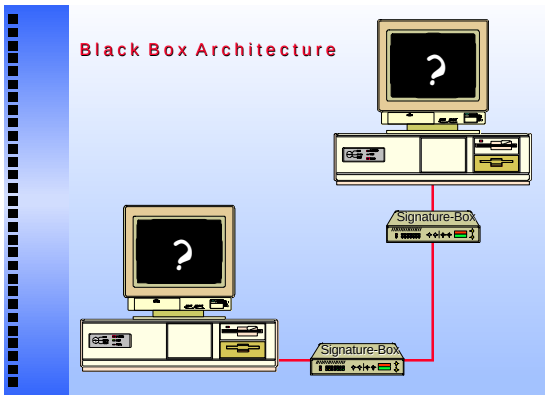
## A.4 PC with integrated signature hardware

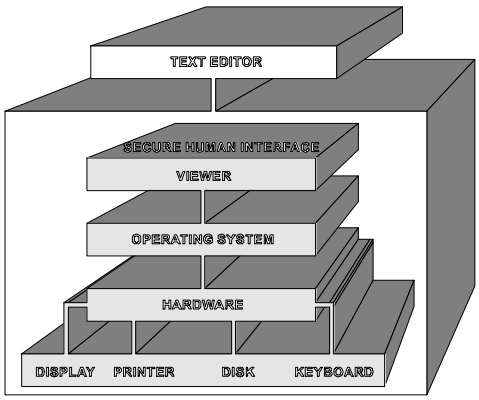



[Glossary: APL - Application Layer; OS - Operating System; SHIF - Secure Human Interface]

This architecture is characterised by activation of the signing process on an independent signature hardware device with a reliable signature application, reliable operating system and reliable hardware. The signature hardware is integrated in a standard computer. The peripheral devices of the standard computer, e.g. keyboard, mouse, monitor and printer, are used in the signing process. When the signing process is activated on the signature box, no applications other than the signing process can be activated on the standard computer. This architecture represents a possible embodiment of solution proposals 6.6.3.1 to 6.6.3.6.

## A.5 Independent signing device




This architecture is characterised by activation of the signing process on a specialised, independent signature hardware device with a reliable signature application, reliable operating system and reliable hardware. The signature hardware is completely self-contained and independent of the user's computer environment. No application other than the signing process can be activated on the signature hardware device. This architecture represents a possible embodiment of solution proposals 6.6.3.5 and 6.6.3.6.

## B. ITSEC functionality class F-C2

[Glossary: EVO = evaluated object:

An IT system or IT product which is subjected to evaluation.]

### Objective

B.11 The example classification F-C2 has been derived from the functionality requirements of US-TCSEC class C2. It provides finer user-definable access control access than class F-C1. It ensures the responsibility of the users for their actions by means of identification processes, the recording of security-related events and the separation of items of equipment.

### Identification and authentication

B.12 The EVO must unambiguously identify and authenticate users. This identification and authentication must be carried out prior to every other interaction of the EVO with the user. Further interactions must be possible only after successful identification and authentication. The authentication information must be stored in such a manner as to ensure that it may be accessed by authorised users only. The EVO must be able to establish the identify of the user in each case of interaction.

### Access control

B.13 The EVO must be capable of determining and administrating the access rights of each user to objects which are subject to the administration of rights. This is carried out on the basis of an individual user or a user's membership of a user group, or both. It must be possible to completely deny users or user groups access to an object. It must also be possible to restrict a user's access to an object to non-modifying operations. It must be possible to grant access rights to an object in an individual manner for each individual user. No person other than an authorised user must be able to grant or revoke rights pertaining to an object. The system for administering these rights must monitor the passing-on of access rights. Equally, the incorporation of new users and the deletion or blocking of users must also be possible by authorised users only.

B.14 In each instance of attempted access by users or user groups to objects which are subject to the administration of rights the EVO is to verify the legitimacy of the request. Unauthorised attempts to access objects must be rejected.

### Preservation of evidence

B.15 The EVO must incorporate a recording component which is capable of recording each of the following events together with the stated data:

a) Use of the identification and authentication mechanism:

Required data: Date; time; employed user ID; indication of the device on which the identification and authentication mechanism was used (e.g. terminal ID); success or failure of the attempt.

b) Attempted access to an object subject to the administration of rights: Required data: Date; time; user ID; name of the object; type of attempted access; success or failure of the attempt.

d) Actions by authorised users which are of relevance to the security of the EVO:

Required data: Date; time; user ID; type of action; name of the object to which the action related (such actions include the insertion or deletion (blocking) of users, for example; insertion or removal of data storage media; starting and stopping of the EVO).

B.16 Record information must be accessible only to users possessing the appurtenant authorisation. It must be possible to restrict the preservation of evidence to one or several users. Tools for evaluating and managing record data must be available and documented. These tools must enable selective identification of the actions of one or several users.

**Evaluation of records**

B.17 Tools to examine the record files for revision purposes must be available and documented. These tools must enable selective identification of the actions of one or several users.

**Reprocessing**

B.18 All data storage objects which are made available to the EVO must be processed prior to reuse by other users in such a manner as to as to eliminate the possibility of inference of their former contents.

## 6.7 Signature component

There is a choice of various technological facilities for implementation of the signature components required by the Digital Signature Act. According to the intended operational environment and application, IT solutions with different structural properties and functional attributes are required. Within the spectrum of solutions available at present, the 'security box' is at the top of the range and the 'chipcard' is at the bottom of the range, in terms of performance, scope of functions and price. Other designs of signature components which lie between these two extremes in terms of performance and price, and which will become available in the foreseeable future in the form of bus or interface cards (e.g. PC-CAT or PC-PCI) or in the form of PCMCIA (PC) cards, may also be taken into consideration.

### 6.7.1. Requirements stipulated in the Act and the Ordinance

#### 6.7.1.1 General stipulations

| Reference | Quotation | Interpretation |
|---|---|---|
| **§ 1 (1) SigG** | The purpose of this Act 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. | The purpose of the act results in the requirement for digital signatures and, subsequently, the components which are necessary in order to generate and verify a digital signature, to be configured in such a manner that they may be deemed to be 'secure' (the meaning of 'secure' within this legislation is set out in § 14 (1) SigG). The probative value of a digital signature is derived from this 'security'. This article also requires the technical process for digital signatures to be designed in such a manner that manipulations of the digital signatures and changes to the signed data can be ascertained 'reliably', that is, subject to the minimum possible residual risk.<br><br>Derived requirement: REC-SBOX 1.6. |

| | | |
|---|---|---|
| **Explanatory note on § 1 (1) SigG** | Manipulation includes every form of alteration, including alterations resulting from technical faults. | In practice, the causes of such alterations may be:<br>• manipulations to software and hardware,<br>• technical defects and inadequacies (material fatigue, ageing, etc.), resulting in the failure of a memory chip or a hardware mechanism, for example,<br>• maloperation and incorrect data input,<br>• force majeure, such as lightning or power failure,<br>• lack of system administration or inadequate system administration.<br>Derived requirement: REQ-SBOX 1.5. |
| **§ 2 (1) SigG** | For the purposes of this Act "digital signature" shall mean a seal affixed to digital data which is generated by a private signature key and establishes the holder 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 of this Act. | This is the definition of the digital signature as a 'seal', which establishes the identity of the signing party and the integrity of the digital data. The digital signature is employed to sign digital data. The article does not define how these data are to be interpreted..<br>Derived requirements: REQ-CHIP 2.1, REQ-CHIP 3.4, REQ-CHIP 7.1. |
| **Explanatory note on § 2 (1) SigG** | The technical process for digital signatures comprises<br>- a process for generating key pairs, each pair consisting of a private key and the appurtenant public key,<br>- a so-called hashing algorithm, i.e. a process to calculate a 'digital fingerprint' from digital data, whereby this 'fingerprint' has a specific fixed format and represents these data. The digital signature generally involves signing not of the digital data themselves, but of their 'digital fingerprint',<br>- a process to calculate the digital signature with the aid of a private signature, which is at the disposal of the party signing only,<br>- a process to verify the digital signature with the aid of a public key. | The technical process for digital signatures thus covers key generation, a hashing function and the process for calculating and verifying signatures. The hashing process in particular forms part of the technical process for digital signatures. |

| | | |
|---|---|---|
| **Explanatory note on § 2 (1) SigG** | [...] The digital signature process must be designed in such a manner as to ensure the authenticity and integrity of the signed data. In specific terms, this means:<br>- assignment of the key pairs to persons must be performed by a trustworthy institution (certification authority),<br>- the duplication (either by mistake or intentionally) of a key pair must be practically impossible<br>- a signature which is verifiable using the public key of a key pair can only have been generated using the private key; in particular, it must be practically impossible to calculate the private key from the public key, and<br>- it must be practically impossible to find different digital data with the same 'digital fingerprint' or digital data belonging to a stipulated 'digital fingerprint'. | The following alternatives are available for key generation:<br>a) in a secure component at the home or premises of the final user or<br>b) in a secure component at the certification authority.<br>The following technical variants are possible:<br>a) generation in a signature component or<br>b) generation at the certification authority and subsequent storage in a signature component.<br>If the signature component itself generates the key, it must be adequately ensured that no key pair is generated in duplicate. This means that the initialisation values of the key generators of all signature components must be different.<br>In order to ensure different starting values, supplementary parameters can be incorporated, e.g. via interaction with the user, or time parameters.<br>Derived requirement: REQ-SBOX 4.1. |
| **Explanatory note on § 2 (1) SigG** | [...] On the basis of the combination of safeguards stipulated by the legal provisions - personal identification, reliable key assignment via a certificate, establishment of a link between the private key and the person via possession (e.g. chipcard) and knowledge (e.g. PIN or password), secure technical components - the digital signature enables reliable ascertainment of the identity of the person who has generated the signature. | It is assumed below that the private key is stored within the signature component only.<br>When the user identifies himself to the signature component by means of knowledge, both knowledge and possession are required in order to generate a signature. When the signing component is a chipcard, knowledge is sufficient. Where appropriate, biometric methods may also be employed for the purpose of user authentication.<br>Derived requirements: REQ-SBOX 1.1, REC-SBOX 1.3, REQ-SBOX 1.3, REC-SBOX 6.2, REC-SBOX 1.4, and<br>REQ-CHIP 8.1. |

| | | |
|---|---|---|
| **Explanatory note on § 4 (5) SigG** | The certification authority may issue the 'root certificate' to the signature key holder concerned in authentic manner, together with his own certificate (storage on the data carrier with the signature key). | This constitutes a recommendation to load the certificates of the root authority and of the certification authority on the signature component when carrying out personalisation of the signature component.<br>Derived requirement: REC-SBOX 2.1, and<br>REC-CHIP 3.1. |
| **§ 5 (4) SigG** | The certification authority shall take measures to prevent undetected forgery or manipulation of the data intended for certificates.<br>It shall also take measures to ensure confidentiality of private signature keys. Storage of private signature keys by the certification authority shall not be permitted. | It must not be possible to read out the private key from the signature component.<br>Derived requirements: REQ-SBOX 1.3, REQ-SBOX 1.4, REQ-SBOX 4.2, REQ-SBOX 5.1, REQ-SBOX 7.1, and<br>REQ-CHIP 8.3, REQ-CHIP 10.1. |
| **Explanatory note on § 5 (4) SigG** | The requirement for confidentiality of the signature key as stipulated in Sentence 2 is absolute. No person (including the signature key holder) is to obtain a knowledge of the private signature key, as it will otherwise be impossible to exclude the possibility of misuse of the signature key with an adequate degree of certainty. The precautions to be taken by the certification authority are to preclude the disclosure or storage in the area of the certification authority (Sentence 3) by means of technical and organisational measures, when the keys are provided by the certification authority. When the keys are generated by the signature key holder himself, the certification authority is to verify that he uses a suitable process which adequately precludes the disclosure of a key (e.g. via a key generator on the chipcard which is to carry the key, such that the private key never leaves the chipcard). | This reinforces the stipulation that it must never be possible to read out private keys from the signature component by any means. This imposes security requirements on the hardware and on the operating system of the signature component.<br>Derived requirements: REQ-SBOX 1.3, REQ-SBOX 1.4, REQ-SBOX 4.2, REQ-SBOX 5.1, REQ-SBOX 7.1, and<br>REQ-CHIP 1.2. |

| | | |
|---|---|---|
| **Explanatory note on § 14 SigG** | This article stipulates the requirements imposed on the technical components. Further details are regulated by the supplementary Ordinance (cf. § 16 (6). Certification authorities are obliged to use suitable technical components (cf. § 5 (5) Sentence 2 and 3 and § 9). Signature key holders are informed of the requirement to use suitable technical components and of the possible technical components. With regard to the signature key and the appurtenant signing component (both may be located on a chipcard, for example), in accordance with § 5 (4) Sentence 2 the certification authority provides a guarantee that only suitable technical components are used, and refuses to issue a certificate when this is not the case. | The certification authority issues a certificate for the public key only after verifying the use of a tested and confirmed signing component (e.g. using check sums, serial numbers, etc.).<br><br>Derived requirements: REQ-SBOX 2.2, REC-SBOX 6.2, and<br><br>REQ-CHIP 3.1. |
| **§ 14 (1) SigG** | Technical components with safeguards are required for the generation and storage of signature keys and for the generation and verification of digital signatures which reliably reveal forged digital signatures and manipulated signed data and provide protection against unauthorised use of private signature keys. | In this connection signature components are required to be capable of reliably detecting forged signatures and must not be usable without authorisation. In particular, disclosure or unauthorised access to the private key must be prevented.<br><br>With regard to multifunctional chipcards in particular, this means that the signature application must be separate from other applications. In particular, other applications must have no access to the private key.<br><br>Derived requirements: REQ-SBOX 1.1, REC-SBOX 1.3, REC-SBOX 1.4, REQ-SBOX 1.3, REQ-SBOX 1.4, REC-SBOX 1.8, REQ-SBOX 4.2, REC-SBOX 4.1, REC-SBOX 5.1, REC-SBOX 5.2, REC-SBOX 6.1, and<br><br>REQ-CHIP 1.2, REQ-CHIP 3.3, REQ-CHIP 8.3, REQ-CHIP 8.4, REQ-CHIP 8.6, REQ-CHIP 10.1. |

| | | |
|---|---|---|
| **Explanatory note on § 14 (1) SigG** | Suitable technical components (hardware, software and mathematical methods) are required in order to ensure that a digital signature cannot be forged without detection and that signed data cannot be manipulated without detection. When suitable technical components are used to generate a digital signature and the private signature key and the identification data (personal identification number (PIN) or password) required to apply the private signature key are protected from unauthorised persons, the signed data are, with the utmost probability, secure against forgery and manipulation.<br><br>The provision in Sentence 1 requires each signature assigned by a certification authority to be unique. This can be ensured by mathematical/technical means. Key generating algorithms are available which are able to generate a virtually unlimited number of different signature keys, thus practically eliminating the possibility of two identical key pairs, even when billions of keys are assigned. | This specifies the cases and circumstances in which a digital signature is deemed to be secure:<br>• suitable technical component,<br>• protection of the private key and<br>• protection of the identification data from unauthorised persons.<br><br>If the signature component generates the keys itself, the uniqueness of the keys must be guaranteed with an adequate degree of certainty.<br><br>Derived requirements: REC-SBOX 1.4, REQ-SBOX 1.3, REQ-SBOX 1.4, REC-SBOX 5.1, REC-SBOX 5.2, REC-SBOX 6.1, and<br><br>REQ-CHIP 3.2. |
| **Explanatory note on § 14 (1) SigG** | The private (secret) signature key can be stored on a chipcard, for example, in such a manner as to ensure that it cannot be read out (at least not without extremely complex analytical processes which will destroy the card). Generation of the key pair on the card itself can be carried out in such a manner that the private key never leaves the card. If key generation is performed outside the card, technical and organisational (dual control principle) procedures can be implemented for loading the chipcard with the private key so as to reliably ensure the uniqueness and secrecy of the private signature key in this case too. | All signature components are to be subject to adequate requirements to protect the private signature key.<br><br>In the case of the chipcard, read-out of the private key must only be possible by means of extremely complex chip analyses, if at all.<br><br>Derived requirements: REQ-CHIP 1.1, REQ-CHIP 1.2, REQ-CHIP 2.1. |

| | | |
|---|---|---|
| Explanatory note on § 14 (1) SigG | The mathematical methods (hashing algorithms and signing algorithms) required for the signing process are the subject of an on-going course of discussion in the scientific sector worldwide. On the basis of current technological standards, they are assessed by the experts as 'unbreakable', subject to suitable dimensioning of the other parameters (e.g. length of the signature keys). Current technological standards also permit technical implementation and verification of the mathematical methods in a manner which adequately precludes errors of relevance to security or manipulations. The signature components in the form in which they are implemented on chipcards, for example, can thus be described as very secure. | The question as to what 'unbreakable' means in accordance with current technological standards should be specified in concrete terms and qualified in accordance with the duration of use of the signature component. |
| **Explanatory note on § 14 (1) SigG** | In order to preclude any improper use of signing components with the private signature key, reliable assignment of each signature key pair to a specific person is necessary (via a forgREC-Proof signature key certificate) and secure identification of the signature key holder via the signature component must be carried out prior to use of the signature key on the basis of possession (signature key) and knowledge (e.g. personal identification number (PIN)). | Security functions are to be implemented in the signature component which enable secure identification and authentication between the user and the signature component.<br><br>Vis á vis the chipcard, the user can only furnish proof of his identity on the basis of knowledge, as the object of possession is the chipcard itself to which he wishes to identify himself. Authentication to the chipcard on the basis of possession thus appears unrealistic.<br><br>In order to protect the security box against attempted manipulation and unauthorised access, authentication of the maintenance personnel would appear expedient here.<br><br>Derived requirements: REQ-SBOX 1.1, REC-SBOX 1.3, REC-SBOX 1.7, REC-SBOX 1.8, REQ-SBOX 5.1. |

| | | |
|---|---|---|
| **§ 4 (1) No. 1 SigV** | The data storage medium with the private signature key must be kept in the applicant's personal custody. If this data storage medium is lost, invalidation of the signature key certificate must be arranged without delay. If the data storage medium with the private signature key is no longer required, it must be rendered unusable and invalidation of the signature key certificate must be arranged, if the signature key certificate has not yet expired. | The loss of the signature component containing the private signature key must be apparent to the user.<br>This is difficult in the case of chipcards, as the loss of the chip must not necessarily involve loss of the chipcard.<br>In the course of informing the users, the certification authority must explain how a chipcard is rendered unusable.<br>Derived requirements: REC-SBOX 1.7, REQ-SBOX 2.1, REC-SBOX 4.1, REC-SBOX 5.1, and<br>REQ-CHIP 4.1, REQ-CHIP 5.1. |
| **§ 4 (1) No. 2 SigV** | Personal identification numbers or other data used for identification in conjunction with the data storage medium with the private signature key must be kept secret. If such identification data is disclosed, or if there are grounds to assume it has been disclosed, the data must be changed without delay. | Knowledge-based identification data must be alterable.<br>Derived requirements: REQ-SBOX 1.2, REC-SBOX 6.2, and<br>REQ-CHIP 8.2. |
| **§ 4 (1) No. 3 SigV** | For generation and verification of digital signatures, and for display of data that must be signed or of signed data that must be verified, technical components shall be used that fulfil the requirements of the Digital Signature Act and of this Ordinance and whose security pursuant to the Digital Signature Act and this Ordinance has been confirmed. Such components shall be protected from unauthorised access. | Signature components must be verified and the results of the verification must be confirmed.<br>No exceptions are permissible. |
| **§ 5 (1) SigV** | If the signature key holder generates signature keys, the certification authority shall reliably establish whether the signature key holder uses suitable technical components, pursuant to the Digital Signature Act and this Ordinance, for storage and use of the private key signature. | The functions of the signature component must support such verification measures by the certification authority.<br>This also applies in cases in which the signature component is not presented to the certification authority.<br>Derived requirements: REQ-SBOX 2.2, REC-SBOX 6.2, and<br>REQ-CHIP 3.1. |

| | | |
|---|---|---|
| **Explanatory note on § 5 (1) SigV** | In conjunction with the notification in accordance with § 4, this provision ensures a high level of consumer protection. In order to meet the requirements stipulated here, the certification authority must verify that the signature key holder uses a chipcard, for example, with a standard of security which has been tested and confirmed in accordance with § 17. To this end, the manufacturer may incorporate authentication in the chipcard. If the certification authority is unable to verify the security of the deployed technical components in an appropriate manner, issuance of the signature key certificate must be refused. | This is a requirement relating to the hardware security of the signature component. Read-out must be practically impossible. |
| **Explanatory note on § 5 (2) SigV** | This provision is intended to prevent the disclosure or storage of keys or identification data at the certification authority. If the possibility of disclosure cannot be fully excluded, any disclosures must be ascertainable at least. The checks stipulated in § 15 already provide for verification of the suitability of the technical components employed by a certification authority for generation of the keys. Storage of the private signature key outside of the provided key data storage medium is already precluded by the technical components (cf. § 16 subsection 1). | The user should always be able to alter his identification data. In particular, knowledge-based identification data should be altered prior to initial use.<br>Derived requirement: REC-SBOX 1.2, and<br>REC-CHIP 3.2. |
| **§ 16 (1) SigV** | The technical components required for generation of signature keys must function in such a manner that it is nearly certain that any given key can occur only once and that a private key cannot be derived from the relevant public key. The secrecy of private keys must be assured, and it must not be possible to duplicate keys. Security-relevant changes in technical components must be apparent for the user. | If the signature component generates the cryptographic keys itself, they must be unique with statistical certainty.<br>The need for it to be impossible to read out the private key imposes requirements on hardware security and the operating system.<br>Derived requirements: REQ-SBOX 4.1, REQ-SBOX 5.1, REC-SBOX 5.1, and<br>REQ-CHIP 1.2, REQ-CHIP 2.2, REQ-CHIP 8.5. |

| | | |
|---|---|---|
| **Explanatory note on § 16 (1) SigV** | The requirement for uniqueness of the key as stipulated in Sentence 1 can be fulfilled with available key generators.<br><br>The secrecy of the key as stipulated in Sentence 2 requires a technical component (e.g. chipcard or special component for mainframe applications) for key storage which cannot be read out (including read-out by the signature key holder himself) in accordance with current technological standards. The signature keys can be generated externally and transferred to the chipcards or, in future, generated on modern chipcards themselves. In view of the attendant security, generation of the keys on the key data storage medium itself should be standard in future. | This explanatory note substantiates the requirement for a hardware component and the use of a chipcard or special component which is identical to the security box considered here.<br><br>Derived requirements: REQ-SBOX 4.1, REQ-SBOX 4.2, REQ-SBOX 5.1, REQ-SBOX 7.1. |
| **Explanatory note on § 16 (1) Sentence 3 SigV** | A security-relevant change (in comparison to the evaluated and confirmed secure state) in accordance with Sentence 3 applies when the security of the component is no longer adequately ensured as a result of a technical change. Such a change may be detectable in the form of external destruction or a functional failure, for example. This is intended to protect the user of the technical components from security-relevant manipulations, which in this context may be aimed in particular at disclosing private signature key. | Security-relevant changes may be caused by:<br>• manipulations to software and hardware,<br>• technical defects and inadequacies (material fatigue, ageing, etc.), resulting in the failure of a memory chip or a hardware mechanism, for example,<br>• maloperation and incorrect data input,<br>• force majeure, such as lightning or power failure,<br>• lack of system administration or inadequate system administration.<br><br>Such changes would be apparent if the signature component were to become inoperable.<br><br>Derived requirements: REC-SBOX 6.1, and<br><br>REQ-CHIP 1.3. |

| | | |
|---|---|---|
| **§ 16 (2) SigV** | The technical components required for generation or verification of digital signatures must function in such a manner that the private signature key cannot be derived from the signature and the signature cannot be forged by any other means. Use of the private signature key must be possible only following identification of the holder and must require proper possession and knowledge; the key must not be disclosed during use. | This provision again requires it to be impossible to read out the private keys from the signature component and stipulates the required quality standard for key generation. Prior to calculation of the signature, the holder must authenticate himself to the signature component.<br><br>The holder can authenticate himself to the chipcard by means of knowledge only, and not by means of possession. Vis á vis the signing system (operational environment) the holder can additionally identify himself by means of possession, however, as he is required to insert the chipcard.<br><br>Derived requirements: REQ-SBOX 1.1, REC-SBOX 1.3, REC-SBOX 1.4, REQ-SBOX 3.1, REQ-SBOX 3.2, and<br><br>REQ-CHIP 7.1, REC-CHIP 8.1. |
| **§ 16 (2) Sentence 3ff SigV** | Biometrical characteristics may also be used for identification of the signature key holder. The technical components required for collecting identification data must function in such a manner that they do not reveal identification data and that the identification data is stored only on the data storage medium with the private signature key. Security-relevant changes in technical components must be apparent for the user. | Identification of the signature key holder can be effected via the user of biometric processes. Only the signature component is able to perform the comparison of the measured biometric characteristic with the characteristic stored in the signature component.<br><br>Derived requirements: REC-SBOX 1.1, REC-SBOX 5.1, REC-SBOX 6.1, and<br><br>REQ-CHIP 8.7.<br><br>As the chipcard is not able to render security-relevant changes directly apparent to the user, this requirement can be met, for example, by the refusal to execute functions on the part of the chipcard, or implicitly via appropriate responses by the background system.<br><br>Derived requirements: REQ-CHIP 1.3, REQ-CHIP 6.1, REQ-CHIP 7.2 |

| | | |
|---|---|---|
| **Explanatory note on § 16 (2) SigV** | The signing technology is generally implemented on a chipcard or a comparable data-carrier (e.g. PCMCIA card). Biometric characteristics (e.g. face, personal signature or finger structure) may be used in order to establish a link between card and owner beyond possession (card) and knowledge (PIN or password).<br><br>The technical components may be designed so as to require renewed input of the identification data, either prior to each digital signature or after the elapse of a certain period during which the signing technology is not used. The procedure to be adopted by the user remains at his discretion - with due regard to the specific application environment.<br><br>The identifiability of security-relevant changes required in Sentence 6 is intended to protect the user from changes of relevance to security, which in this context may in particular be aimed at disclosing the private signature key or the identification data. cf. also explanatory note on subsection 1. | Identification and authentication of the user of a signature component can also be effected by means of biometric characteristics. In this connection the requirement applies that the identification and authentication process must take place prior to each interaction with the user, and that subsequent interactions must be possible only after successful identification and authentication.<br><br>Otherwise, appropriate error messages must be output.<br><br>Derived requirements: REQ-SBOX 1.1, REC-SBOX 1.1, REC-SBOX 1.3, REC-SBOX 1.4, and<br><br>REQ-CHIP 8.7, REC-CHIP 8.1. |
| **§ 16 (3) Sentence 5 and 6 SigV** | If technical components pursuant to Sentences 1 to 4 are commercially provided to third parties for use, clear, reliable interpretation of the relevant data must be assured, and the technical components must automatically be checked for genuineness when used. Security-relevant changes in technical components must be apparent for the user. | The user's signature component must verify the genuineness of the component. This could be implemented via authentication of the component to the signature component which, in turn, transfers a password of which only the user has knowledge to the component only after successful authentication, whereupon the component displays this password.<br><br>Derived requirements: REQ-SBOX 1.6, and<br><br>REQ-CHIP 7.2. |

| | | |
|---|---|---|
| **§ 17 (4) SigV** | The competent authority shall publish, in the Federal Gazette, a list of agencies pursuant to § 14 (4) of the Digital Signature Act as well as a list of technical components that have received confirmation by such agencies pursuant to (3); the competent authority shall provide this list directly to the certification authorities. Note must be made, for all technical components, of the date until which the confirmation is valid.<br><br>If a certification is revoked or a confirmation declared invalid, notice of such actions shall also be published in the Federal Gazette and communicated directly to the certification authorities. | Derived requirement: REC-CHIP 1.1 |

#### 6.7.1.2 Supplementary requirements for chipcards

| Reference | Quotation | Interpretation |
|---|---|---|
| **§ 14 (2) Sentence 2 SigG** | Technical components with safeguards are required for the verification of signed data which allow the integrity of the signed data, the data to which the digital signature applies and the holder of the signature key to whom the digital signature belongs to be established. | Although the chipcard serves to verify signed data, it is unable to fulfil the requirements stipulated here, as it does not possess display facilities. These requirements must therefore be fulfilled by a different component, e.g. the operational environment. |

#### 6.7.1.3 Supplementary requirements for security boxes

| Reference | Quotation | Interpretation |
|---|---|---|
| **§ 9 SigG** | Upon request, the certification authority shall affix a time stamp to digital data.<br><br>§ 5 (5) sentences 1 and 2 shall apply mutatis mutandis. | When necessary, the time stamping service must be directly or indirectly available to the security box.<br><br>Derived requirements: REC-SBOX 1.9, REC-SBOX 8.1. |

| | | |
|---|---|---|
| **Explanatory note on § 9 SigG** | The allocation of time stamps (cf. § 2 subsection 4) is to be stipulated as an obligatory service for certification authorities, as [...]<br><br>A time stamp may be requested by anyone who [...].<br><br>In the case of signed data it is sufficient to obtain a time stamp for the digital signature, as this signature represents the entire signed data. | For the purposes of secure application of the time stamping service, it would be expedient for the security box to verify automatically whether the intended data have been provided with a time stamp. This will enable errors to be detected along the transmission route.<br><br>Derived requirement: REC-SBOX 1.8. |
| **§ 14 (2) Sentence 2 SigG** | Technical components with safeguards are required for the verification of signed data which allow the integrity of the signed data, the data to which the digital signature applies and the holder of the signature key to whom the digital signature belongs to be established. | Within the context of the overall system, the security box must possess a capability for disclosing verification results. This can be ensured via a display on the security box itself or via the secure operational environment.<br><br>Derived requirement: REC-SBOX 1.7. |
| **§ 4 (1) No. 5 SigV** | If a particular time can be of considerable significance with regard to use of signed data, a time stamp shall be appended. | When necessary, the time stamping service must be directly or indirectly available to the security box.<br><br>Derived requirements: REC-SBOX 1.9, REC-SBOX 8.1. |
| **§ 4 (1) No. 7 SigV** | In verification of digital signatures, it shall be determined whether the signature key certificate and attribute certificates were valid at the time the signature was generated, whether the signature key certificate contains restrictions pursuant to § 7 (1) No.7 of the Digital Signature Act and whether Numbers 4 and 5 were complied with, if applicable. | In accordance with this provision, the security box should be able to establish a direct or indirect link to the components 'directory service' and 'time stamping service'.<br><br>Derived requirement: REC-SBOX 8.1. |
| **Explanatory note on § 4 (1) No. 7 SigV** | Verification of the validity of certificates in accordance with Number 7 includes checking the digital signatures which belong to the certificates. It is left to the discretion of the person verifying the signature to decide whether the certificates should additionally be verified via the appropriate public directory of certificates (whether they are registered there and were valid at the time of generation of the signature). | The security box is able to verify the authenticity of the information from the directory service and to provide the result for further use and display.<br><br>Derived requirement: REC-SBOX 8.1. |

| | | |
|---|---|---|
| **Explanatory note on § 6 SigV** | The provision in sentence 1 is intended to ensure reliable handover of the private signature keys and identification data. Another possible form of handover, for example, would be formal service to the signature key holder in person, in accordance with the German Code of Civil Procedure, insofar as the prospective signature key holder requests this mode of handover and thus accepts any attendant risks. | These are organisational requirements pertaining to delivery of the security box to the user, for which appropriate arrangements must be made (e.g. secure delivery process).<br>Derived requirement: REC-SBOX 2.2. |
| **§ 16 (1) Sentence 3 SigV** | Security-relevant changes in technical components must be apparent for the user. | The purpose of this provision is to protect the security box itself against manipulation, and to ensure that any manipulations are subsequently discernible at least.<br>Changes of relevance to security can be rendered apparent via optical indication, appropriate error messages or the refusal to execute functions.<br>Derived requirements: REQ-SBOX 1.5, REC-SBOX 6.1. |

### 6.7.2. Generic security requirements and recommendations

The following generic security requirements and recommendations can be established from the Digital Signature Act and the appurtenant Ordinance. These generic security requirements serve as guidelines for general signature components. The security requirements for chipcards and signature boxes, to which reference has also been made in the cited legal provisions, will be considered separately at a later juncture. The safeguards have also been formulated initially for chipcards and signature boxes only.

#### 6.7.2.1 Security requirements and recommendations for the hardware of the signature component

REQ-SK 1.1 Read-out from the signature component of the authorised user's authentication data, that is, the data with which a user furnishes proof of his authorisation for the signing process, must not be possible without an unrealistic scope of tampering.
cf.: Explanatory note on § 14 (1) SigG

REQ-SK 1.2 The read-out of private signature keys from the signature component must not be possible without an unrealistic scope of tampering.
cf.: Explanatory note on § 5 (4) SigG, § 14 (1) SigG, Explanatory note on § 14 (1) SigG, § 16 (1) SigV

REQ-SK 1.3 The outward behaviour (e.g. emanation, power consumption, time response) of the signature component must be neutral. It must not be possible to infer any information regarding private keys, identification parameters or other confidential information from observation of this behaviour.
cf.: § 1 (1) SigG, § 5 (4) SigG, Explanatory note on § 5 (4) SigG

REC-SK 1.1 As the rapid pace of technological development involves a continual increase in the possibilities of attack and each successive generation is unable to offer protection against newly developed forms of attack, a signature component for the application 'Digital Signature' should not be more than 3 years old.
cf.: Explanatory note on § 7 (1) SigV, § 17 (4) SigV and limitation of the validity period for certificates to 5 years

#### 6.7.2.2 Security requirements and recommendations for key generation in the signature component

REQ-SK 2.1 The intentional generation of a duplicate key pair must not be possible. The form of implementation for the key generating process must guarantee with virtual certainty that no duplicate keys are generated. The starting value for each key generation process must be individual for each signature component and must be calculated internally. It must not be possible to read out data or states which are included in calculation of the starting value.
Note: Section 6.2 should also be considered in this connection. The starting value for the key generating process must not be dependent solely on an arbitrary input from outside.
cf.: Explanatory note on § 2 (1) SigG, Explanatory note on § 14 (1) SigG

REQ-SK 2.2 It must not be possible to calculate the private signature key from the public signature key.
Note: Section 6.2 should also be considered in this connection. When key generation is performed in the signature component, the quality requirements for key generation must be observed (e.g. primality test, selection of prime numbers of appropriate length).
cf.: § 16 (1) SigV

#### 6.7.2.3 Security requirements and recommendations for initialisation/personalisation

REQ-SK 3.1 It must be possible for the certification authority to verify that a signature component is suitable as such.
Note: To enable manufacturers to adapt their products accordingly, each certification authority should stipulate how it intends to establish whether a signature component is suitable as such.
cf.: Explanatory note on § 14 SigG, § 5 (1) SigV

REQ-SK 3.2 If the keys are generated outside of the signature component, the signature component must provide mechanisms which guarantee the secrecy of the private signature key during the personalisation process.
Note: The certification authority must ensure the uniqueness of the private signature key within its sphere of responsibility.
cf.: Explanatory note on § 14 (1) SigG

REQ-SK 3.3 The subsequent loading of software which would enable the read-out or alteration of authentication data, private or public signature keys is to be prevented.
cf.: § 14 (1) SigG

REQ-SK 3.4 The personalisation process should be carried out by trustworthy personnel in a secure personalisation environment.
Note: The requirements defined in Section 6.3 with regard to personalisation environment, personnel, organisation, personalisation systems, security during the transportation of personalisation data, control of rejected items, etc. are to be observed.
cf.: § 2 (1) SigG

REC-SK 3.1 The public key of the root and of the certification authority can be loaded into the signature component during the personalisation process. In addition, loading of the appurtenant certificates is also possible, where appropriate.
cf.: Explanatory note on § 4 (5) SigG

REC-SK 3.2 Should a PIN or a password be preset during the personalisation process, upon the signature component being used for the first time by its holder it should compel the signature component holder to alter this PIN or password.
Note: This enables the signature component holder to establish whether the signature component has been tampered with prior to handover.
cf.: Explanatory note on § 5 (1) SigV

REC-SK 3.3 Arrangements are to be made with regard to the reliable handover of the key parameters and authentication parameters and to ensure a secure delivery procedure for the security box.
cf.: Explanatory note on § 6 SigV

#### 6.7.2.4 Security requirements and recommendations regarding destruction of the signature component

REQ-SK 4.1 When a certificate expires or when the private signature key is no longer required, it is to be rendered unusable in a reliable manner.
Note: Rendering a key unusable may involve actively erasing the key, i.e. physically overwriting the key data, or destroying the signature component.
cf.: § 4 (1) Nr.1 SigV

#### 6.7.2.5 Security requirements and recommendations regarding identification / authentication

REQ-SK 5.1 Each user must identify and authenticate himself unambiguously to the signature component. This identification and authentication must take place prior to the signing process. The signing process itself must only be possible after successful identification and authentication. The authentication information must be stored in such a manner as to ensure that it cannot be read out and can be altered only by persons possessing the necessary authorisation.
Note: After 3 successive failed attempts, the signature function must be blocked.
Note: Authentication can be carried out by means of knowledge-based methods (PIN, password) and/or biometric methods. All methods must satisfy the requirements of standard 'E4, high'.
cf.: Explanatory note on § 2 (1) SigG, § 16 (2) SigV

REQ-SK 5.2 The alteration of authentication data must be possible by authorised users only. It must not be possible to deactivate the user authentication function.
cf.: Explanatory note on § 2 (1) SigG

REQ-SK 5.3 It must be possible for the authorised user to alter authentication data for knowledge-based methods. This does not apply to all types of biometric authentication data, however.
Note: It must be possible for the user to initiate the alteration of knowledge-based authentication data (PIN, password) at any time. In the course of informing the user as to how to use signature applications, the user must be notified of the risks relating to PINs and passwords and informed of how to select these in an appropriate manner.
cf.: § 4 (1) No. 2 SigV

REQ-SK 5.4 When biometric characteristics are employed to identify and authenticate authorised users, it must be ensured that the authentication data are stored in the signature component and are not disclosed.
cf.: § 16 (2) Sentence 3 ff. SigV, Explanatory note on § 16 (2) SigV

REQ-SK 5.5 When the signature component is employed in technical components which are offered for use to third parties on a commercial basis, the signature component must verify the genuineness of the component. It must furthermore establish whether any changes of relevance to security have taken place on the component. Genuineness or security-relevant changes must be rendered apparent to the user via an appropriate display.
cf.: § 16 (3) Sentence 3 SigV

#### 6.7.2.6 Security requirements and recommendations regarding access control

REQ-SK 6.1 The private signature key is stored exclusively and solely in a signature component, where it is subject to access control. Only the process which is in progress in the signature component in connection with signature generation is authorised to access the private signature key, for the purpose of signature generation.
cf.: § 2 (1) SigG, Explanatory note on § 2 (1) SigG, § 5 (4) SigG, Explanatory note on § 5 (4) SigG, § 14 (1) SigG, Explanatory note on § 14 (1) SigG

REQ-SK 6.2 Private signature keys must not be transmitted from the signature component. cf.: § 5 (4) SigG, § 14 (1) SigG

REQ-SK 6.3 The generation of digital signatures must be possible only after successful authentication of the authorised user.
cf.: § 14 (1) SigG

REQ-SK 6.4 The private signature key must not be duplicable.
cf.: § 16 (1) SigV

REQ-SK 6.5 With regard to signature components on which other applications also run, it must be ensured that these other applications do not obtain access to the authentication data and private signature key.
cf.: § 14 (1) SigG

REC-SK 6.1 The software employed in the generation and verification of signatures, stored certificates, public signature keys and all keys which require to be kept secret (e.g. transport keys) must be subject to access control, so as to ensure that only authorised persons or processes obtain access.
cf.: § 1 (1) SigG

REC-SK 6.2 Prior to using his private signature key, the signature component holder must authenticate himself. Authentication should take place directly prior to the execution of signing processes, so as to ensure that the signing process is carried out with the user's knowledge and consent. The signing process may involve the signing of several data records. The signature component should require explicit authentication prior to each signing process as a standard configuration. Each time other applications are initiated, renewed authentication shall be required for signing processes.
Note: If it is possible for the user to enable his signature component for several signing processes after successful authentication, in the course of the standard user notification he must be informed as to the risks of enabling his signature component in this manner and the appropriate number of signing processes to be enabled. The terminal should require renewed authentication when a prolonged period elapses without any inputs or outputs at the terminal.
cf.: § 16 (2) SigV

#### 6.7.2.7 Security requirements and recommendations regarding the preservation of evidence and the evaluation of records

REC-SK 7.1 Information on security problems (e.g. repeated input of incorrect PIN) should be stored in the signature component.
Note: To enable the detection of improper use which is of relevance to security, only authorised users should be entitled to view the data which are stored for the purpose of the preservation of evidence. Further details of the system for the preservation of evidence can be determined by the market.

REC-SK 7.2 Actions which are of relevance to and critical to security, such as the most recent signing processes, should be stored in the signature component. To this end information on the signing processes, such as date, terminal indicator, hashing value and file name of the signed document, should be stored. Other actions of relevance to security include maintenance work, attempted manipulations and identified error states. It should be possible for the users to read the record data. The record data should be protected against unauthorised alteration.

#### 6.7.2.8 Security requirements and recommendations regarding reprocessing

REQ-SK 8.1 In the case of multifunctional signature components it must be ensured that memory areas which have been used by the signature application are erased prior to further use by other applications.
cf.: § 5 (4) SigG, § 14 (1) SigG

#### 6.7.2.9 Security requirements and recommendations regarding integrity

REQ-SK 9.1 Changes to the signature component which are of relevance to security must be apparent to the user.
cf.: § 16 (1) Sentence 3 SigV, Explanatory note on § 16 (1) Sentence 3 SigV

#### 6.7.2.10 Security requirements and recommendations regarding secure data transmission

REC-SK 10.1 Data transmission between security box and the area of application should be secured against manipulation and malfunctions.
cf.: § 2 (1) SigG, Explanatory note on § 9 SigG, § 14 (1) SigG, Explanatory note on § 14 (1) SigG

#### 6.7.2.11 Security requirements and recommendations relating to the administrative environment

REQ-SK 11.1 The loss of the signature component must be apparent to the user of the signature component.
cf.: § 4 (1) No. 1 SigV

REQ-SK 11.2 The signature component must provide the certification authority with the ability to verify that the component represents a suitable component with regard to key generation and personal identification/authentication.

cf.: § 5 (1) SigV

REC-SK 11.1 The root certificate can be loaded into the signature component together with the user certificate in the course of the personalisation process.
cf.: Explanatory note on § 4 (5) SigG

REC-SK 11.2 Arrangements are to be installed regarding the reliable handover of key parameters and authentication parameters and a secure delivery procedure for the signature component.
cf.: Explanatory note on § 6 SigV

### 6.7.3. Threats

The following enumeration does not draw a strict distinction between threats as defined in ITSEC and any vulnerabilities which may be exploitable as a result of implementation. Equally, the enumeration is certainly not to be regarded as complete or final.

#### 6.7.3.1 General threats

1. Unauthorised use of the signature component.
   Safeguards: S-CHIP 7.1, S-CHIP 7.3, S-SBOX 1.1, S-SBOX 1.6
2. Use of a trivial password or a PIN of inadequate length.
   Safeguards: S-CHIP 7.1, organisational safeguards
3. Lack of expiry date for passwords or PINs.
   Safeguards: S-SBOX 1.3
4. Unauthorised access to authentication information.
   Safeguards: S-CHIP 7.3, S-SBOX 1.2, S-SBOX 1.8
5. Generation of cryptographically weak signature keys.
   Safeguards: S-SBOX 3.1, S-SBOX 4.1, S-SBOX 4.2
6. Duplication of signature keys.
   Safeguards: S-SBOX 3.1, S-SBOX 4.1, S-SBOX 4.2
7. Private signature key is calculable.
   Safeguards: S-SBOX 3.1
8. Implemented hashing function or implemented signing algorithm are compromised.
   Safeguards: S-SBOX 3.1
9. Read-out of the private signature key.
   Safeguards: S-CHIP 1.1 to S-CHIP 1.17, S-SBOX 2.3, S-SBOX 4.3
10. Ascertainment and passing-on of the private signature key.
    Safeguards: S-CHIP 1.1 to S-CHIP 1.17, S-CHIP 7.3, S-CHIP 7.4, S-SBOX 1.9, S-SBOX 1.12, S-SBOX 2.3, S-SBOX 4.3, S-SBOX 4.4, S-SBOX 4.5, S-SBOX 5.2
11. Incorrect calculation or forwarding of a signature.
    Safeguards: S-SBOX 1.18, S-SBOX 1.25, S-SBOX 1.26, S-SBOX 3.2, S-SBOX 4.4
12. Incorrect result of a signature verification process, or display of an incorrect result.
    Safeguards: S-SBOX 1.24, S-SBOX 1.25, S-SBOX 1.26, S-SBOX 3.2
13. Changes to user certificates.
    Safeguards: S-SBOX 1.10
14. Inappropriate disposal of rejected signature components (thus enabling attempted read-outs).
    Safeguards: S-CHIP 5.1, S-SBOX 1.13
15. Non-secure transmission of sensitive data.
    Safeguards: S-SBOX 1.19, S-SBOX 1.21
16. Unauthorised subsequent loading of supplementary software (e.g. software which enables the read-out of keys).
    Safeguards: S-CHIP 3.1, S-SBOX 1.22
17. Subsequent loading of unapproved software.
    Safeguards: S-CHIP 3.1, organisational safeguards.

18. Incomplete records.
    Safeguards: --
19. Failure of the recording function for events of relevance to security.
    Safeguards: S-SBOX 1.26
20. Changes to records.
    Safeguards: S-CHIP 7.5, S-SBOX 1.15, S-SBOX 1.16
21. Manipulations on components of relevance to security (e.g. analysis via current tapping, attacks via altered operating parameters, attacks by measuring internal signals or attacks via structural analyses).
    Safeguards: S-CHIP 1.1 to S-CHIP 1.16, S-SBOX 1.10, S-SBOX 1.11, S-SBOX 1.23, S-SBOX 5.1
22. Duplication of the signature component.
    Safeguards: S-CHIP 1.1 to S-CHIP 1.3, S-CHIP 1.12
23. Deduction of sensitive information from electromagnetic emanation.
    Safeguards: S-SBOX 1.9, S-SBOX 7.1
24. Unauthorised or unintentional generation of a signature.
    Safeguards: S-CHIP 3.1, S-CHIP 6.1, S-CHIP 7.1 to S-CHIP 7.3, S-CHIP 7.6, S-CHIP 7.7, S-SBOX 1.4, S-SBOX 1.5, S-SBOX 1.8
25. Undetected memory errors.
    Safeguards: S-CHIP 6.1
26. Theft or substitution of the signature component.
    Safeguards: S-CHIP 4.2 to S-CHIP 4.4, S-CHIP 4.6, S-CHIP 6.1

#### 6.7.3.2 Additional threats for chipcards

27. Damage from external environmental influences.
    Safeguards: S-CHIP 4.1
28. Mistaken use of the wrong chipcard.
    Safeguards: S-CHIP 4.2 to S-CHIP 4.4

#### 6.7.3.3 Additional threats for security boxes

29. No display or incorrect display of the security status.
    Safeguards: S-SBOX 1.19, S-SBOX 1.21
30. Manipulation of the system time.
    Safeguards: S-SBOX 1.17
31. Connection of the security box to a public network.
    Safeguards: S-SBOX 1.17
32. Read-in of forged inquiry results (e.g. directory, time or validity inquiries).
    Safeguards: --
33. Impeding of inquiries relating to certificates.
    Safeguards: --

### 6.7.4. Chipcards as signing components

Signing components may take the form of chipcards. The advantage of chipcards over all other possible signature components is that their capacity and compact design enable them to provide personal information and secret data in a secure and mobile manner. The information stored on the chipcard includes the user's private signature key, his certificate and the public key of the certification authority. The user must authenticate himself successfully, prior to accessing the 'Digital Signature' application.

#### 6.7.4.1. Generic security requirements and recommendations

The security requirements and recommendations described below can be established for the chipcard employed as the signing component on the basis of the Digital Signature Act and the appurtenant Ordinance.

REC-CHIP 0.1 In order to guarantee the uniformity and interoperability of all signature components and terminals, the 'interface to chipcards with digital signature application/function in accordance with SigG and SigV, draft for DIN standard, DIN NI-17.4' is to be used in the implementation of these components and terminals.
cf.: § 16 (2) and (3) SigV
Safeguards pertaining to this recommendation: S-CHIP 7.7

##### 6.7.4.1.1 Security requirements and recommendations regarding the hardware of the chip

REQ-CHIP 1.1 Read-out from the chipcard of the authorised user's authentication data, that is, the data with which a user furnishes proof of his authorisation for the signing process, must not be possible without an unrealistic scope of tampering.
cf.: Explanatory note on § 14 (1) SigG
Safeguards pertaining to this requirement: see S-CHIP 1.1, S-CHIP 1.2, S-CHIP 1.3, S-CHIP 1.4, S-CHIP 1.5, S-CHIP 1.6, S-CHIP 1.7, S-CHIP 1.8, S-CHIP 1.9, S-CHIP 1.10, S-CHIP 1.11, S-CHIP 1.14, S-CHIP 1.15, S-CHIP 1.16

REQ-CHIP 1.2 The read-out of private signature keys from the chipcard must not be possible without an unrealistic scope of tampering. (Note: In particular, so-called bellcore attacks must not be possible).
cf.: Explanatory note on § 5 (4) SigG, § 14 (1) SigG, Explanatory note on § 14 (1) SigG, § 16 (1) SigV
Safeguards pertaining to this requirement: S-CHIP 1.1, S-CHIP 1.2, S-CHIP 1.3, S-CHIP 1.4, S-CHIP 1.5, S-CHIP 1.7, S-CHIP 1.8, S-CHIP 1.9, S-CHIP 1.10, S-CHIP 1.11, S-CHIP 1.14, S-CHIP 1.15, S-CHIP 1.16

REQ-CHIP 1.3 Changes to the chip hardware which are of relevance to security must be apparent to the user.
As the chipcard is not able to render security-relevant changes directly apparent to the user, this requirement can be met, for example, by the refusal to execute functions on the part of the chipcard, or implicitly via appropriate responses by the background system.
cf.: § 16 (1) Sentence 3 SigV, § 16 (2) Sentence 3 ff SigV
Safeguards pertaining to this requirement: S-CHIP 1.10, S-CHIP 1.14, S-CHIP 1.15, S-CHIP 1.16, S-CHIP 6.1

REC-CHIP 1.1 As the rapid pace of technological development in the area of chipcards involves a continual increase in the possibilities of attack and each successive generation is unable to offer protection against newly developed forms of attack, a chipcard for the application 'Digital Signature' should not be more than 3 years old
cf.: § 17 (4) SigV and limitation of the validity period for certificates to 5 years
Safeguards pertaining to this recommendation: S-CHIP 1.17

#### 6.7.4.1.2 Security requirements and recommendations regarding key generation in the chipcard

REQ-CHIP 2.1 The intentional generation of a duplicate key pair must not be possible. The form of implementation for the key generating process must guarantee with virtual certainty that no duplicate keys are generated. The starting value for each key generating process must be different for each individual chipcard, and must be calculated internally in the chipcard. It must not be possible to read out data or chipcard statuses which are included in calculation of the starting value.
Section 6.2 should also be noted in this connection.
Note: The starting value for the key generating process must not be dependent solely on an arbitrary input from outside.
cf.: Explanatory note on § 2 (1) SigG, Explanatory note on § 14 (1) SigG
Safeguards pertaining to this requirement: S-CHIP 2.1

REQ-CHIP 2.2 It must not be possible to calculate the private signature key from the public signature key.
Section 6.1 should also be considered in this connection.
Note: When key generation is performed in the chipcard, the quality requirements for key generation must be observed (e.g. primality test, selection of prime numbers of appropriate length).
cf.: § 16 (1) SigV
Safeguards pertaining to this requirement: S-CHIP 2.1

#### 6.7.4.1.3 Security requirements and recommendations relating to initialisation/personalisation

REQ-CHIP 3.1 It must be possible for the certification authority to verify that a chipcard is suitable as a signature component.
Note: To enable manufacturers to adapt their products accordingly, each certification authority should stipulate how it intends to establish whether a chipcard is suitable as a signature component.
In particular, it should be verified whether the requirement for the 'interface to chipcards with digital signature application/function in accordance with SigG and SigV, draft for DIN standard, DIN NI-17.4' has been complied with.
cf.: Explanatory note on § 14 SigG, § 5 (1) SigV
Safeguards pertaining to this requirement: see Section 6.3

REQ-CHIP 3.2 If the keys are generated outside of the chipcard, the chipcard must provide mechanisms which guarantee the secrecy of the private signature key during the personalisation process.
Note: The certification authority must ensure the uniqueness of the private signature key within its sphere of responsibility.
cf.: Explanatory note on § 14 (1) SigG
Safeguards pertaining to this requirement: see Section 6.3

REQ-CHIP 3.3 The subsequent loading of software which would enable the read-out or alteration of authentication data, private or public signature keys is to be prevented.
cf.: § 14 (1) SigG
Safeguards pertaining to this requirement: S-CHIP 3.1

REQ-CHIP 3.4 The personalisation process should be carried out by trustworthy personnel in a secure personalisation environment.
Note: The requirements defined in Section 6.3 with regard to personalisation environment, personnel, organisation, personalisation systems, security during the transportation of personalisation data, control of rejected items, etc. are to be observed.
cf.: § 2 (1) SigG
Safeguards pertaining to this requirement: see Section 6.3

REC-CHIP 3.1 The public key of the root and of the certification authority can be loaded into the chipcard during the personalisation process. In addition, loading of the appurtenant certificates is also possible, where appropriate.
cf.: Explanatory note on § 4 (5) SigG
Safeguards pertaining to this recommendation: see Section 6.3

REC-CHIP 3.2 Should a PIN or a password be preset during the personalisation process, upon the chipcard being used for the first time by its holder it should compel the chipcard holder to alter this PIN or password. When the chipcard incorporates a signature counter, the customer can be recommended to check whether the signature counter is set to zero when he uses it for the first time.
Note: This enables the chipcard holder to establish whether the chipcard has been tampered with prior to handover.
cf.: Explanatory note on § 4 (5) SigG
Safeguards pertaining to this recommendation: see Section 6.3

#### 6.7.4.1.4 Security requirements and recommendations relating to the physical body of the chipcard

REQ-CHIP 4.1 The loss of a private signature key must be apparent to the authorised user, even if only the chip is removed from the chipcard in an unauthorised manner. Furthermore, 'duping' the chipcard holder with a duplicate of the chipcard of the same appearance should not be possible without extensive forgery measures.
cf.: § 4 (1) Nr.1 SigV
Safeguards pertaining to this requirement: S-CHIP 4.1, S-CHIP 4.2, S-CHIP 4.3, S-CHIP 4.4, S-CHIP 4.5, S-CHIP 4.6

#### 6.7.4.1.5 Security requirements and recommendations relating to destruction of the chipcard

REQ-CHIP 5.1 When a certificate expires or when the private signature key is no longer required, it is to be rendered unusable in a reliable manner.
Note: Rendering a key unusable may involve actively erasing the key, i.e. physically overwriting the key data, or destroying the chip.
cf.: § 4 (1) No. 1 SigV
Safeguards pertaining to this requirement: S-CHIP 5.1

#### 6.7.4.1.6 Security requirements and recommendations relating to violations of the security policy

REQ-CHIP 6.1 Changes to software or data which are of relevance to security must be apparent to the user.
cf.: § 16 (2) Sentence 3 ff SigV
Safeguards pertaining to this requirement: S-CHIP 6.1

#### 6.7.4.1.7 Security requirements and recommendations relating to identification/authentication

REQ-CHIP 7.1 Each user must identify and authenticate himself unambiguously to the chipcard. This identification and authentication must take place prior to the signing process. The signing process itself must only be possible after successful identification and authentication. The authentication information must be stored in such a manner as to ensure that it cannot be read out.
Note: After 3 successive failed attempts, the signature function must be blocked.
Note: Authentication can be carried out by means of knowledge-based methods (PIN, password) and/or biometric methods. All methods must satisfy the requirements of standard 'E4, high'.
cf.: Explanatory note on § 2 (1) SigG, § 16 (2) SigV
Safeguards pertaining to this requirement: S-CHIP 7.1

REQ-CHIP 7.2 When the chipcard is employed in technical components which are offered for use to third parties on a commercial basis, the chipcard must verify the genuineness of the component. It must furthermore establish whether any changes of relevance to security have taken place on the component. Genuineness or security-relevant changes must be rendered apparent to the user via an appropriate display.
cf.: § 16 (2) Sentence 3 ff SigV, § 16 (3) Sentence 3 SigV
Safeguards pertaining to this requirement: S-CHIP 7.2

#### 6.7.4.1.8 Security requirements and recommendations relating to access control

REQ-CHIP 8.1 Alteration of authentication data must be possible by authorised users only. It must not be possible to deactivate the user authentication function.
cf.: Explanatory note on § 2 (1) SigG
Safeguards pertaining to this requirement: S-CHIP 7.3

REQ-CHIP 8.2 It must be possible for the authorised user to alter authentication data for knowledge-based methods. This does not apply to all types of biometric authentication data, however.
Note: It must be possible for the user to initiate the alteration of knowledge-based authentication data (PIN, password) at any time. In the course of informing the user as to how to use signature applications, the user must be notified of the risks relating to PINs and passwords and informed of how to select these in an appropriate manner.
cf.: § 4 (1) No. 2 SigV
Safeguards pertaining to this requirement: S-CHIP 7.1

REQ-CHIP 8.3 Private signature keys must not be transmitted from the chipcard.
cf.: § 5 (4) SigG, § 14 (1) SigG
Safeguards pertaining to this requirement: S-CHIP 7.3

REQ-CHIP 8.4 The generation of digital signatures must be possible only after successful authentication of the authorised user.
cf.: § 14 (1) SigG
Safeguards pertaining to this requirement: S-CHIP 7.1, S-CHIP 7.3

REQ-CHIP 8.5 The private signature key must not be duplicable.
cf.: § 16 (1) SigV
Safeguards pertaining to this requirement: S-CHIP 7.3

REQ-CHIP 8.6 In the case of multifunctional chipcards it must be ensured that other applications have no access to the authentication data and the private signature key.
cf.: § 14 (1) SigG
Safeguards pertaining to this requirement: S-CHIP 7.3

REQ-CHIP 8.7 When biometric characteristics are employed to identify and authenticate authorised users, it must be ensured that the authentication data are stored in the chipcard and are not disclosed.
cf.: § 16 (2) Sentence 3 ff SigV, Explanatory note on § 16 (2) SigV
Safeguards pertaining to this requirement: S-CHIP 7.1, S-CHIP 7.3

REC-CHIP 8.1 Prior to using his private signature key, the chipcard holder must authenticate himself. Authentication should take place directly prior to the execution of signing processes, so as to ensure that the signing process is carried out with the user's knowledge and consent. The chipcard may be enabled for a stipulated number of signing processes or for a set period of time. The chipcard should require explicit authentication prior to each signing process as a standard configuration. Each time other applications are initiated, renewed authentication shall be required for signing processes.
Note: If it is possible for the user to enable his chipcard for several signing processes after successful authentication, in the course of the standard user notification he must be informed as to the risks of enabling his chipcard in this manner and the appropriate number of signing processes to be enabled. The terminal should require renewed authentication when a prolonged period elapses without any inputs or outputs at the terminal.
cf.: § 16 (2) SigV, Explanatory note on § 16 (2) SigV
Safeguards pertaining to this recommendation: S-CHIP 7.6

#### 6.7.4.1.9 Security requirements and recommendations regarding the preservation of evidence and the evaluation of records

REC-CHIP 9.1 Information on security problems (e.g. repeated input of incorrect PIN) should be stored in the chipcard.
Note: To enable the detection of improper use of relevance to security, only authorised users should be entitled to view the data which are stored for the purpose of the preservation of evidence. Further details of the system for the preservation of evidence can be determined by the market.
Safeguards pertaining to this recommendation: S-CHIP 6.1, S-CHIP 7.1, S-CHIP 7.5

REC-CHIP 9.2 The actions relating to the most recent signing processes should be stored in the chipcard. To this end information on the signing processes, such as date, terminal indicator, hashing value and file name of the signed document, should be stored. It should be possible for the users to read the record data. The record data should be protected against unauthorised alteration. Safeguards pertaining to this recommendation: S-CHIP 7.5

#### 6.7.4.1.10 Security requirements and recommendations regarding reprocessing

REQ-CHIP 10.1 In the case of multifunctional chipcards it must be ensured that memory areas which have been used by the signature application are erased prior to further use by other applications.
cf.: § 5 (4) SigG, § 14 (1) SigG
Safeguards pertaining to this requirement: S-CHIP 7.4

### 6.7.4.2 Proposed solutions

In order to fulfil the above-stated security requirements, various solutions may be considered when chipcards are employed as signature components:

1. One solution is a monoapplicative chipcard which supports the application 'Digital Signature' only.
2. A second solution is a multiapplicative chipcard which permits other applications in addition to the application 'Digital Signature'.
3. A third solution is a mono- or multiapplicative chipcard on which the function 'Digital Signature' is combined with other application functions (e.g. on a medical insurance card).

The first solution is simpler to implement than the other solutions in terms of security, as multiapplicative chipcards impose special requirements on the chipcard's operating system and safeguards for the subsequent loading of applications.

Not all chipcards which are available today are able to hash the complete scope of data to be signed internally. Different variants are thus possible with regard to the hashing process:

- Chipcards without a hash function: in this case, the complete scope of hash functions is performed by the operational environment and the hashed value is transmitted to the chipcard for signing or verification.
- Chipcards with a hash function: the complete hashing process can be performed internally in the chipcard. However, according to the volumes of data to be hashed and the chipcard's performance capabilities, it is also possible for the operational environment to perform the hashing process apart from the final round, and for the intermediate result and the final data block to be transmitted to the chipcard, which then performs the final hashing prior to the signing process internally.

#### 6.7.4.3. Safeguards

##### 6.7.4.3.1. Safeguards regarding chipcard hardware

**S-CHIP 1.1 Use of special controllers**

When a special chip which is not otherwise available in this form is developed for an application, no attacker will be able to draw comparisons with other applications. When standard components are used there is always a risk that an attacker may be able to gain information by analysing other systems which employ identical chips. When unpublished internal processes are employed in the chip, an attacker will find it difficult to analyse programme data. This requires the production of a processor designed especially for the task concerned or modification of an existing processor. Due to cost constraints, this will only be possible in the smallest number of applications.

**S-CHIP 1.2 Restricted access to testing and development equipment for chips**

If the manufacturer adopts a highly restrictive policy with regard to the distribution of testing and development equipment for the employed chips, a 'normal' attacker will find it more difficult to investigate the employed chips by means of individual test software which he produces himself. This will make it more difficult to identify chip structures and to locate memory locations in which specific content items are stored.

**S-CHIP 1.3 Non-publication of the mask layout**

Once an attacker has managed to expose the chip surface, it is easy for him to carry out a visual comparison of the chip surface with published mask layouts, in order to identify the employed chip type or controller. The attacker's work will be made more difficult if the manufacturer refrains from publishing the mask layout (e.g. in advertising brochures).

**S-CHIP 1.4 Deactivation of test functions via blowing of the test fuse**

To enable functional testing of the chipcards after manufacture, the microcontrollers are provided with special test modes. These permit access to all memory areas for test purposes. After completing the test phase for the chips, the test mode is to be irreversibly deactivated. A deactivation mechanism can be implemented in the form of polysilicon fuses, for example. It is to be noted that the security safeguards in this area should not be based on fuses alone. When such polysilicon fuses are used, they should not be simple to recognise when the chip is opened.

**S-CHIP 1.5 Deactivation of test functions by setting logical flags**

A specific value which prevents subsequent activation of the test phase is written in a non-erasable part of the non-volatile memory after the test phase. This safeguard is particularly effective in combination with S-CHIP 1.4.

**S-CHIP 1.6 Incorporation of dummy structures into the chip layout**

Structures are installed on the chip mask which are similar in appearance to a known structure (sensor, memory locations, computing register, etc.) but which have no relevance to the chip's mode of functioning. Should an attacker manage to expose the chip surface, the dummy structure will hinder his analysis of the chip structure.

**S-CHIP 1.7 Encapsulation of the chip in a special housing**

The chip is encapsulated in a hard, opaque material which is structured in such a manner as to destroy the chip, should it be removed.

### S-CHIP 1.8 Scrambling of the chip's internal bus

The internal bus of the chip is installed in scrambled form, that is, the conductors run over the chip surface in a disorderly manner. This makes it more difficult to locate, contact and read out bus data. It should be noted, however, that this scrambling process is only static in nature and only extends the time required to carry out an analysis. The aim is to render read-out and interpretation of the data more difficult. In addition to scrambling the chip's internal bus, other methods which pursue the same objective are also conceivable.

### S-CHIP 1.9 Ensurance of uniform current input

The aim is to prevent analysis of the code 'from outside'. To this end, it must not be possible to deduce current commands from the current input. This is attainable by either of the following alternatives:

- the process guarantees virtually the same current input for all machine commands, or
- different current profiles occur at all times, even during processing of the same command sequences.

### S-CHIP 1.10 Application of protective films over the chip

Important chip components are protected against attacks from outside by means of a suitable covering in the top layer. Metal plating or a special security structure can be applied over the chip, for example. This prevents the measurement of charge potentials and contacting with the aid of a microprobing station. An additional monitoring function for the metal plating can be implemented to initiate functional failure of the chip in the event of the metal plating being removed.

### S-CHIP 1.11 ROM structure

The physical body of the ROM must ensure that analysis of the ROM's contents is not possible simply via optical analysis of the chip surface. This means that a 'metal- or contact-hole ROM' is not suitable for use, for example. An ion-implanted ROM would be more suitable. These cannot be read out by analysing the chip structure, as the ROM bits differ only in terms of the doping patterns.

### S-CHIP 1.12 Consecutive serial numbering for the chip

A unique serial number, which cannot be erased or altered, is installed for each chip in a special area of the EEPROM. Logical use can be made of this number to render the generation of duplicates more difficult.

### S-CHIP 1.13 Integration of a passivation layer sensor

The passivation layer of the chip, which protects the chip against external influences, can additionally be connected to a sensor which actively tests whether this layer is still in place by measuring resistance or capacitance. If the layer is no longer in place, the chip will be deactivated. This prevents manipulations and dynamic analyses of the chip, for the purposes of which the passivation layer would have to be removed beforehand.

### S-CHIP 1.14 Integration of a Power On detector

The Power On detector ensures that the chip is always in a defined initial state when switched on, irrespective of the Reset signal. This prevents the chip from starting up in an undefined

state after being switched on, in which manipulations or attempted read-outs could be carried out.

**S-CHIP 1.15 Integration of a voltage monitor**

The voltage monitor effects defined deactivation of the chip when an upper or lower limit is violated. This ensures that the processor can only be operated in a controlled manner within a voltage range in which its performance characteristics are stable.

**S-CHIP 1.16 Integration of a frequency monitor**

The frequency monitor ensures that the chip operates only when the externally applied frequency is above a minimum limit and, where applicable, below a maximum limit. This prevents analysis in single-step mode.

**S-CHIP 1.17 Limitation of validity**

As the rapid pace of technological development in the area of chipcards involves a continual increase in the possibilities of attack and each successive generation is unable to offer protection against newly developed forms of attack, the period of validity for chipcards employed for the application 'Digital Signature' should be limited to 3 years.

#### 6.7.4.3.2. Safeguards regarding key generation in the chipcard

**S-CHIP 2.1 Secure key generation in chipcards**

When key pairs for digital signatures are generated by a chipcard, it must be ensured that suitable and approved processes are employed for the purpose of key generation. These processes must guarantee that only suitable keys are generated, thus ensuring that the private key cannot be calculated from the public key.

The key generating process generally requires a random number generator. When such a generator is not available as a reliable and suitable physical noise source, a suitable mathematical pseudo-random number generator or a pseudo-random generator employing biometric characteristics can be used. In the first case, it is to be ensured that the starting value of the generator is not dependent solely on inputs from outside. This requirement may be met, for example, by loading a physically generated, individual card-related random value into the chipcard during initialisation of the chipcard, to serve as the starting value for the internal pseudo-random number generator.

#### 6.7.4.3.3. Safeguards regarding initialisation and personalisation

The safeguards stated in the section on Personalisation must be observed in the personalisation of chipcards. The following additional safeguards are also to be provided:

**S-CHIP 3.1 Secure subsequent loading of applications**

In the case of chipcards for digital signatures, it must be ensured that it is not possible to read out or alter data which require protection (keys, passwords) via the subsequent loading of applications and software. This requirement can be met in a variety of ways:

Variant 1: A general ban is imposed on the subsequent loading of applications, software or operating system patches. In technical terms, this is ensured by implementing no such subsequent loading commands in the chipcard operating system.

Variant 2: Subsequent loading is possible in transport-encoded and MAC-secured form only. After transmission of the data to the chipcard, the latter decodes the data and calculates the MAC. If the MAC has been calculated correctly, the chipcard will import the supplied data.

The necessary transport code is to be incorporated on an individual chipcard-related basis during initial personalisation of the chipcard. The transport code must be known to the competent certification authority only. The certification authority must ensure that no security problems can arise as a result of data to be subsequently loaded. When no security problems are to be expected, the certification authority may encode the data for transport and make the data available for subsequent loading.
Variant 3: Appropriate protective safeguards are implemented for the hardware and the operating system of the chipcard to ensure that no unauthorised access to sensitive data of the signature application can be effected from subsequently loaded applications.
Variant 4: The subsequently loaded code consists not of a directly executable native code for the CPU nucleus concerned, but of a form of intermediate code which is regarded as interpretable data within the operating system and is thus able to initiate actions indirectly, provided that the interpreting operating system permits such actions. Here again, it is to be ensured that no unauthorised access to the sensitive data of the signature application is possible as a result of this variant.

Note: In the case of multiapplicative chipcards, the chipcard operating systems must be designed in such a manner as to guarantee freedom from interference, that is, the chipcard operating system must offer an inherent security function preventing another application from accessing the memory areas in which the application 'Digital Signature' is located. The scope of testing for the operating system and the 'Digital Signature' application could then be reduced to evaluation standard 'E4 high'.

#### 6.7.4.3.4. Safeguards regarding the physical body of the chipcard

**S-CHIP 4.1 Physical stability in accordance with applicable standards**
In order to ensure that the chipcard is ready for operation, i.e. available, at all times, the physical body of the card must be best equipped to resist the environmental influences which it encounters in daily use of the chipcard and must protect the embedded chip. The chipcard, and the physical body of the card in particular, must be able to guarantee a standardised high level of physical stability. To this end, the chipcard must pass the test procedures required in the standard [ISO 10373] and fulfil the requirements of the standards [ISO 7810], [ISO 7813], [ISO 7816-1].

**S-CHIP 4.2 Name of the card holder**
The name of the card holder should be applied to the body of the card in clearly legible and non-alterable form. This provides a simple means of personalising the card body.

**S-CHIP 4.3 Photograph of the card holder**
A photograph of the card holder on the body of the card provides a quickly verifiable means of personalising the card body. The photograph serves to identify the owner. It should be provided on all chipcards for which the link to the holder is of special importance. Technical measures should be taken to render manipulation of the photograph very difficult.

**S-CHIP 4.4 Signature strip**
The individual, personal signature of the chipcard holder on the chipcard serves as an identification feature for the holder and further strengthens the link between the holder and the chipcard. For this purpose, an alteration-resistant signature strip can be provided on the card

for application of the holder's signature or for transfer of the chipcard holder's signature from the application form.

**S-CHIP 4.5 Information (address) in case of loss**

In case of loss of the chipcard, a contact address should be stated on the body of the card, so as to enable the honest finder to return the chipcard to the owner via this channel. The address of the certification authority may be used for this purpose, for example.

**S-CHIP 4.6 Individual feature to prevent chip substitution**

In order to prevent the substitution of chips, in all chipcards the chip should be integrated into the body of the card in such a manner as to render it impossible to detach the chip without destroying the chip. In order to counteract punching-out of the chip from the body of the card in particular and to render any substitutions apparent, an individual card body feature should be applied to the rear of the card. This feature (e.g. photograph of the holder, signature strip, stamped name) should be applied to the rear of the card over the chip, so that punching out the chip will lead to destruction of the individual feature and will be easily detectable by the user.

**6.7.4.3.5 Safeguards regarding destruction of the chipcard**

**S-CHIP 5.1 Destruction of private signature keys**

A private key in a chipcard can be rendered unusable in either of two ways. If the chipcard so permits, a command can be initiated to delete a specific private key. This requires an intact, operational chipcard which incorporates such a command, however. Identification and authentication of the user should be essential prior to activating this command, so as to ensure that no-one is able to delete a key without authorisation. However, this means that a third party, such as the certification authority, will be unable to effect this deletion after calling in chipcards for replacement.

A second method of rendering a private key unusable involves the physical destruction of the chipcard's chip. To this end, the chip can be punched out and destroyed by a physical effect (e.g. hammer blow). When a chipcard is defective, this method can also be applied by third parties.

**6.7.4.3.6. Safeguards in case of violations of security policy**

**S-CHIP 6.1 Detectability of changes which are of relevance to security**

The following points must be considered as changes to chipcards which are of relevance to security:

- bit error in the memory area of the chip (accidental or provoked),
- attempted unauthorised use of the chipcard and
- manipulation of the chipcard's chip.

The following safeguards are expedient in order to render these changes apparent to the user:

- Memory areas in the chipcard which contain data subject to high integrity requirements (e.g. cryptographic keys) can be provided with an integrity protection feature which detects undesired changes and defects in the memory. To this end, a CRC or MAC security device can be applied over this memory area. In the event of changes, the chipcard may output an error message or refuse to function.
- In order to render attempts to use the chipcard without authorisation apparent, the number of attempts which a user may undertake with his chipcard before it is blocked should be limited. This is normally achieved by means of a maloperation counter, which blocks the

card after three failed attempts. The owner is able to recognise changes of relevance to security by reference to the status of the maloperation counter or by the fact that the card is blocked.

- The owner of a chipcard is able to recognise manipulations on the chip of a chipcard by the fact that that the chip is exposed or punched out and replaced. Safeguard S-CHIP 4.6 can be applied to render such manipulations apparent. In this connection, reference is also made to safeguards S-CHIP 1.10, S-CHIP 1.13, S-CHIP 1.14, S-CHIP 1.15 and S-CHIP 1.16, which provide for deactivation of the chip in the event of attempted manipulation.

#### 6.7.4.3.7. Safeguards regarding the chip card operating system

**S-CHIP 7.1 Identification and authentication of the user**

The chipcard operating system and the application 'Digital Signature' must ensure that use of the chipcard in connection with digital signatures is possible only after successful identification and authentication of the user.

It must be possible for the authenticated user to alter knowledge-based authentication data. The extent to which biometric authentication data should be alterable and under what conditions such alterations should be possible is to be clarified in the certification authorities' safety concepts.

If knowledge-based identification data (e.g. PIN, password) are required for authentication, on being used for the first time by its holder the chipcard should compel the holder to alter the authentication data which have been preset during personalisation. This enables the chipcard holder to establish whether the chipcard has been subject to misuse prior to handover.

The user must be able to initiate the alteration of knowledge-based authentication data (PIN, password) at any time. In the case of PINs the range of possible combinations is limited, on account of the reduced number of characters. Consequently, when a PIN change is carried out the chipcard should preselect a new PIN for the user, as the same probability for every possible PIN combination cannot be guaranteed if PINs are user-selectable. If user-selectable PINs are nevertheless to be approved, the users must be informed as to the attendant risks and the selection of suitable PINs or passwords.

After three incorrect entries for the authentication data, the application 'Digital Signature' must be blocked. It should be possible to cancel this blocking function in a secure manner, i.e. to reset the maloperation counter. This should be effected by entering a resetting code which, in turn, must also be protected against incorrect entries by means of a maloperation counter (= 3).

The chipcard operating system must ensure that the maloperation counter cannot be accessed from outside, i.e. that it can be reset only via correct entry of the authentication data.

It is to be clarified within the certification authorities' security concepts whether the resetting code is to be handed over to the user in a separate sealed PIN brief in addition to the actual PIN letter, or whether administrative bodies of the certification authority are able to cancel the blocking function for the card, subject to appropriate conditions being fulfilled (e.g. secure identification of the chipcard owner, authentication of the operating personnel, dual control principle, secure environment for the cancellation process).

The requirements which must be imposed on user authentication for the application 'Digital Signature' are limited on the one hand by the technical capabilities of chipcards and terminals, and on the other hand by the requirements of evaluation standard 'E 4 high'. At present, only decimal numbers can be entered at most terminals, and most of the available chipcards are unable to process passwords of more than 8 characters in length.

In order to attain the mechanism strength 'high', a decimal PIN must have at least 6 digit positions. However, the assessment of mechanism strength includes other technical safeguards, in addition to the technical and administrative operational environment. Consequently, it must be ensured that

- authentication information is not compromised by persons or by technical system components,
- the probability is uniformly distributed for every possible PIN combination,
- the confidentiality and integrity of the authentication information stored on the card are ensured by the chipcard operating system,
- read accesses and unauthorised alterations to PIN or key files are prevented during the generation of PIN and key files by appropriate access control settings,
- the required PIN length can be set only at the time of generating a PIN file and the PIN cannot be shorter than the minimum required length,
- the number of failed attempts and release attempts for a blocked PIN is limited and can only be set at the time of generating a PIN file,
- the PIN/key files required for authentication are correctly selected,
- verification is carried out prior to an authentication procedure to establish whether the referenced PIN exists on the card and whether it is blocked,
- further authentication attempts are rejected after three failed attempts,
- the length of the resetting code is at least 8 digit positions, and that
- the user himself is not able to alter the requirements relating to PIN authentication, but can only initiate a PIN change.

It depends on the specific implementation and the operational environment whether the mechanism strength 'high' is attained, and the specific mechanism strength can only be determined by means of an ITSEC evaluation.

**S-CHIP 7.2 Identification and authentication of terminals for commercial use**

When the user deploys his chipcard at a terminal, the security status of which he is unable to verify himself (e.g. terminal for commercial use), the chipcard must carry out this verification. Authentication of the terminal to the chipcard is then required prior to each subsequent transaction.

For this purpose, the terminal may possess a private key, together with the appurtenant certificate. Such sensitive data must be stored in areas provided with special protection against unauthorised access (e.g. security modules), and the processing of these data is also to take place in this area only. The chipcard then generates a random number, which it communicates to the terminal. The terminal signs this random number and transmits the signature and the certificate back to the chipcard.

The chipcard then verifies the validity of the certificate and the signature. Assuming that the terminal is sufficiently secure to prevent read-out of the private key and that the private key will be deleted automatically in the event of attempted manipulation, if the signature and certificate are valid then the terminal concerned must be a non-manipulated terminal. If the signature or certificate is not correct, this is an indication of manipulation.

If the chipcard is unable to communicate this verification result to the user autonomously, the result must be communicated indirectly, via the display of the terminal. In the case of a positive result, the chipcard could communicate an indicator to the terminal which has been selected by the user and incorporated in the course of personalisation, and this indicator would then be displayed by the terminal. As the terminal only receives this indicator when it is manipulation-

free, the terminal cannot mislead the user with regard to the result of the verification. The serial number counteracts renewed read-in of the result.

### S-CHIP 7.3 Access control

The access control facility of the chipcard operating system must ensure that secret information is stored in the chipcard's memory in such a manner that it cannot be read out from outside or by other applications. Such data includes private keys and the authentication data (passwords, biometric reference data).
Only the application 'Digital Signature' is to be permitted internal access to the private keys, whereby such access shall only be possible after due authentication of the user. Other applications on the chipcard must not have any access to data of the application 'Digital Signature'. If other applications access commands of the application 'Digital Signature', it must be ensured that this takes place in a correct and proper manner.

### S-CHIP 7.4 Reprocessing

The operating system of the chipcard must ensure that all memory areas (RAM, EEPROM) of the chipcard which have been used by the application 'Digital Signature' are erased prior to being used by another application.
However, as erasure of the appropriate EEPROM areas is not possible in the event of a failure of the chipcard's electric power supply, a flag system can be used to indicate that certain memory areas of the EEPROM are to be erased the next time the status Power On applies.
Another method of solving this problem involves reserving dedicated memory areas for the application 'Digital Signature', which are then available for this application only and cannot be used by any other application.

### S-CHIP 7.5 Records

The chipcard should be capable of recording actions which are relevant or critical to security, such as maloperation counters or actions relating to signing processes, for the purposes of analysis and the preservation of evidence.
The actions relating to the most recent signing processes should be recorded on the chipcard. For this purpose, information on the signing processes, such as date, terminal indicator, hashing value and filename of the signed document, should be stored. It should be possible for the users to read the record data. The record data should be protected against unauthorised alteration.

### S-CHIP 7.6 Enabling chipcards

Authentication should be carried out directly prior to the execution of signing processes. It is also possible to use chipcards which can be enabled for more than one signing process per authentication. The enablement for a preset number of signing processes or a preset period of time must be monitored by the chipcard. The chipcard should require explicit authentication prior to each signing process as a standard configuration. Each time other applications are initiated, renewed authentication shall be required for signing processes.
If it is possible for the user to enable his chipcard for several signing processes after successful authentication, in the course of the standard user notification he must be informed as to the risks of enabling his signature component in this manner and the appropriate number of signing processes to be enabled.

**S-CHIP 7.7 Implementation of the specification**

In configuring the operating system for chipcards incorporating the Digital Signature application, the 'interface for chipcards with digital signature application/function in accordance with SigG and SigV, draft for DIN standard, DIN NI-17.4' is to be implemented.

#### 6.7.4.4. Assignment of safeguards to proposed solutions

| Safeguard | Counteracts threat | Solution model | |
|---|---|---|---|
| | | Monofunctional solution | Multifunctional solution |
| S-CHIP 1.1 | 9,10,21,22 | recommended | recommended |
| S-CHIP 1.2 | 9,10,21,22 | required | required |
| S-CHIP 1.3 | 9,10,21,22 | recommended | recommended |
| S-CHIP 1.4 | 9,10,21 | required | required |
| S-CHIP 1.5 | 9,10,21 | required | required |
| S-CHIP 1.6 | 9,10,21 | recommended | recommended |
| S-CHIP 1.7 | 9,10,21 | recommended | recommended |
| S-CHIP 1.8 | 9,10,21 | required | required |
| S-CHIP 1.9 | 9,10,21 | required | required |
| S-CHIP 1.10 | 9,10,21 | required | required |
| S-CHIP 1.11 | 9,10,21 | required | required |
| S-CHIP 1.12 | 9,10,21,22 | recommended | recommended |
| S-CHIP 1.13 | 9,10,21 | recommended | recommended |
| S-CHIP 1.14 | 9,10,21 | required | required |
| S-CHIP 1.15 | 9,10,21 | required | required |
| S-CHIP 1.16 | 9,10,21 | required | required |
| S-CHIP 1.17 | 9,10 | recommended | recommended |
| S-CHIP 2.1 | 5,6,7 | required | required |
| S-CHIP 3.1 | 16,17,24 | required | required |
| S-CHIP 4.1 | 27 | required | required |
| S-CHIP 4.2 | 26,28 | required | required |
| S-CHIP 4.3 | 26,28 | recommended | recommended |
| S-CHIP 4.4 | 26,28 | recommended | recommended |
| S-CHIP 4.5 | ./. | recommended | recommended |
| S-CHIP 4.6 | 26 | required | required |
| S-CHIP 5.1 | 14 | required | required |

| | | | |
|---|---|---|---|
| S-CHIP 6.1 | 24,25,26 | required | required |
| S-CHIP 7.1 | 1,2,24 | required | required |
| S-CHIP 7.2 | 24 | required | required |
| S-CHIP 7.3 | 1,4,10,24 | required | required |
| S-CHIP 7.4 | 9,10 | recommended | required |
| S-CHIP 7.5 | 18,20 | recommended | recommended |
| S-CHIP 7.6 | 24 | recommended | recommended |
| S-CHIP 7.7 | 24 | recommended | recommended |

#### 6.7.4.5. Assignment of safeguards to the security requirements and recommendations

| Security requirements/ Recommendation | Measure |
|---|---|
| REQ-CHIP 1.1 | S-CHIP 1.1, S-CHIP 1.2, S-CHIP 1.3, S-CHIP 1.4, S-CHIP 1.5, S-CHIP 1.6, S-CHIP 1.7, S-CHIP 1.8, S-CHIP 1.9, S-CHIP 1.10, S-CHIP 1.11, S-CHIP 1.14, S-CHIP 1.15, S-CHIP 1.16 |
| REQ-CHIP 1.2 | S-CHIP 1.1, S-CHIP 1.2, S-CHIP 1.3, S-CHIP 1.4, S-CHIP 1.5, S-CHIP 1.7, S-CHIP 1.8, S-CHIP 1.9, S-CHIP 1.10, S-CHIP 1.11, S-CHIP 1.14, S-CHIP 1.15, S-CHIP 1.16 |
| REQ-CHIP 1.3 | S-CHIP 1.10, S-CHIP 1.14, S-CHIP 1.15, S-CHIP 1.16, S-CHIP 6.1 |
| REQ-CHIP 2.1 | S-CHIP 2.1 |
| REQ-CHIP 2.2 | S-CHIP 2.1 |
| REQ-CHIP 3.1 | see Section 6.3 Personalisation |
| REQ-CHIP 3.2 | see Section 6.3 Personalisation |
| REQ-CHIP 3.3 | S-CHIP 3.1 |
| REQ-CHIP 3.4 | see Section 6.3 Personalisation |
| REQ-CHIP 4.1 | S-CHIP 4.1, S-CHIP 4.2, S-CHIP 4.3, S-CHIP 4.4, S-CHIP 4.5, S-CHIP 4.6 |
| REQ-CHIP 5.1 | S-CHIP 5.1 |
| REQ-CHIP 6.1 | S-CHIP 6.1 |
| REQ-CHIP 7.1 | S-CHIP 7.1 |

| | |
|---|---|
| REQ-CHIP 7.2 | S-CHIP 7.2 |
| REQ-CHIP 8.1 | S-CHIP 7.3 |
| REQ-CHIP 8.2 | S-CHIP 7.1 |
| REQ-CHIP 8.3 | S-CHIP 7.3 |
| REQ-CHIP 8.4 | S-CHIP 7.1, S-CHIP 7.3 |
| REQ-CHIP 8.5 | S-CHIP 7.3 |
| REQ-CHIP 8.6 | S-CHIP 7.3 |
| REQ-CHIP 8.7 | S-CHIP 7.1, S-CHIP 7.3 |
| REQ-CHIP 10.1 | S-CHIP 7.4 |
| REC-CHIP 0.1 | S-CHIP 7.7 |
| REC-CHIP 1.1 | S-CHIP 1.17 |
| REC-CHIP 3.1 | see Section 6.3 Personalisation |
| REC-CHIP 3.2 | see Section 6.3 Personalisation |
| REC-CHIP 8.1 | S-CHIP 7.6 |
| REC-CHIP 9.1 | S-CHIP 6.1, S-CHIP 7.1, S-CHIP 7.5 |
| REC-CHIP 9.2 | S-CHIP 7.5 |

#### 6.7.4.6. Requirements for the tests

§ 14 (4) SigG requires chipcards employed as signature components to undergo adequate testing in accordance with current engineering standards. Confirmation that they comply with the requirements of the Digital Signature Act and the Digital Signature Ordinance is also required. As hardware security plays a vital role with regard to chipcards, evaluation of the hardware is imperative.

**Hardware evaluation**

For the purposes of hardware evaluation it is expedient to minimise the scope of documentation while at the same time guaranteeing adequate protection for the confidential manufacturer's information. The following evaluation measures could be carried out by a hardware laboratory:

Black box tests:

1. The testing laboratory tests the hardware under normal and abnormal operating conditions via the interfaces of the chipcard.
2. The testing laboratory checks for irregularities in time response or current input in connection with cryptographic processes.
3. The testing laboratory carries out penetration tests after exposing the chip (microprobing, bellcore attacks, ...).

White box tests:

4. The manufacturer describes the hardware-related security features of the chip. The testing laboratory verifies the completeness of these features and investigates possible theoretical forms of attack.

5. The manufacturer explains the circuit diagram area and specifies where and how the hardware security has been implemented by reference to the physical chip layer. The testing laboratory verifies the manufacturer's specifications.

6. The manufacturer and the testing laboratory carry out joint tests for the forms of attack established in step 4.

All in all, the hardware testing described here involves the verification of manufacturers' specifications (conformity tests) and penetration tests without and with inside knowledge.

Only accredited testing laboratories are to be approved (and appointed) for this testing work.

**Software evaluation**

Of the above-stated security requirements, the following must be verified in the course of an ITSEC evaluation:

REQ-CHIP 1.1, REQ-CHIP 1.2, REQ-CHIP 1.3, REQ-CHIP 2.1, REQ-CHIP 3.3, REQ-CHIP 3.4, REQ-CHIP 6.1, REQ-CHIP 7.1, REQ-CHIP 7.2, REQ-CHIP 8.1, REQ-CHIP 8.2, REQ-CHIP 8.3, REQ-CHIP 8.4, REQ-CHIP 8.5, REQ-CHIP 8.6, REQ-CHIP 8.7, REQ-CHIP 10.1.

### 6.7.5 Security boxes as signature components

The security box is a basic component of an overall system for the generation and verification of digital signatures. The security box is intended as a special component for mainframe applications, and represents a physically, cryptographically and temporarily closed-off confidential area within the overall open system, in which individual steps (operations) of the signature process which are of relevance to security can be carried out in a reliable and secure manner. The trust which is placed in the security box is justified in that both the individual components of this module (be they implemented in software, hardware and/or firmware) which are subject to a risk of manipulation and the operations carried out in the security box which are considered to be critical to security (such as the key generation process) are protected against external attack by means of special 'hardware-supported[16]' security safeguards[17]. Together with the functions of the operating system and with the aid of an automatic memory conditioning process, it is further ensured that the activation of such operations is permitted only when an authorised status applies, and that all plain-text files requiring protection (such as authentication information and private signature keys) will be erased immediately, in the event of forced entry into the module. The following operations are considered relevant to security here:

- the authentication of users,
- key generation and key management,
- calculation of the hashing value,
- the verification of certificates,
- storage of the root authority's public key,
- signature calculation and
- signature verification.

The operations carried out in the security box are generally initiated from a host computer. The security box is also connected via the host to the public network, to enable it to use the directory and time stamping services. This indirect network link may result in additional security requirements. Such requirements can only receive due consideration in a security concept for the operational environment, however. At this point it is thus important to note that functional and security objectives set for the signature process as a whole can only be attained by an overall system in which the security box under consideration here constitutes a system component. In particular, this means that effective interaction is required between the security box and the other components of the overall system (cf. Section 6.6).

In order to establish security requirements and concrete security safeguards with regard to the security box, it is first of all expedient to separate the security box from the overall system, and then to apply the requirements stipulated in the Digital Signature Act and the Digital Signature Ordinance to the component 'security box'.

[16] The storage of and maintenance of secrecy with regard to signature keys and authentication data in keeping with the legal requirement to reliably eliminate the possibility of such sensitive data being disclosed in accordance with current engineering standards justifies the requirement for a hardware component which cannot be read out without an unrealistic scope of tampering (cf. Explanatory note on § 16 (1) SigV, for example).

[17] Generally consisting of a mechanical and electronic / sensor-based protective facility.

#### 6.7.5.1 Generic security requirements and recommendations

The following security requirements and recommendations can be established for the technical component 'security box' on the basis of the Digital Signature Act and the appurtenant Ordinance:

##### 6.7.5.1.1 Requirements pertaining to the operating system

**Identification and authentication of the user to the security box**

REQ-SBOX 1.1 The user (e.g. signature user, administrator, revisor, auditor, maintenance technician) must identify and authenticate himself to the security box. This process must take place prior to each subsequent interaction with the security box. Subsequent interactions may only be possible after successful identification and authentication. The authentication information is to be protected against unauthorised access.
cf.: Explanatory note on § 2 (1) SigG, § 14 (1) SigG, Explanatory note on § 14 (1) SigG, § 16 (2) SigV, Explanatory note on § 16 (2) SigV
Safeguards pertaining to this requirement: S-SBOX 1.1, S-SBOX 1.2, S-SBOX 1.11

REQ-SBOX 1.2 The user must be provided with a facility which enables him to alter his knowledge-based authentication data.
Safeguards pertaining to this requirement: S-SBOX 1.3

REC-SBOX 1.1 Biometric user characteristics can be used for authentication purposes. In this case, the identification data must be stored in the security box in such a manner that they cannot be read out and can be altered by duly authorised persons only.
cf.: § 16 (2) Sentence 3ff. SigV, Explanatory note on § 16 (2) SigV

REC-SBOX 1.2 The security box is to require alteration of the knowledge-based authentication data when it used for the first time.
cf.: Explanatory note on § 5 (1) SigV
Safeguards pertaining to this recommendation: S-SBOX 1.3

**Authentication of the user[18] in the course of the signing process and auto-logout**

REC-SBOX 1.3 In order to ensure that the signing process performed with the user key in the security box takes place with the knowledge and consent of the user, a renewed request for input of the PIN or password should be output directly prior to execution of the signing process. The signing process may comprise the signing of several data - including signing in batch mode. In all cases, the user should be able to recognise whether the security box is enabled / is in the corresponding signing mode after a successful authentication process. When no inputs or outputs into or from the security box occur over a prolonged period in this state, the authentication state is to be reset

[18] Depending on the specific operational scenario (home environment, banking sector) and application (single signature, multiple signature, etc.), it may be necessary to manage several users, in addition to various roles.

automatically. It should be possible for this period to be set individually by the system administrator. The resumption of a signing process which is in progress requires reverification of the authentication data. All authentication information is to be protected against unauthorised access. A limitation of the number of authentication attempts is necessary in this connection. A compulsory password change at specific intervals is also recommendable.
cf.: Explanatory note on § 2 (1) SigG, § 14 (1) SigG, Explanatory note on § 14 (1) SigG, § 16 (2) SigV, Explanatory note on § 16 (2) SigV
Safeguards pertaining to this recommendation: S-SBOX 1.4, S-SBOX 1.5

**Mutual identification and authentication between security box and external processes**

REC-SBOX 1.4 When it is necessary to ensure that the security box may only interact with specific external processes or programmes (e.g. processes or programmes which have been initiated in the host or on a special chipcard), a mutual authentication protocol is expedient.
cf.: Explanatory note on § 2 (1) SigG, § 14 (1) SigG, Explanatory note on § 14 (1) SigG, § 16 (2) SigV, Explanatory note on § 16 (2) SigV
Safeguards pertaining to this recommendation: S-SBOX 1.6

REC-SBOX 1.5 When the security box is employed by users who have no control over the security box and its security features, the security box must also be able to authenticate itself to these users.
Safeguards pertaining to this recommendation: S-SBOX 1.7

**Access control**

REQ-SBOX 1.3 The private signature key is stored solely and exclusively in the security box, where it is subject to access control. Only the process executed in the security box in connection with signature generation is authorised to access the private signature key, for the purpose of signature generation.
cf.: § 2 (1) SigG, Explanatory note on § 2 (1) SigG, § 5 (4) SigG, Explanatory note on § 5 (4) SigG, § 14 (1) SigG, Explanatory note on § 14 (1) SigG
Safeguards pertaining to this requirement: S-SBOX 1.8, S-SBOX 1.9

REC-SBOX 1.6 The software, stored certificates, public signature keys and all keys requiring secrecy (e.g. transport keys) which are employed in the generation and verification of signatures must be subject to access control, so as to ensure that only authorised persons or processes are able to obtain access.
cf.: § 1 (1) SigG
Safeguards pertaining to this recommendation: S-SBOX 1.10

**Reprocessing**

REQ-SBOX 1.4 Those memory areas which are occupied by the private signature key in the course of the signature calculation process (including the register of the cryptoprocessor) are to be erased after the completion of signature generation.
cf.: § 5 (4) SigG, Explanatory note on § 5 (4) SigG, § 14 (1) SigG, Explanatory note on § 14 (1) SigG

Safeguards pertaining to this requirement: S-SBOX 1.12, S-SBOX 1.13

**Records**

REC-SBOX 1.7 The security box should be able to record actions which are of relevance to and critical to security for the purposes of analysis and the preservation of evidence (e.g. by means of a directly connected printer), or to supply such information to the host for subsequent evaluation and processing. Examples of such actions are signing processes, maintenance work, attempted manipulations and identified error statuses.
cf.: Explanatory note on § 14 (1) SigG, § 14 (2) Sentence 2 SigG, § 4 (1) No. 1 SigV
Safeguards pertaining to this recommendation: S-SBOX 1.14, S-SBOX 1.15, S-SBOX 1.16

**Transmission security**

REC-SBOX 1.8 Data transmission between security box and operational environment (e.g. host computer, time stamping service, directory service) should be secured against manipulations and malfunctions.
cf.: § 2 (1) SigG, Explanatory note on § 9 SigG, § 14 (1) SigG, Explanatory note on § 14 (1) SigG
Safeguards pertaining to this recommendation: S-SBOX 1.17, S-SBOX 1.18, S-SBOX 1.19, S-SBOX 1.20, S-SBOX 1.21

**Integrity**

REQ-SBOX 1.5 The security box must verify its integrity and freedom from manipulation automatically when in use. Should changes to the security box which are of relevance to security have taken place, this fact must be clearly displayed to the user. Changes of relevance to security may result from:

- manipulations of software and hardware,
- technical defects and inadequacies (material fatigue, ageing, etc.), which would lead to the failure of a memory chip or a hardware mechanism, for example,
- maloperation and entry of incorrect data,
- force major, such as lightning or power failure,
- lack of system administration or inadequate system administration.

cf.: § 16 (2) Sentence 4 SigV
Safeguards pertaining to this requirement: S-SBOX 1.22, S-SBOX 1.25

REQ-SBOX 1.6 If the security box is to be used on a terminal for signature generation and verification which is offered for commercial use, the security box must be able to verify that the terminal is genuine and has not bee manipulated.
cf.: § 16 (3) Sentence 3 SigV
Safeguards pertaining to this requirement: S-SBOX 1.23

REC-SBOX 1.9 A reliable system time is to be provided for the purposes of verifying a time stamp in connection with the generation of a digital signature and verifying the validity of a signature key certificate in the course of signature verification.
cf.: § 9 SigG, § 4 (1) No. 5 SigV
Safeguards pertaining to this recommendation: S-SBOX 1.24

#### 6.7.5.1.2 Requirements for the administrative environment

REQ-SBOX 2.1 The loss of the signature component must be apparent to the user of the security box.
cf.: § 4 (1) No. 1 SigV
Safeguards pertaining to this requirement: S-SBOX 2.3

REQ-SBOX 2.2 The security box must provide the certification authority with a facility by which it is able to verify that the security box constitutes a suitable component with regard to key generation and personal identification/authentication.
cf.: § 5 (1) SigV
Safeguards pertaining to this requirement: S-SBOX 2.4

REC-SBOX 2.1 The root certificate can be loaded into the security box together with the user certificate in the course of the personalisation process.
cf.: Explanatory note on § 4 (5) SigG
Safeguards pertaining to this recommendation: S-SBOX 2.1

REC-SBOX 2.2 Arrangements are to be made for reliable handover of the key parameters and authentication parameters and for a secure delivery process for the security box.
cf.: Explanatory note on § 6 SigV
Safeguards pertaining to this recommendation: S-SBOX 2.2

#### 6.7.5.1.3 Encoding security

REQ-SBOX 3.1 It must be ensured that the private signature key cannot be calculated from the signature.
cf.: § 16 (2) SigV
Safeguards pertaining to this requirement: S-SBOX 3.1

REQ-SBOX 3.2 The possibility of manipulation of a digital signature or forgeries of signed data must be excluded during signature generation and ascertainable in the course of signature verification.
cf.: § 16 (2) SigV
Safeguards pertaining to this requirement: S-SBOX 1.26, S-SBOX 3.2

#### 6.7.5.1.4 Key management

REQ-SBOX 4.1 The generation of signature keys in the security box must ensure
- that a signature key is generated once only,
- that the private signature key cannot be calculated from the public key, and
- that the private signature key cannot be duplicated.

cf.: Explanatory note on § 2 (1) SigG, § 16 (1) SigV
Safeguards pertaining to this requirement: S-SBOX 4.1, S-SBOX 4.2, S-SBOX 4.3, S-SBOX 4.4

REQ-SBOX 4.2 It must be ensured that the private signature key remains secret and cannot be read out (including read-out via the interfaces provided for normal access). The inalterability (integrity) of the private signature key in the course of data processing within the security box must also be ensured.
cf.: Explanatory note on § 2 (1) SigG, § 5 (4) SigG, Explanatory note on § 5 (4) SigG, § 14 (1) SigG
Safeguards pertaining to this requirement: S-SBOX 4.3, S-SBOX 4.4

REC-SBOX 4.1 The private signature key should be erased automatically when a non-secure operational status occurs or in the course of decommissioning.
cf.: Explanatory note on § 2 (1) SigG, § 14 (1) SigG, § 4 (1) No. 1 SigV
Safeguards pertaining to this recommendation: S-SBOX 4.5

#### 6.7.5.1.5 Protection of software and hardware components from manipulation

REQ-SBOX 5.1 The physical/material design of the security box is to ensure that the private signature key and the authentication information cannot be read out or purposefully altered under any circumstances whatsoever.
cf.: § 5 (4) SigG, Explanatory note on § 5 (4) SigG, Explanatory note on § 14 (1) SigG, § 16 (1) SigV
Safeguards pertaining to this requirement: S-SBOX 5.1

REC-SBOX 5.1 Safeguards should be incorporated into the security box to prevent physical access to data by circumventing the interfaces provided for normal access (e.g. by opening the device and establishing contacts with internal hardware components), or at least to ensure that any such accesses are subsequently detectable.
cf.: Explanatory note on § 2 (1) SigG, § 14 (1) SigG, Explanatory note on § 14 (1) SigG, § 4 (1) No. 1 SigV, § 16 (1) SigV, § 16 (2) Sentence 3ff SigV
Safeguards pertaining to this recommendation: S-SBOX 5.2

REC-SBOX 5.2 The security box should incorporate a deactivation function to put the security box temporarily out of operation on request from the user.
cf.: § 14 (1) SigG, Explanatory note on § 14 (1) SigG, § 4 (1) No. 1 SigV, § 16 (2) Sentence 4 SigV, Explanatory note on § 16 (1) Sentence 3 SigV
Safeguards pertaining to this recommendation: S-SBOX 5.3

#### 6.7.5.1.6 Fail-safe operation (safeguards in case of malfunctions and maloperation)

REC-SBOX 6.1 The internal security status of the security box should be displayable or communicable to and retrievable by the user or an external master process at all times.
cf.: § 2 (1) SigG, § 14 (1) SigG, Explanatory note on § 14 (1) SigG, § 16 (2) Sentence 4 SigV, § 16 (1) Sentence 3 SigV, § 16 (2) Sentence 3ff SigV
Safeguards pertaining to this recommendation: S-SBOX 6.1

REC-SBOX 6.2 The two operations 'authentication' and 'PIN or password change' should take place under the control of a clear and user-friendly menu system.
cf.: § 2 (1) SigG, § 4 (1) No. 2 SigV, § 5 (1) SigV
Safeguards pertaining to this recommendation: S-SBOX 6.2

#### 6.7.5.1.7 Emanation security, prevention/attenuation of concealed channels

REQ-SBOX 7.1 The external behaviour (for example emanation, current input, time response) of the security box must be neutral. It must not be possible to infer any details regarding private keys, identification parameters or other confidential information by observing this behaviour.
cf.: § 1 (1) SigG, § 5 (4) SigG, Explanatory note on § 5 (4) SigG
Safeguards pertaining to this requirement: S-SBOX 7.1, S-SBOX 7.2

#### 6.7.5.1.8 Other functional requirements

REC-SBOX 8.1 The security box should be able to establish a direct or indirect link to the time stamping service and the directory service.
cf.: § 9 SigG, § 4 (1) No. 5 SigV, Explanatory note on § 4 (1) No. 5 SigV
Safeguards pertaining to this recommendation: S-SBOX 8.1

#### 6.7.5.2 Proposed solutions

Figure 1 shows the fundamental configuration for the overall system, comprising the basic components:

- host (with a direct link to the security box),
- operating terminal (e.g. keyboard, scanner[19]),
- display component (e.g. printer, screen, display, verification indicator),
- security box,
- chipcard terminal and chipcard.

In addition, there is a link via the host to the components

- directory service and
- time stamping service.

Solution variants for the security box:

Two basic solution variants come into consideration:

1. **Integrated security box**

   In this variant, the security box possesses its own input facility (e.g. keyboard, scanner) and display component (e.g. display, screen or connected printer), a chipcard terminal and chipcard and an indirect link to the directory and time stamping service. Where possible, the components involved in this variant are integrated directly into the security box (cf. Fig. 1).

2. **Dedicated security box**

   In contrast to the architecture outlined above, in this variant the security box possesses only a direct transmission channel to the operational environment. It has no input facility, only limited display facilities (e.g. LEDs), no chipcard terminal and only indirect access to the directory and time stamping service via the operational environment (cf. Fig. 2).

[19] For the input of biometric characteristics.

Configuration of the overall system

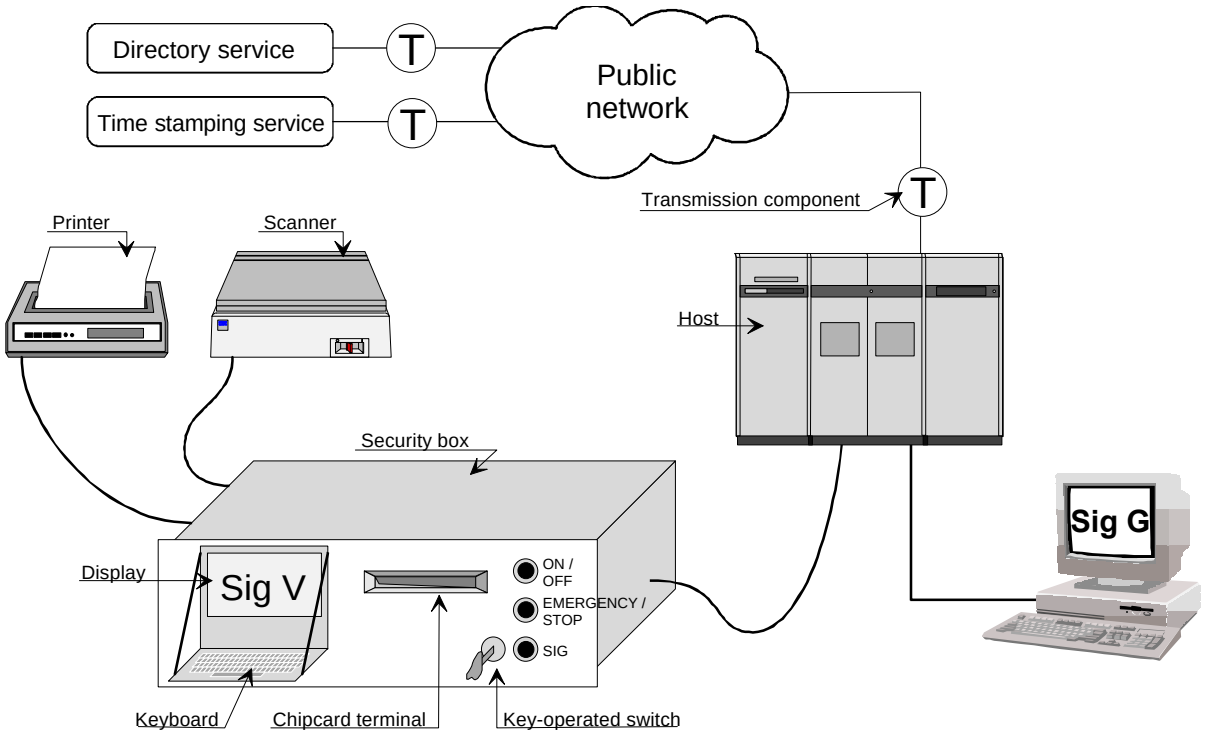



Figure 1: Integrated security box

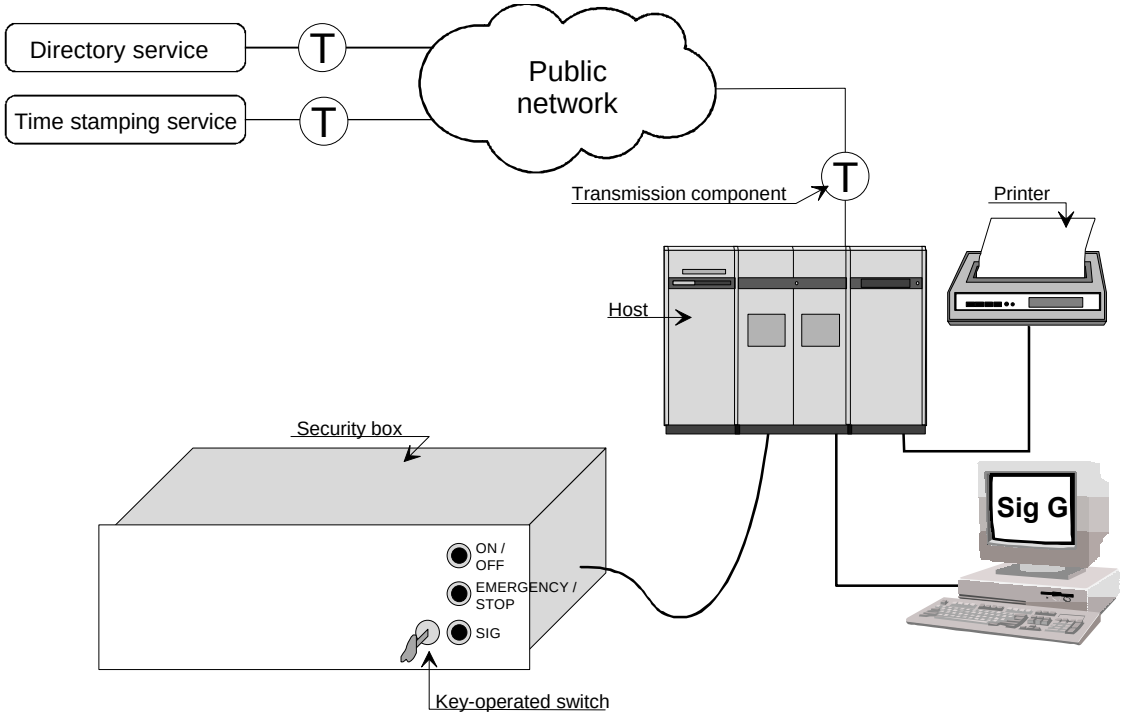



Figure 2: Dedicated security box

Operating modes:

Three alternatives are available for key management, including the personalisation process:

1. generation of the private signature key inside the security box,
2. generation of the private signature key at the certification authority and
   a) central personalisation or
   b) decentralised personalisation.

Use of the directory service:

The two following alternatives are available with regard to use of the directory service:

1. use of the service when the sender's certificate is known or
2. use of the service when the serial number of the certificate is known.

Hashing of the data to be signed:

Data interchange between the security box and the host is effected via a direct and secure communications link between the two facilities. Again, two possibilities are available with regard to hashing of the data to be signed:

1. hashing of the data to be signed on the host or
2. hashing of the data to be signed in the security box.

User authentication during the signing process:

Successful user authentication is a strict prerequisite for any form of use of the security box. In order to maintain the authenticity gap between a user and the signing process which is in progress in the security box on an acceptable scale, it is recommendable to carry out user authentication directly before each signing process. The use of methods including biometric processes is recommended in this connection for the purposes of user identification and authentication.

Presentation of verification and status information:

The verification and status information supplied by the security box includes the authentication dialogue, the operational and security status, the time stamp and the result of the signature verification process. This information can be presented, identified or forwarded in either of two ways:

1. directly, via a display/presentation element on the security box, or
2. as a data record for subsequent use in the area of the application concerned.

Transport medium for keys and certificates:

A chipcard[20] represents a suitable transport medium for the transfer (and thus temporary intermediate storage) of signature keys and certificates between the certification authority and the area of deployment of the security box.

[20] The examination of the area 'signature components' does not include security requirements and safeguards relating to this application of the chipcard.

Life cycle of the security box:

The overall life cycle of the security box comprises the following phases:

0. Concept development

   In a procedure involving the development, production, installation, etc. through to decommissioning of the security box according to a life cycle model, the specifications are drawn up at the end of the concept development phase. The main contents of these specifications are the stipulations and requirements imposed on the security box and the solution concepts. This approach is idealistic in that additional needs generally arise in the subsequent phases, e.g. as a result of development work or requirements of the production process.

1. Development

   In accordance with the security concept for the specific implementation of the security box, development of the necessary product components is carried out in the development area under the control of the responsible design engineer. This area incorporates an access-controlled and trustworthy working area in which both the complete product documentation (incl. any manuals and the source code / hardware design drawings) and the employed development tools and facilities are protected from unauthorised changes and examination by means of an access control system.

2. Production and assembly

   The security box consists of software and hardware components. Its essential design is characterised by

   i) a maintenance-free security module[21],

   ii) an active key-erasing function in the event of attempted attack, and

   iii) sensor and signalling devices to provide active protection against manipulation.

   The production and integration of these components (including their electromechanical assembly) is carried out in the production area, under the control of the responsible manufacturer. The production processes and the production environment are subject to continuous quality assurance and quality control. In turn, the quality assurance and control systems form part of a standard acceptance inspection and delivery procedure. Prior to commissioning, a serial number and a transport key are also generated and assigned, both being accommodated in the security box. In order to preserve the integrity of the security box, it is also provided with an inherent authentication code (e.g. MAC or CRC), which is known solely to the responsible staff of the manufacturer, and which reaches the application / operational environment of the security box via a reliable channel.

3. Commissioning and configuration

   Embedding and connection of the security box in the operational environment are carried out by the personnel of the operating centre (e.g. system administrator). As this personnel possesses the authentication code of the security box, it is able to verify the integrity of the security box. The initialisation work concludes with loading of the private or transmission of

[21] New release statuses can be loaded by authorised persons (e.g. the system administrator) in the course of the product's life cycle.

the public signature key from/onto the supplied chipcard. This is to be seen in the context of the following 'operating modes':

a) Key generation inside the security box

The supplied chipcard[22] (functioning here solely as a transport medium) is already in a prepersonalised state, in which the chipcard contains its operating system in the version evaluated and approved by the certification authority. In order to establish a communications link between the chipcard and the security box, a successful identification and authentication process must first of all be completed between the two devices. After generation of the signature key pair in the security box, the public signature key is transmitted in transport-encoded form into the chipcard's data blocks and the chipcard is transferred to the competent certification authority for the purpose of personalisation.

b) Key generation at the certification authority

In this operating mode the signature key pair is generated at the certification authority.

i) Central personalisation

In the case of central personalisation, the security box is first of all delivered to the certification authority for the purpose of personalisation. After a successfully completed identification and authentication process, the personnel of the certification authority load the private signature key into the security box in transport-encoded form, together with the public signature key and the signature key certificate. Only then is the security box delivered to the operational environment.

ii) Decentralised personalisation

Decentralised personalisation involves a process whereby the security box is delivered directly to the operational environment. As generation of the signature key pair is carried out at the certification authority, a chipcard is employed here also as the transport medium for the key pair. After delivery of the chipcard to the operational environment, the signature key pair is loaded on site by the personnel of the operating centre. Appropriate IT measures are to be installed to ensure that the private signature key is subsequently erased on the chipcard.

After decoding the private signature key, the security box carries out a verification of the signature key pair. Only after obtaining a positive result from the verification process are the preconditions for operation of the security box deemed to be fulfilled.

The authentication data (passwords, PINs or biometric characteristics) which identify the user, revisor, auditor or maintenance technician as an authorised user of the security box in the operational, updating and maintenance phase are also generated and stored via an initialisation process during the commissioning/configuration phase, and subsequently communicated to the users via a reliable channel.

[22] Use of the chipcard as a transport medium constitutes only a recommendation here. The important aspect at this point is an unambiguous link to the private key. This can be achieved, for example, by means of a digital signature under the public key.

4. Operation

   There are three possible operational states for the security box in its operational phase:

   a) OFF state

      The security box is switched off, including the chipcard terminal and any incorporated display and control elements.

   b) ON state

      In this system state the security box fulfils all the security requirements for secure and reliable key generation and signature verification. With regard to the possibility of sending inquiries to the directory service, two alternatives are available:

      i) inquiries based on a known sender certificate, or

      ii) inquiries based on a known certificate serial number.

      Prior to generating a signature, the user must successfully authenticate himself to the security box.

   c) EMERGENCY STOP state

      This operational status indicates that a technical malfunction has occurred or that the system state is no longer considered secure. The security box is released from this system state by the revisor in the course of the maintenance phase.

5. Maintenance

   This phase primarily concerns inspection and the rectification of errors and defects. At the same time, the revisor is also able to evaluate information which has been recorded by the security box. After completing the maintenance work, the security box is returned to the defined 'ON' state. The revisor/auditor must successfully authenticate himself to the security box, prior to carrying out maintenance work.

6. Decommissioning

   In order to prevent signatures from being generated with the security box beyond the desired duration of its operational phase, the memory area containing the private signature key at least is to be processed accordingly (i.e. erased or, if applicable, overwritten).

#### 6.7.5.3 Safeguards

##### 6.7.5.3.1 Security safeguards for the operating system

**Identification and authentication of the user to the security box**

**S-SBOX 1.1 User administration and authentication**

The security box is able to distinguish and administrate different user roles. Each user who wishes to obtain access to objects or other resources of the security box must furnish proof of his identity and authenticity, prior to initial interaction with the security box. Subsequent interactions are possible only after successful verification.

**S-SBOX 1.2 Limitation of the number of failed access attempts**

The authentication information is stored in one-way encoded form and is subject to access control. The number of authentication attempts is limited. After three failed attempts, the user indicator is temporarily invalidated. In the event of a lost PIN or password, only the administrator is able to reset the authentication data to the initialisation values.

**S-SBOX 1.3 Password change**

A PIN or password can be altered by the user at any time in operational state 'ON'. The user is compelled to change the knowledge-based authentication data upon using the security box for the first time and after a varying time span for the user.

**Authentication of the user during the signing process and auto-logout**

**S-SBOX 1.4 User authentication during the signing process**

The object of authenticating the user directly prior to executing the signing process is to prevent unauthorised and unintentional (accidental) signing. After a successfully completed authentication operation, it is indicated to the user that the security box is currently enabled for the signature generation process (signing mode).

**S-SBOX 1.5 Auto-logout**

The logout process for the user is carried out automatically and cannot be deactivated. An auto-logout is effected after a defined period during which no actions have been carried out in an incomplete signing process. Further interaction with the security box is then possible only after renewed identification and authentication.

**Mutual identification and authentication between security box and external processes**

**S-SBOX 1.6 Identification and authentication of the host**

Similarly to the user, the user programme which is running on the host must also furnish proof of the legitimacy of the intended access, prior to controlled access to the objects contained in the security box. This authentication process also serves to identify changes on the host and to verify the integrity of the host process. A challenge-response protocol provides a suitable method here.

**S-SBOX 1.7 Identification and authentication of the security box**

The trustworthiness of the security box is based on the verification and confirmation of its security functions and characteristics in accordance with recognised standards and guidelines. Prior to integration of the security box into an operational environment, it is recommendable for the security box to authenticate itself to its operational environment.

**Access control**

**S-SBOX 1.8 Administration of rights**

The security box is able to distinguish and administrate the access and execution rights of users and external processes with regard to objects which require protection. In this context, the security box is able to identify the user roles of 'user', 'administrator' and 'revisor' and the external process of the host system. It is possible to restrict access to objects individually for each role. In particular, it is possible to define access rights to certain objects in exclusive terms, i.e. for the signing process, for example, so that this process can only be executed by the user.

**S-SBOX 1.9 Restrictive use of the private signature key**

The object 'private signature key' is subject to access control. Only the process which has been initiated by the user and is currently running in the security box in connection with signature generation is authorised to access the private signature key for the purposes of signature generation.

**S-SBOX 1.10 Limitation of the number of access attempts**

The software and hardware, stored user certificates, public signature keys and other secret keys (e.g. transport keys) employed for the purposes of signature generation and signature verification are subject to access control, such that only authorised persons or processes possess a corresponding access or execution right. The granting of access can furthermore be defined so as to be dependent on the current day of the week/time of day, the current security status of the security box and/or the responsible user.

**S-SBOX 1.11 Dual control principle**

The execution of particularly sensitive functions, such as maintenance and repair work, is monitored via application of the dual control principle.

**Reprocessing**

**S-SBOX 1.12 Reuse of memory areas**

The memory areas which are occupied in the course of signature calculation and released for reuse by the security box are completely erased after the signature generation process, so as to ensure that no information on the private signature key can be inferred from the former contents of such areas.

**S-SBOX 1.13 Destruction of private signature keys**

Security boxes which are withdrawn from service are processed so as to ensure that the private signature key cannot be deduced from their former content.

**Records**

**S-SBOX 1.14 Recording of attempts to obtain unauthorised access**

Failed authentication attempts are recorded with the appurtenant date, time and user role. Unauthorised accesses are also recorded for the purposes of their identification and the preservation of evidence. Examples of other actions which are recorded include signing processes, maintenance/administration work and identified error statuses.

**S-SBOX 1.15 Access right for record information**

The record information is subject to access control. Only the revisor/auditor is permitted access to the record information.

**S-SBOX 1.16 Storing of record information**
The record information is written onto a storage medium which permits writing once only.

**Transmission security**

**S-SBOX 1.17 Secure transmission protocol**
A special transmission protocol is used for the communications link between the security box and the host computer, for the purposes of error detection and error rectification. This protocol also serves to detect the unauthorised renewed read-in of previously transmitted data.

**S-SBOX 1.18 Acknowledged receipt of data**
The security box contains a mechanism which provides the host computer with confirmation of the correct receipt of transmitted data.

**S-SBOX 1.19 Encoded data transmission**
The security box offers a facility for end-to-end encoding. The parameter required for decoding is subject to access control.

**S-SBOX 1.20 Use of serial numbers and time markers**
A time marker is assigned to the transmitted data, in order to verify the time authenticity of the transmitted data and thus to prevent interception and subsequent read-in. The insertion of additional messages and the substitution of transmitted data blocks are identified and/or prevented via the insertion of serial numbers.

**S-SBOX 1.21 Error-checking transmission protocol**
Responses to inquiries submitted to the time stamping and directory services are transmitted via a publicly accessible communications network. The employed transmission protocol guarantees that any manipulations or faults relating to the user data and protocol data are detectable at least. Further safeguards are proposed in Section 6.4 and Section 6.5.

**Integrity**

**S-SBOX 1.22 Detectability of changes relevant to security**
In order to render security-relevant changes to software and hardware components apparent, the security box possesses an integrated integrity protection system based on a cryptographic check-sum method (MAC). After production and assembly of the security box, once it has been verified and confirmed that the software and hardware components fulfil their functions without errors and in accordance with the specifications, the manufacturer calculates a MAC and incorporates this code into the security box. The algorithm and key for calculation of the MAC are also stored in the security box where, similarly to the MAC, they are subject to access control by the operating system. When the security box is called, or during the start-up phase of the security box, the MAC enables automatic determination of whether the components are operated in authentic mode with due integrity. To this end, the security box applies the algorithm with the key to the software or firmware and checks whether the result corresponds to the stored MAC. Any change will result in the security box switching to 'EMERGENCY STOP' state.

**S-SBOX 1.23 Verification of genuineness and non-manipulated state**
When the security box is operated on a terminal which is provided for commercial use for the purposes of signature generation or signature verification, the genuineness and non-

manipulated state of the terminal is verified via mutual authentication. In this connection, it is assumed that the keys required for authentication will be erased automatically in the event of manipulations on such a terminal.

**S-SBOX 1.24 IT-supported system time**

To enable verification of a time stamp or the validity of a signature key certificate, the security box possesses a trustworthy, IT-supported system time which enables ascertainment of the current time and date.

**S-SBOX 1.25 Individual serial number as proof of authenticity**

A serial number which is registered at the certification authority is incorporated in a special memory area within the security. This serial number cannot be altered or erased by the users. The structure of this serial number and the appurtenant calculation process permit the security box to provide proof of its authenticity by means of this number

**S-SBOX 1.26 Integrated voltage monitor**

An integrated voltage monitor ensures that certain relations between various data remain correct during a computing or processor operation, and that data are not loss in the course of their transmission.

**6.7.5.3.2 Security safeguards relating to the administrative environment**

**S-SBOX 2.1 Loading of the root and user certificate**

The root certificate can be loaded together with the user certificate in the course of personalisation of the security box.

**S-SBOX 2.2 Secure delivery procedure**

Arrangements are provided for reliable handover of the key parameters and authentication parameters and for a secure delivery procedure.

**S-SBOX 2.3 Access control in the operational zone**

The security box is located in an access-controlled operational zone. The authorised users obtain access to the operational zone only as necessary in direct connection with the discharging of their duties. The certification authority is to be notified immediately, in the event of loss of the security box.

**S-SBOX 2.4 Confirmation of conformity within the meaning of the Digital Signature Act**

The security box enables the certification authority to verify that the security box constitutes a suitable component within the meaning of the Digital Signature Act for the purposes of key generation and personal identification/authentication of the users. For this purpose, the security box possesses a serial number, which is calculated at the time of its manufacture and assembly, registered, and incorporated into its memory area. In the operational zone, the stored serial number can be called up and compared with the registered serial number. Should such a verification process reveal that the components concerned have not undergone ITSEC evaluation, this fact is clearly indicated to the user and recorded for the purpose of the preservation of evidence.

#### 6.7.5.3.3 Encoding security

**S-SBOX 3.1 Suitable signature process**

Only generally recognised mathematical algorithms and signature schemes which have been approved by the competent authority are employed for the purposes of signature generation and signature verification.

**S-SBOX 3.2 Suitable software and hardware components**

Only software and hardware components whose suitability has been established and confirmed by independent testing are incorporated into the security box.
Further safeguards are proposed in Section 6.1.

#### 6.7.5.3.4 Key management

**S-SBOX 4.1 Generation of (pseudo-) random numbers**

For the purpose of generating key data the security box possesses a random number generator whose random results are derived from a physical noise source, or a pseudo-random number generator based on a suitable mathematical algorithm, for example.

**S-SBOX 4.2 Secure key generation in the security box**

The calculation of signature keys is based exclusively on generally recognised mathematical algorithms and signature processes which have been approved by the competent authority.

**S-SBOX 4.3 Secure storage of the private signature key**

The private signature key is subject to access control by the operating system. After initial key generation and storage of the signature key by the operating system in the initialisation phase, there is no authorisation access for read-out, alteration or copying of the signature key.

**S-SBOX 4.4 Transport encoding**

When key generation is effected at the certification authority, supplementary encoding with a transport key provides protection against manipulation, malfunctions and disclosure during transfer of the private signature key to the security box.

**S-SBOX 4.5 Secure decommissioning of the security box**

When a non-secure operational state occurs or in the course of decommissioning of the security box, the private signature key is erased automatically. The implementation of a monitor in conjunction with an integrated voltage monitor ensures that this emergency erase function cannot be deactivated or bypassed.
Further safeguards are proposed in Section 6.2 and Section 6.3.

#### 6.7.5.3.5 Security safeguards to prevent the manipulation of software and hardware components

**S-SBOX 5.1 Active sensors and transducers**

For the purposes of monitoring the physical and mechanical characteristics and to provide protection against unauthorised opening of the security box while in operation, active sensors and transducers (e.g. temperature, light, touch, mechanical contacts, etc.) are installed.

**S-SBOX 5.2 Elimination of contacting possibilities**

In order to provide protection against unauthorised contacting of the electronic components, all unnecessary contacting possibilities are eliminated. Sealing the electronic components in a hard, non-conductive, opaque material would represent a passive mechanism to this end. The installation of a protection layer to prevent drilling through the security box, activation of which initiates erasure of the confidential keys, would represent an active mechanism.

**S-SBOX 5.3 User-initiated deactivation facility**

The security box possesses a deactivation function which permits the user to shut down operation of the security box temporarily.

**6.7.5.3.6 Fail-safe operation (safeguards in case of malfunctions and maloperation)**

**S-SBOX 6.1 Implementation of a state monitor**

The internal system and security status of the security box is displayed to the users and the external control process on the host at all times, and/or is made available for retrieval by the users and this process in the form of a data record. The central element here is the implementation of a state monitor, the state of which indicates the current phase in accordance with the life cycle of the security box. During operation, the state data provided by this monitor further indicate the current operational status - 'ON', 'OFF" or 'EMERGENCY STOP'.

**S-SBOX 6.2 User-friendly menu-assisted control system**

The two procedures 'Authentication' and 'PIN or password change' are carried out by means of a clearly structured and user-friendly menu-assisted control system which is controlled exclusively by the operating system. Deactivation or bypassing of these two procedures is actively prevented via the use of a reference monitor.

**6.7.5.3.7 Emanation security, prevention/attenuation of concealed channels**

**S-SBOX 7.1 Ensuring of neutral external behaviour**

In order to ensure that the external behaviour of the electromagnetic emanation from the security box, including its external interfaces, is neutral, i.e. that no information on private keys, identification parameters or any other confidential information can be inferred from any form of field measurements, data transmission via external interfaces is effected in encoded form. The security module is furthermore encapsulated in a metal housing and the housing is electromagnetically shielded.

**S-SBOX 7.2 Ensuring of secure current input**

Appropriate programming ensures that no conclusions which might pose a threat to security can be drawn by observing the time response. The power supply is designed such that the current input of the security box is virtually constant.

**8.7.5.3.8 Other functional requirements**

**S-SBOX 8.1 Use of time stamping and directory services**

The security box possesses a direct or indirect link to the time stamping service and the directory service.

### 6.7.5.4 Assignment of safeguards to solutions

| Safeguard | Counter-acts threat | Solution model | | | | | |
|---|---|---|---|---|---|---|---|
| | | Autonomous security box | | | Dedicated security box | | |
| | | Key generation variant | | | Key generation variant | | |
| | | 1 | 2a | 2b | 1 | 2a | 2b |
| S-SBOX 1.1 | 1 | req | req | req | req | req | req |
| S-SBOX 1.2 | 4 | req | req | req | req | req | req |
| S-SBOX 1.3 | 3 | req | req | req | req | req | req |
| S-SBOX 1.4 | 24 | rec | rec | rec | rec | rec | rec |
| S-SBOX 1.5 | 24 | rec | rec | rec | rec | rec | rec |
| S-SBOX 1.6 | 1 | rec | rec | rec | rec | rec | rec |
| S-SBOX 1.7 | ./. | rec | rec | rec | rec | rec | rec |
| S-SBOX 1.8 | 4,24 | req | req | req | req | req | req |
| S-SBOX 1.9 | 10,23 | req | req | req | req | req | req |
| S-SBOX 1.10 | 13,21 | rec | rec | rec | rec | rec | rec |
| S-SBOX 1.11 | 21 | req | req | req | req | req | req |
| S-SBOX 1.12 | 10 | req | req | req | req | req | req |
| S-SBOX 1.13 | 14 | req | req | req | req | req | req |
| S-SBOX 1.14 | ./. | rec | rec | rec | rec | rec | rec |
| S-SBOX 1.15 | 20 | rec | rec | rec | rec | rec | rec |
| S-SBOX 1.16 | 20 | rec | rec | rec | rec | rec | rec |
| S-SBOX 1.17 | 30,31 | rec | rec | rec | rec | rec | rec |
| S-SBOX 1.18 | 11 | rec | rec | rec | rec | rec | rec |
| S-SBOX 1.19 | 15,29 | rec | rec | rec | rec | rec | rec |
| S-SBOX 1.20 | ./. | rec | rec | rec | rec | rec | rec |
| S-SBOX 1.21 | 15,29 | rec | rec | rec | rec | rec | rec |
| S-SBOX 1.22 | 16 | req | req | req | req | req | req |
| S-SBOX 1.23 | 21 | req | req | req | req | req | req |
| S-SBOX 1.24 | 12 | rec | rec | rec | rec | rec | rec |
| S-SBOX 1.25 | 11,12 | req | req | req | req | req | req |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| S-SBOX 1.26 | 11,12,19 | req | req | req | req | req | req |
| S-SBOX 2.1 | ./. | rec | rec | rec | rec | rec | rec |
| S-SBOX 2.2 | ./. | rec | rec | rec | rec | rec | rec |
| S-SBOX 2.3 | 10 | req | req | req | req | req | req |
| S-SBOX 2.4 | ./. | req | ip | ip | req | ip | ip |
| S-SBOX 3.1 | 5,6,7,8 | req | req | req | req | req | req |
| S-SBOX 3.2 | 11,12 | req | req | req | req | req | req |
| S-SBOX 4.1 | 5,6 | req | nr | nr | req | nr | nr |
| S-SBOX 4.2 | 5,6 | req | nr | nr | req | nr | nr |
| S-SBOX 4.3 | 9,10 | req | req | req | req | req | req |
| S-SBOX 4.4 | 10,11 | nr | rec | req | nr | rec | req |
| S-SBOX 4.5 | 10 | rec | rec | rec | rec | rec | rec |
| S-SBOX 5.1 | 21 | req | req | req | req | req | req |
| S-SBOX 5.2 | 10 | rec | rec | rec | rec | rec | rec |
| S-SBOX 5.3 | ./. | rec | rec | rec | rec | rec | rec |
| S-SBOX 6.1 | ./. | rec | rec | rec | rec | rec | rec |
| S-SBOX 6.2 | ./. | rec | rec | rec | rec | rec | rec |
| S-SBOX 7.1 | 23 | req | req | req | req | req | req |
| S-SBOX 7.2 | ./. | req | req | req | req | req | req |
| S-SBOX 8.1 | ./. | rec | rec | rec | rec | rec | rec |

req = required, rec = recommended, ip = in part, nr = not required

#### 6.7.5.5 Allocation of the safeguards to the security requirements and recommendations

| Security requirement / Recommendation | Measures |
|---|---|
| REQ-SBOX 1.1 | S-SBOX 1.1, S-SBOX 1.2, S-SBOX 1.11 |
| REQ-SBOX 1.2 | S-SBOX 1.3 |
| REQ-SBOX 1.3 | S-SBOX 1.8, S-SBOX 1.9 |
| REQ-SBOX 1.4 | S-SBOX 1.12, S-SBOX 1.13 |
| REQ-SBOX 1.5 | S-SBOX 1.22, S-SBOX 1.25 |
| REQ-SBOX 1.6 | S-SBOX 1.23 |
| REQ-SBOX 2.1 | S-SBOX 2.3 |
| REQ-SBOX 2.2 | S-SBOX 2.4 |
| REQ-SBOX 3.1 | S-SBOX 3.1 |
| REQ-SBOX 3.2 | S-SBOX 1.26, S-SBOX 3.2 |
| REQ-SBOX 4.1 | S-SBOX 4.1, S-SBOX 4.2, S-SBOX 4.3, S-SBOX 4.4 |
| REQ-SBOX 4.2 | S-SBOX 4.3, S-SBOX 4.4 |
| REQ-SBOX 5.1 | S-SBOX 5.1 |
| REQ-SBOX 7.1 | S-SBOX 7.1, S-SBOX 7.2 |
| REC-SBOX 1.1 | N.N. |
| REC-SBOX 1.2 | S-SBOX 1.3 |
| REC-SBOX 1.3 | S-SBOX 1.4, S-SBOX 1.5 |
| REC-SBOX 1.4 | S-SBOX 1.6 |
| REC-SBOX 1.5 | S-SBOX 1.7 |
| REC-SBOX 1.6 | S-SBOX 1.10 |
| REC-SBOX 1.7 | S-SBOX 1.14, S-SBOX 1.15, S-SBOX 1.16 |
| REC-SBOX 1.8 | S-SBOX 1.17, S-SBOX 1.18, S-SBOX 1.19, S-SBOX 1.20, S-SBOX 1.21 |
| REC-SBOX 1.9 | S-SBOX 1.24 |
| REC-SBOX 2.1 | S-SBOX 2.1 |
| REC-SBOX 2.2 | S-SBOX 2.2 |
| REC-SBOX 4.1 | S-SBOX 4.5 |
| REC-SBOX 5.1 | S-SBOX 5.2 |

| | |
|---|---|
| REC-SBOX 5.2 | S-SBOX 5.3 |
| REC-SBOX 6.1 | S-SBOX 6.1 |
| REC-SBOX 6.2 | S-SBOX 6.2 |
| REC-SBOX 8.1 | S-SBOX 8.1 |

### 6.7.6 Other signature components

No further signature components have been considered to date.

## Literature

[ISO 7810] Identification cards - Physical characteristics, ISO IS 1995

[ISO 7813] Identification cards - Financial transaction cards, ISO IS 1995

[ISO 7816-1] Identification cards - Integrated circuit(s) cards with contacts - Part 1: Physical characteristics, ISO IS 1995

[ISO 10373] Identification cards - Test methods, ISO/IEC IS 1993

# 7 Issuance of licences for certification authorities

In the context of the licensing of certification authorities, the Digital Signature Act and Digital Signature Ordinance include provisions for evaluations and confirmations to verify the required technical and organisational trustworthiness of the certification authorities. A summary of the relevant references from this legislation is followed by an overview of all the bodies concerned. The core element is Section 7.4, in which the licensing procedure for certification authorities is presented. This is followed by a discussion of the assessment and confirmation bodies for security concepts and technical components.

In all instances below, the term 'certification authority' is used within the meaning of the Digital Signature Act and the Digital Signature Ordinance. Certification authorities which issue security certificates in accordance with ITSEC are referred to as security certification authorities.

## 7.1 Requirements stipulated in the Act and the Ordinance

| Reference | Quotation | Interpretation |
|---|---|---|
| **§ 2 (2) SigG** | For the purposes of this Act "certification authority" shall mean 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 of this Act. | A certification authority is an institution which generates and issues certificates. |
| **§ 2 (3) SigG** | For the purposes of this Act "certificate" shall mean a digital certificate bearing a digital signature and pertaining to the assignment of a public signature key to a natural person (signature key certificate) or a separate digital certificate containing further information and clearly referring to a specific signature key certificate (attribute certificate). | A certificate is an intangible product via which a key pair is assigned to a natural person. |
| **§ 3 SigG** | The granting of licences, the issue of certificates used for the signing of certificates, and the monitoring of compliance with this Act and with the ordinance having the force of law pursuant to §16 are incumbent on the authority according to § 66 of the Telecommunications Act. | The licence to operate certification authorities is issued by the competent authority, which at the same time is also responsible for monitoring compliance with the appurtenant requirements. |

| | | |
|---|---|---|
| **§ 4 (1) SigG** | The operation of a certification authority shall require a licence from the competent authority. A licence shall be granted upon application. | The following are to be regarded as duties relating to the issuance of licences:<br>a) stipulation of the procedures for the issuance, transfer and revocation of a licence and of the procedure upon the cessation of approved activities,<br>b) stipulation of the duties of the certification authorities,<br>c) stipulation of measures for monitoring certification authorities (see also § 16 SigG). |
| **§ 4 (2) SigG** | A licence shall be denied when facts warrant the assumption that the applicant does not possess the reliability necessary to operate a certification authority, when the applicant does not furnish proof of the specialised knowledge required to operate a certification authority or when there is reason to believe that, upon starting operation, the other requirements pertaining to the operation of the certification authority as set out in this Act and in the ordinance having the force of law pursuant to §16 will not be met. | This obliges the applicant to furnish proof that the relevant requirements are met; in the absence of such proof, no licence can be granted. |
| **§ 4 (3) Sentence 1 SigG** | Whosoever as operator of a certification authority guarantees compliance with the legal provisions applicable to the operation of such an authority shall be deemed to possess the necessary reliability. | The scope of the required proof of reliability includes a guarantee that the authority will be operated in accordance with the requirements of the Act and the Ordinance.<br>This obliges the applicant:<br>a) to submit an organisational chart, details of financers, a description of the applied procedures and documentation of the legal form, and<br>b) to make adequate provisions to ensure trustworthiness at all levels of the organisation. |

| | | |
|---|---|---|
| **§ 4 (3) Sentence 2 SigG** | The required specialised knowledge shall be deemed available when the persons engaged in the operation of the certification authority have the necessary knowledge, experience and skills. | The scope of required specialised knowledge extends to the legal and technical/administrative area.<br>This obliges the applicant:<br>a) to deploy competent personnel, and<br>b) to present details of the qualifications, training and professional experience of the employees, including clearly documented instructions for the personnel. |
| **§ 4 (3) Sentence 3 SigG** | The other requirements pertaining to the operation of the certification authority shall be deemed met when the competent authority has been notified in a timely manner by means of a security concept of the measures ensuring compliance with the security requirements in this Act and the ordinance having the force of law pursuant to §16 and their implementation has been checked and confirmed by a body recognised by the competent authority. | The scope of proof to be furnished for the other requirements covers the entire security infrastructure with regard to its suitability and effectiveness in fulfilling the security requirements.<br>This obliges the applicant to furnish proof that the certification authority will commence operation in a secure state and will maintain this state. |
| **§ 4 (4) SigG** | Collateral clauses may be attached to a licence where necessary to ensure compliance by the certification authority with the requirements in this Act and in the ordinance having the force of law pursuant to §16 upon starting operation and thereafter. | This enables the regulatory authority to require appropriate corrective measures and to monitor their implementation. |

| | | |
|---|---|---|
| **Explanatory note on § 4 / § 4 (1-4) SigG** | The certification service is to be provided by private companies in open competition, under official supervision [...]. The provisions are largely concordant with the provisions to this effect contained in the Telecommunications Act regarding the operation of telecommunications systems (cf. § 71 and § 91 TKG).<br><br>Issuance of the licence is to be carried out according to a process similar to that stipulated in the TKG [...]. The Administrative Procedures Act shall also apply. The licence applies specifically to the proprietor of the certification authority (there is no provision for transfer, assignment or the passing of the licence to another person in any other manner).<br><br>The issuance of certificates for signature keys is to require an official government licence, the issuance of which is subject to fulfilment of the requirements stipulated in Sentence 2.<br><br>Collateral provisions may be imposed, for example, to stipulate that the certification authority shall be permitted to commence operation only upon receipt of due approval from the competent authority, after the latter has evaluated the security concept and assessed the check report. | The licensing procedure is to be carried out as an administrative act. The licence is granted after verification of fulfilment of the licence preconditions; the consent of the competent authority is required, prior to the commencement of operations. |
| **§ 10 SigG** | The certification authority shall document the security measures for compliance with this Act and the ordinance having the force of law pursuant to §16 and the certificates issued in a manner such that the data and their integrity can be verified at all times. | This means that a system is required for monitoring the entire documentation of the certification system, together with a recording system for the purpose of the preservation of evidence and to maintain records of all activities over an appropriate period. |
| **Explanatory note on § 10 SigG** | Documentation of the security safeguards is intended above all to help ensure that effective controls are implemented and [...] that any breaches of duty can be established. | The form and content of the documentation must be appropriate for the purposes of examination and review; in particular, the competent authority should stipulate all the procedures required to carry out controls and provide the necessary resources. |

| | | |
|---|---|---|
| **§ 14 (4) SigG** | Technical components according to § 14 (1) to (3) above shall be adequately tested against current engineering standards and their compliance with requirements confirmed by a body recognised by the competent authority. | To this end it requires to be established which procedures are to be deemed adequate and in accordance with current engineering standards with regard to the evaluation and confirmation of technical components. |
| **Explanatory note on § 14 (4) SigG** | The most prominent body for confirming the security of technical components is the BSI. In accordance with the law regulating the establishment of the BSI ('BSI-Errichtungsgesetz'), the BSI has a mandate to evaluate the security of IT components and to issue security certificates.<br><br>The BSI is not granted a monopoly in this area, however. In addition to the BSI, the competent authority may also recognise other bodies, provided that the security certificates (or other forms of confirmation) issued by these bodies establish the required standard of security. | This requires stipulation of the conditions which the evaluating and confirmation bodies are required to fulfil.<br><br>This requires stipulation of the terms of reference for evaluation and confirmation and a procedure for the recognition (by the regulatory authority) of evaluating and confirming bodies for technical components. |

| | | |
|---|---|---|
| **§ 14 (5) SigG** | Technical components lawfully manufactured or placed on the market in accordance with regulations or requirements in force in another Member State of the European Union or [...] which ensure the same level of security shall be assumed to fulfil the technical security requirements according to § 14 (1) to (3) above.<br><br>In a given justified instance and at the request of the competent authority proof shall be furnished of compliance with the requirements according to sentence 1 above. Insofar as presentation of a confirmation by a body recognised by the competent authority is required as evidence of compliance with the technical security requirements within the meaning of § 14 (1) to (3) above, confirmations by bodies licensed in other Member States of the European Union or other States parties to the Agreement on the European Economic Area shall also be accepted if the technical requirements, tests and test procedures on which the test reports of these bodies are based are deemed equivalent to those of the bodies recognised by the competent authority. | In this connection it is to be established which regulations ensure the same level of security with regard to the relevant technical requirements, tests and evaluation procedure for technical components. |
| **Explanatory note on § 14 (5) SigG** | Products and recognised product evaluations within the meaning of Subsection 4 from the stated European states are hereby accorded equal status. | In this connection it is to be established which regulations ensure the same level of security with regard to products and product evaluations. |
| **§ 15 (1) SigG** | Digital signatures capable of being verified by a public signature key certified in another Member State of the European Union or in another State party to the Agreement on the European Economic Area shall be deemed equivalent to digital signatures under this Act insofar as they show the same level of security. | This requires stipulation of the basic terms of reference for the operation of certification authorities and of the licensing procedure for certification authorities (by the regulatory authority). |
| **Explanatory note on § 15 (1) SigG** | This provision accords equal status to digital signatures from the stated European states, provided that they ensure a comparable level of security. | In this connection, it requires to be established which regulations ensure a comparable level of security with regard to digital signatures and certification authorities |

| | | |
|---|---|---|
| **§ 1 (1) SigV** | Licenses for the operation of a certification authority pursuant to §4 (1) of the Digital Signature Act must be applied for in writing; such applications must be submitted to the competent authority. | This requires stipulation of the form and content of the application and the official notification, specification of the licensing procedure and regulation of the decision-making process for licences. |
| **Explanatory note on § 1 (1) SigV** | The written form of application provides a sound legal basis for all parties involved. | |
| **§ 1 (2) SigV** | The competent authority shall obtain the information necessary to determine if the applicant fulfils prerequisites for issuance of a license. It can require the applicant to submit necessary documents, especially a current extract from the commercial register and current certificates of good conduct pursuant to § 30 (5) of the Federal Central Register Act ('Bundeszentralregistergesetz') for the legal representatives of the certification authority.<br><br>To permit determination of whether the applicant possesses the necessary specialised knowledge, the applicant must prove that personnel involved in the certification procedure or in issuing time stamps have the necessary professional qualifications. | This requires the competent authority to stipulate the prerequisites to be fulfilled in applications, to verify the completeness of the application and to stipulate the preconditions for the granting of licences. |
| **Explanatory note on § 1 (2) SigV** | Sentence 2 is intended to oblige the applicant to submit the necessary documents. The competent authority may additionally obtain information from third parties. A certification authority requires legal and IT expertise, in order to fulfil the requirements stipulated in the Act and the Ordinance in a proper manner. Strict standards are to be applied here. Should the certification authority commission third parties to discharge part of its scope of duties, this shall not detract from its overall responsibility. | |
| **§ 1 (3) SigV** | Before rejecting, withdrawing or revoking a license, the competent authority shall hear the applicant and give him the opportunity to eliminate the reasons for the rejection, withdrawal or revocation. | This requires the competent authority to specify the complaints procedure. |

| | | |
|---|---|---|
| **Explanatory note on § 1 (3) SigV** | By way of derogation from the Administrative Procedures Act, the applicant is to be heard in all cases in order to exclude the possibility of incorrect decisions, in view of the sometimes complex organisational and technical facts and circumstances. | |
| **§ 10 SigV** | The certification authority shall reliably establish the reliability of persons involved in the certification procedure or in issuing time stamps. In particular, it may require presentation of a certificates of good conduct pursuant to § 30 (1) of the Federal Central Register Act. Unreliable people shall be excluded from the certification procedure and from issuance of time stamps. | This requires stipulation of the requirements regarding reliability. |
| **§ 12 (1) SigV** | The security concept pursuant to § 4 (3) Sentence 3 of the Digital Signature Act shall include all security measures and, especially, an overview of the technical components used and a description of the procedures used in certification.<br>The concept shall be changed without delay in cases of security-relevant changes. | This requires the competent authority to stipulate the requirements relating to the form and content of the security concept. |
| **Explanatory note on § 12 (1) SigV** | The security concept is intended to provide a comprehensive overview of the certification authority's security safeguards. If, in addition to the obligatory services, the certification authority also offers additional services in connection with digital signatures on a contractual basis [...], these should be included in the security concept. The security concept includes a description of the specific threats and risks which apply to the certification authority. | |
| **§ 13 (1) Sentence 1 SigV** | The documentation pursuant to § 10 of the Digital Signature Act shall include the security concept, including the changes, the check reports and confirmations pursuant to § 15 (1), the contractual agreements with the applicants and the certificates received by the competent authority. | |

| | | |
|---|---|---|
| **§ 15 (1) SigV** | Before beginning its operation, following security-relevant changes and at regular two-year intervals, the certification authority shall arrange for checks pursuant to § 4 (3) Sentence 3 of the Digital Signature Act and shall submit to the competent authority a relevant check report and confirmation showing that it fulfils the provisions of the Digital Signature Act and this Ordinance. | This requires stipulation of the arrangements which are to be adopted with regard to the evaluation and confirmation of security concepts; in particular, it is to be stipulated how the security relevance of changes is to be established. |
| **Explanatory note on § 15 (1) SigV** | The selection and recognition of the bodies is carried out on the basis of technical aspects, according to requirements and the best judgement of the regulatory authority. In accordance with § 4 (3) Sentence 3 of the Digital Signature Act, checks and confirmations require proof of practical experience in the field of administrative and technical security (furnishing of references) and one or more successful checks in accordance with Subsection 1 under the technical supervision of the competent authority and with the involvement of the BSI. In accordance with DIN EN 45000 ff. the evaluation and the confirmation are to be carried out by two mutually independent bodies. The evaluation and confirmation bodies require to be recognised by the competent authority. The BSI is the most prominent recognised body here. Other evaluation and confirmation bodies may also perform this function, however. | This requires stipulation of the conditions which the evaluation and confirmation bodies for security concepts are required to fulfil.<br>This requires stipulation of the terms of reference for evaluation and confirmation and the procedure for recognition (by the regulatory authority) of the evaluation and confirmation bodies. |
| **§ 15 (2) SigV** | The competent authority can carry out checks at appropriate intervals, and whenever there are reasons to suspect violations of provisions of the Digital Signature Act or of this Ordinance. | This requires the competent authority to stipulate the frequency and scope of the checks internally. |

| | | |
|---|---|---|
| **§ 17 (3) Sentence 3 SigV** | If this authority has reason to suspect there are deficiencies in testing or in confirmed technical components, the authority may obtain an expert opinion from an independent third party to determine if the technical components were tested pursuant to (1) and whether the technical components fulfil the requirements of the Digital Signature Act and this Ordinance. | This requires stipulation of the procedure for obtaining expert opinions on technical components and of the arrangements for and consequences of deficiencies. |
| **§ 17 (4) SigV** | The competent authority shall publish, in the Federal Gazette, a list of agencies pursuant to § 14 (4) of the Digital Signature Act as well as a list of technical components that have received confirmation by such agencies pursuant to (3); the competent authority shall provide this list directly to the certification authorities. Note must be made, for all technical components, of the date until which the confirmation is valid. If a certification is revoked or a confirmation declared invalid, notice of such actions shall also be published in the Federal Gazette and communicated directly to the certification authorities. | This requires stipulation of the procedure which is to be adopted in the case of a licence being revoked or a confirmation being declared invalid. |
| **Explanatory note on § 17 (4) SigV** | At least two private (security-certifying) bodies are to be recognised which are authorised to confirm the compliance of technical components with legal requirements in accordance with § 14 (4) of the Digital Signature Act. | In this connection it is to be established how security-certifying bodies and confirmation bodies differ from one another, and how this difference is manifested in terms of operational procedures. |

## 7.2 Roles, functions, authorisation and responsibility

The diagram overleaf illustrates the roles and processes in the context of the Digital Signature Act and the Digital Signature Ordinance. The table below shows the allocation of roles to actual organisational units, institutions and persons as stipulated in the Act and the Ordinance.

| Roles | Functions | Responsibilities in accordance with SigG/V (including explanatory notes) |
|---|---|---|
| CO | Issuing of licences, issuing of certificates, monitoring of compliance with SigG/V | Regulatory authority in accordance with § 66 TKG (functions performed by the Federal Post and Telecommunications Ministry (BMPT) up to 1st January 1998). |
| CA | Certification of the assignment of public signature keys to natural persons | Certification authority within the meaning of SigG |
| ABS | Assessment of the safeguards specified in the security concept and their implementation | Independent, private body recognised by the competent authority |
| CBS | Confirmation of fulfilment of the security requirements of the Act and the Ordinance | Body which is recognised by the competent authority and independent of the assessing body |
| EBT | Adequate evaluation in accordance with current engineering standards on the basis of ITSEC | |
| CBT | Confirmation of compliance with requirements | (Security-certifying) body recognised by the competent authority |

Table: Assignment of roles and functions

The following subjects are defined:

CO = Competent authority

CA = Certification authority within the meaning of SigG/V

ABS = Assessment body for security concepts

CBS = Confirmation body for security concepts

EBT= Evaluation body for technical components

CBT = Confirmation body for technical components

The following objects are defined:

SC = Security concept

TC = Technical components

RE = Reliability and expertise

The following processes are defined:

| | |
|---|---|
| A_CA = | Process for the licensing of certification authorities |
| A_PSS = | Recognition of assessment bodies for security concepts |
| A_BSS = | Recognition of confirmation bodies for security concepts |
| A_PSK = | Recognition of evaluation bodies for technical components |
| A_BSK = | Recognition of confirmation bodies for technical components |
| P_S = | Assessment of security concepts |
| B_S = | Confirmation of security concepts |
| P_K = | Evaluation of technical components |
| B_K = | Confirmation of technical components |

The functions, authorisation and responsibility for the specific roles in the context of the Digital Signature Act and Ordinance are defined in the descriptions of the individual processes.

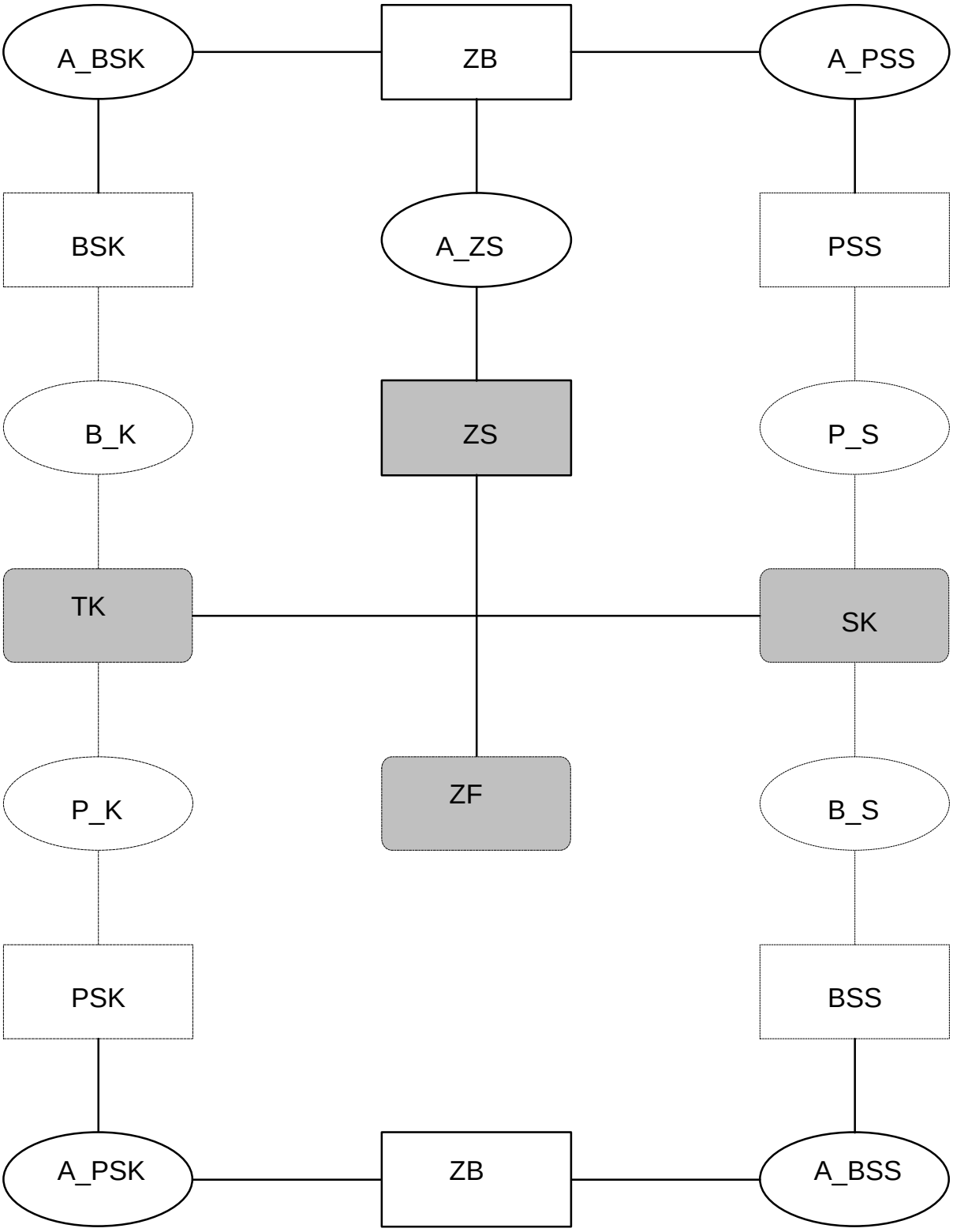



Fig.: Roles and procedures in the context of the Digital Signature Act and Ordinance

In the following sections, the term 'appraisal' is employed to describe the processes of 'assessment', 'evaluation' and 'confirmation'. The term 'appraisors' thus refers to those parties performing these tasks, irrespective of whether this role is ultimately performed by natural persons (independent experts) or organisational units (accredited testing laboratories).

## 7.3 Trustworthiness of certification authorities

Apart from the legal quality of digital signatures, a further essential aspect is the trustworthiness of those authorities which are responsible for generating, issuing and administrating the signature key certificates. Special attention is thus to be accorded to verification of the technical, organisational and personnel situation within these institutions, which are designated 'certification authorities' in the Digital Signature Act. In order to take due account of the necessary legally binding effect and security of digital signatures, verification is to focus both on the basic methods, technologies and tools and on the know-how of the appraisors. The users´ confidence in the digital signature processes is dependent to a decisive extent on the quality and security offered by the certification authorities. Consequently, the organisational requirements are to be considered, in addition to the technical requirements.

The trustworthiness of certification authorities (including the competent authority) is based on:

- confidence in the organisation and organisational arrangements,
- the quality of the operations, processes and practices, which are defined, implemented and carried out in the correct manner (in both organisational and technical terms),
- conformity with accepted standards and applicable legal requirements,
- a legally binding contract between the customer and the certification authority,
- an assessed and approved security policy/security concept (presentation and implementation of safeguards - consistency of administrative, organisational and technical requirements), and
- trustworthy operation of a certification authority and transparent arrangements to verify trustworthy operation.

The following principles are to be applied to all evaluating, confirming and operational activities. The degree to which these principles are fulfilled can thus serve as a measure of the trustworthiness of the overall security environment:

- homogeneity at all levels via comparability, equal status, repeatability, reproducibility,
- reliability through impartiality, objectivity, qualification, know-how,
- transparency through comprehensibility, traceability, verifiability,
- independence via the involvement of neutral authorities, and
- standardisation via the application of recognised standards and practices.

## 7.4 Licensing procedure for certification authorities

### 7.4.1 Intended objective

§ 4 (2) and (3) SigG stipulate the following prerequisites for the issuing and maintenance of a licence for certification authorities:

a) possession of the required reliability, i.e. compliance with the relevant legal requirements,

b) possession of the required specialised knowledge, i.e. the knowledge, experience and skills of the deployed personnel, and

c) fulfilment of the other requirements pertaining to operation, i.e. stipulation of the measures to ensure compliance with the security requirements of the Digital Signature Act and the Ordinance having the force of law pursuant to § 16, and verification and confirmation of their due implementation by a body recognised by the competent authority.

In accordance with § 16 SigG, the ordinance having the force of law sets out the legal provisions required for implementation of §§ 3 to 15 SigG, together with further details of the procedures relating to the granting, withdrawal and revocation of a licence and the procedure upon cessation of approved operation. In particular, the obligations of the certification authorities and the control and monitoring procedures for certification authorities are stipulated in further detail.

### 7.4.2 Subject matter

In accordance with § 4 (2) SigG, the issuance of a licence to operate a certification authority requires proof firstly of the necessary reliability and specialised knowledge and secondly of fulfilment of the security requirements (i.e. a security concept, in particular an overview of the deployed technical components and a presentation of the organisational structure for certification activities).

In order to verify the required reliability and specialised knowledge, the general requirements pertaining to operation of a certification authority are appraised. This appraisal is generally carried out on the basis of the DIN EN 45000 series of standards, by reference to a catalogue of questions for the assessment of certification authorities. The catalogue of questions is based on Section 6-10 and 12-16 of DIN EN 45011, 'General criteria for bodies which certify products' [DIN 45011]. In connection with appraisal of the security concept (including its implementation), verification can be carried out by a body which is recognised for this purpose. The security concept is appraised in order to verify the fulfilment of security requirements as stipulated in the Act and the Ordinance. This appraisal is carried out on the basis of the safeguard catalogue in accordance with § 12 (2) SigV.

### 7.4.3 Description of procedure and actions involved

The licensing procedure for certification authorities which, in the case of a positive conclusion, ends with the issuing of the licence to operate certification authorities, is based on the standard accreditation procedures in which independent experts are appointed to carry out the appraisal work. Similarly to practices in the area of accreditation, a form of steering committee should be set up, to which the competent authority is able to appoint competent representatives of groups which have a particular interest in the licensing proceedings. The licensing procedure is divided into four phases: application, appraisal, granting of the licence and monitoring.

#### 7.4.3.1 Application

The application phase comprises:

1. submission of initial inquiry to the regulatory authority,
2. preliminary meeting,
3. application for a licence,
4. confirmation of the application, and
5. verification of completeness of application.

Applications for licences to operate certification authorities are to be submitted in writing in the German language to the competent authority

The scope of information required in connection with applications includes the following:

- name and address of the organisation applying for the licence,
- name of a contact who is authorised to represent the applicant,
- legal form and/or status of the certification authority within the organisation,
- shareholdings,
- organisational structure and main activities, organisational chart for the certification authority,
- extract from the commercial directory (management and authorised signatories),
- police clearance for the certification authority's legal representatives,
- details of the intended date for the commencement of operation,
- written undertaking by the certification authority to comply with its obligations,
- relevant offences (e.g. fraud or embezzlement), and
- general terms of business.

Granting of the licence is subject to specific conditions which the applicant is required to fulfil. In particular, these conditions include reliability and specialised knowledge and fulfilment of the security requirements imposed by the Digital Signature Act and Digital Signature Ordinance. In order to furnish proof of reliability, the applicant must specify the framework which is in place to ensure compliance with the relevant legal requirements. In order to furnish proof of the required specialised knowledge, the applicant must specify the knowledge, experience and skills which the personnel intended for operation of the certification authority possesses and the previous activities of the certification authority's operators. In order to furnish proof of compliance with the other requirements, the applicant must specify the measures to fulfil the security requirements in an assessed and confirmed security concept.

To enable the granting of a licence, proof of the following must be furnished:

- proof of reliability (insurance, protection against fire and burglary, emanation and tapping security, specimen contract for certificate, information from general credit protection agency, security verification for personnel, ...),

- proof of specialised knowledge (qualifications profile, ...), and
- proof of fulfilment of other requirements (security concept, in particular with overview of deployed technical components and presentation of organisational structure).

In accordance with § 3 SigG, the competent authority is the body which is stipulated in accordance with § 66 of the Telecommunications Act. The explanatory note on § 4 SigG points out that the licence applies specifically to the operator (synonymous with the proprietor of the certification authority), and that no provision exists for any form of transfer or assignment of the licence to a person other than the operator. In such cases, a new licence application is to be submitted in good time. The competent authority assesses compliance with the requirements for issuing of the licence on the basis of the complete documentation with which it has been furnished.

#### 7.4.3.2 Appraisal procedure

The appraisal phase comprises:

1. selection and appointment of the appraisors,
2. appraisal
   a) of reliability and specialised knowledge and
   b) of the security concept, and
3. drafting of the appraisal report.

In principle, two scenarios are possible for the appraisal procedure. The first scenario involves the appointment of the appraisors for all appraisals in the course of the licensing procedure, under the overall control of the competent authority. In the second scenario, appraisal of the security concept is separated from the licensing procedure. These scenarios differ in that in the first scenario the security concept is appraised during the licensing procedure, while in the second the security concept has already been appraised at the time of application.

§ 4 (3) SigG requires the certification authority to specify the measures which it intends to implement in order to fulfil the security requirements imposed by the competent authority in a security concept, § 15 (2) SigV requires the certification authority to arrange for checks to be carried out and to provide the competent authority with a check report and confirmation of compliance with the requirements of the Digital Signature Act and the Digital Signature Ordinance. The second scenario is to be preferred, as it enables the smooth and efficient processing of applications. The contents of the two scenarios are as follows:

**Scenario ZS_1:**
Appointment of all appraisors by CO - Appraisal of the security concept in the course of the licensing procedure - Submission of the security concept at the time of application and check report/confirmation on granting of the licence.

**Scenario ZS_2:**
**Appointment of the appraisors to appraise the security concept by the CO - Appraisal of the security concept separately from the licensing procedure - Submission of security concept and check report/confirmation at time of application**

The explanatory note on § 4 (1-4) SigG points out that proof of fulfilment of the other requirements should be furnished via a security concept and due assessment of this concept by an independent assessment body. The explanatory note on § 15 (1) SigV points out that assessment and confirmation are to be carried out by two mutually independent bodies which are recognised by the competent authority. Both activities are carried out by qualified, competent and independent experts (so-called appraisors), for the recognition (so-called appointment) of whom the competent authority is responsible. The results of the appraisal are to be set out in writing in a report (which may consist of several individual appraisals relating to specific areas), the layout and structure of which is stipulated by the competent authority. This report serves the competent authority as a basis on which to assess fulfilment of the necessary requirements for granting of the licence.

#### 7.4.3.3 Granting of the licence

The license granting phase comprises:

1. assessment of the appraisal results and decision on the granting of a licence,
2. drafting of formal notification, and
3. publication in the register.

In principle, there are two possible results with regard to granting of the licence; the decision on the licence can be positive (initial licence or relicensing) or negative (rejection of licence, withdrawal of the licence, revocation of the licence, prohibition of operations). In both cases, an invoice is made out and appropriate notification is furnished

The competent authority is responsible for the issuing of licences for certification authorities located within its administrative region. For this purpose, the competent authority may establish a committee, referred to below as the expert committee. The appraisal results and any statements provided by the certification authority are submitted to this committee for a recommendation as to whether the licence should be granted or declined. The final decision lies with the competent authority.

Representatives to meet the requirement for public monitoring, such as data protection commissioners, may be appointed to the expert committee where appropriate, at the discretion of the competent authority. The explanatory note on § 12 (2) SigV points out that the competent authority is responsible for maintaining and publishing the catalogue of suitable security safeguards which are to receive due consideration when drafting the security concept. The requirement for measures which differ from the safeguard catalogue to be possible only on condition that it is established that the alternative solutions provide a comparable level of security can be met by appointing a representative of the competent authority to the committee. The need to keep the safeguard catalogue up to date can also be satisfied in this manner.

#### 7.4.3.3.1 Negative decision

The explanatory note on § 1 (3) SigV points out that, by way of derogation from § 28 (2/3) of the Administrative Procedures Act, the certification authority which has applied for a licence must always be heard when a licence being refused or revoked. The competent authority is to provide the certification authority applying for the licence with an opportunity to eliminate the reasons for the refusal or revocation and to initiate corrective measures.

In accordance with § 13 SigG the competent authority may, in particular, temporarily prohibit the use of unsuitable technical components and performance of the approved activities either wholly or in part. After completion of the corrective measures a reappraisal is carried out - if possible by the originally involved appraisors - and the appraisal report is again submitted to the expert committee. The certification authority is prohibited from carrying out its activities during this time. Failure to eliminate the inadequacies will result in complete withdrawal of the licence and is to published immediately in the certificate directory and/or the revocation list. The certification authority concerned is to undertake all the measures stipulated in its specified revocation management system. In accordance with § 13 (5) SigG, this does not affect the validity of the certificates issued by the certification authority; under certain circumstances, however, the competent authority may order the revocation of certificates. In case of withdrawal (corresponding to the cessation of activities) and revocation (corresponding to revocation of the certificates issued by the competent authority), the certification authority is to proceed as stipulated in the security concept. A new application may be submitted after 6 months at the earliest.

#### 7.4.3.3.2 Positive decision

The licence to operate certification authorities is certified in accordance with the official notification after receipt of the amount invoiced to the operator (fees and expenses).

The information in the official notification must include the following:

- date of the application,
- subject of the licence,
- duration,
- revocation of the licence,
- notification requirements,
- data protection,
- collateral provisions (stipulation of appropriate measures to be undertaken prior to commencing operations),
- obligations to notify and report to the competent authority,
- obligations to furnish information,
- advice on applicable legal remedies,
- termination, and
- other applicable enclosures.

#### 7.4.3.4 Monitoring

The monitoring of recognised certification authorities and the extension of licences are carried out in accordance with the arrangements and regulations of the competent authority.

Essentially, two aspects are subject to monitoring requirements: Firstly, the security concept and its implementation are to be monitored in the course of the routine comprehensive assessments. Secondly, compliance with the Digital Signature Act and Ordinance is to be monitored in the course of the supplementary random checks.

The explanatory note on § 4 SigG points out that the routine assessments of the certification authorities are to be carried out by private institutions, while the checks to be carried out on a random basis (at appropriate intervals) or when due cause arises (in case of suspected failure to comply with the Digital Signature Act or Ordinance) may be carried out by the competent authority itself.

##### 7.4.3.4.1 Security concept

The security concept on the basis of which the licence has been granted is to be appraised at a regular interval of two years or after any changes which are of relevance to security, by means of renewed assessment and confirmation. In both cases, the security concept is to be submitted to the competent authority without delay, together with the check report and the confirmation. In accordance with § 4 (6) SigG, the costs are to be borne directly by the party initiating the appraisal. The procedure is identical to that which applies to appraisal of the security concept (examination of documentation and on-site inspection) prior to the commencement of operations. Change management for the security concept is to be organised in a manner corresponding to standard practices in the area of quality management. Each change to the security concept or its implementation is reported to the person who appraised the currently valid security concept. This person decides on the relevance of the change - in cases of doubt in consultation with the competent authority - and either takes direct action or defers action until the next routine appraisal. The decision, which is reached according to the appraisor´s best judgement, is to be documented, added to the security concept and duly taken into account in the course of the next monitoring check.

##### 7.4.3.4.2 Verification of compliance with the Act and the Ordinance

The preconditions applying to issuance of the licence are to be monitored on a random basis and when appropriate grounds arise, and measures are to be undertaken to ensure compliance with the Act and the Ordinance. In this connection it is essential that the certification authority meet its obligation to notify the competent authority of every change (technical, organisational, legal, personnel-related, structural).

In order to enable repeat verification of the deployed technical components, § 17 (3) SigV requires the certification authority to submit a copy of the check report and the confirmation for the deployed technical components to the competent authority. The competent authority may obtain an expert opinion from an independent third party as to whether the technical components have been evaluated in accordance with § 14 (4) SigG and/or § 17 (1) and whether these components fulfil the requirements of the Act and the Ordinance on a random basis and when there are grounds to suspect deficiencies.

### 7.4.4 Parties involved

| Functions | Activities | Responsibility |
|---|---|---|
| Issuing of a licence | Implementation of the licensing procedure and establishment of the required decision | Staff of the competent authority |
| Monitoring of compliance with SigG/SigV | Routine assessments | Appraisor |
| Monitoring of compliance with SigG/SigV | Checks | Staff of the competent authority (this work may be delegated to independent third parties) |
| Appraisal of the certification authority | Appraisal of reliability and specialised knowledge | Staff of the competent authority (this work may be delegated to independent third parties) |
| Appraisal of the certification authority | Appraisal of the security concept | Appraisor |

### 7.4.5 Obligations of and control measures for certification authorities

In view of the possible affects on the basic rights of third parties or the interests of the general public, the state is to ensure that it possesses an adequate scope of control and action to meet its responsibilities. With regard to the services of the certification authority, which are to be provided in open competition under official supervision, additional aspects require to be considered, apart from the obligations and control measures for certification authorities which are stipulated in the Act and the Ordinance.

The following are to be regarded as **obligations** of the certification authority:

- reliable identification of users, confirmation of the unique assignment of signature keys to individuals, verifiable and retrievable certificates (in accordance with § 5 (1) SigG),
- ensuring of the integrity of certificate-related data and the confidentiality of private signature keys (in accordance with § 5 (4) SigG),
- deployment of reliable personnel and suitable technical components in accordance with § 14 SigG for the issuance of certificates and time stamps (in accordance with § SigG and § 9 SigG),
- obligation to notify users of requirements and necessary measures (in accordance with § 6 SigG),

- ensuring of the integrity and availability of the documentation on the security concept (including changes and check reports) and of certificates (in accordance with § 10 SigG), and
- documentation on information furnished to competent bodies (in accordance with § 12 SigG).

Other relevant aspects may include:

- contractual arrangement between customer and certification authority, and
- stipulation of liability arrangements.

In order to safeguard the rights of intervention granted to the competent authority by virtue of § 13 (1) and (2) SigG, the corresponding arrangements are to be documented by the certification authority. This may take the form of procedural instructions for revocation/withdrawal of the licence, prohibition/cessation of certification activities and the revocation of certificates by the competent authority.

The following are to be regarded as **control measures** for the certification authority:

- prohibition of the use of unsuitable technical components and prohibition of execution of the approved activity (in accordance with § 13 (1) SigG),
- entering the operating and business premises during normal operating hours, presentation for inspection of relevant books, records, receipts, documents and other papers, furnishing of information and granting of support (in accordance with § 13 (2) SigG),
- withdrawal of the licence (in accordance with § 13 (3) SigG),
- ordering of the revocation of certificates (in accordance with § 13 (5) SigG), and
- application of § 38 of the Federal Data Protection Act (BDSG), subject to the proviso that verification may also be carried out when there is no indication of a violation of data protection provisions (in accordance with § 12 SigG).

### 7.4.6 Summary

A distinction is to be drawn between the evaluation of information and communications technology and the assessment of management systems[23], with regard to both the applicable criteria and the appropriate methods. Consequently, these two evaluation processes require to be separated from each another. In the area of technical components, an established evaluation, certification and accreditation scheme is already available, while in the area of management systems a corresponding basis is required for objective and transparent assessments and confirmations. Conformity with legal requirements should always be taken into account at the specification stage for components and security concepts. Institutional separation is to be required between the operator of a certification authority and the evaluating / confirming body. In accordance with DIN EN 45000 ff. the evaluating body and the confirmation body are also to be separated from each other via organisational means.

[23]for definition see Section 7.5.5

## 7.5 Procedure for the recognition of assessment bodies and confirmation bodies for security concepts

### 7.5.1 Intended objective

The explanatory note on § 4 (1-4) SigG specifies proof of the necessary specialised knowledge and experience as a prerequisite for the recognition of assessment bodies to appraise security concepts, together with stipulations regarding implementation of the assessments. The explanatory note on § 15 (1) SigV expressly specifies proof of practical experience in the field of administrative and technical security as a prerequisite for assessments and confirmations. Beyond this, proof is to be furnished of the successful assessment of security concepts at least - under the technical supervision of the competent authority and with the involvement of the BSI. In accordance with DIN EN 45000 ff., assessment and confirmation are to be carried out by two mutually independent bodies, both of which require to be recognised by the competent authority.

In addition to the details of the recognition procedure,

- the methods to be applied in appraising security concepts and
- verification of the appraisor´s qualifications and competence

require special consideration.

### 7.5.2 Subject matter

To establish proof of the required specialised knowledge and experience, the appraisor´s technical qualifications are examined. This examination is carried out by means of a technical discussion to assess the standard of qualification and competence of the appraisor, who must also furnish appropriate references. As a general principle, these findings are to be made by the competent authority; this task may be delegated to the expert committee.

In order to verify compliance with specific requirements relating to the general working environment, the organisational requirements relating to the appraisor´s environment are examined. This examination is carried out by means of a catalogue of questions for the assessment of inspection bodies. The catalogue of questions is based on DIN EN 45004, 'General criteria for the operation of various types of bodies which carry out inspections' [DIN 45004]. As a general principle, these findings are to be made by the competent authority; this task may be delegated to the expert committee.

In particular, a knowledge of the Digital Signature Act and Ordinance and of the safeguard catalogue is to be verified.

The Federal Agency for Security in Information Technology represents a recognised body which may function as an assessment and confirmation body; other assessment and confirmation bodies are also possible, however.

### 7.5.3 Description of procedure and actions involved

#### 7.5.3.1 Assessment bodies

In principle, three scenarios are possible with regard to the recognition of assessment bodies for security concepts. The first scenario focuses on specific technical qualification requirements relating to the personnel, thus providing the competent authority with access to the personnel. The second scenario places the emphasis on specific organisational and technical requirements relating to the environment, which thus do not fall within the competent authority's scope of access.

As both of these scenarios harbour shortcomings when strictly applied - the first scenario does not take adequate account of the organisational and technical requirements pertaining to the processing of information which is of relevance to security, while the second scenario fails to address technical qualification requirements pertaining to the personnel to a satisfactory extent in connection with the assessment of security concepts - a combination of the two provides a recommendable recognition procedure. The required specialised knowledge and experience is ensured via the appointment of independent experts, and compliance with specific general conditions is stipulated as a precondition for the assessment process. Where expedient, there would be no obstacle to verification of the technical competence for appraising security concepts by means of catalogues of questions (which have yet to be developed) in the course of an accreditation process. The third scenario permits the appointment of external experts. The assignment of full responsibility for the decision on the appointed appraisors to the competent authority avoids the assignment of parts of the scope of responsibility to another (accreditation) body. It remains at the discretion of the regulatory authority whether this task is to be delegated to a third party.

**Scenario PSS_1:**
Pool of appraisors - personnel-related competence - appointment of appraisors

**Scenario PSS_2:**

Pool of assessment laboratories - organisation-related competence - accreditation of assessment laboratories

**Scenario PSS_3:**
**Combination of 1 and 2 - independent experts with specific conditions relating to the general environment - appointment of appraisors plus stipulation of preconditions for the assessment process**

#### 7.5.3.2 Confirmation bodies

In principle, two scenarios are possible with regard to the recognition of confirmation bodies for security concepts. The first scenario focuses on specific technical qualification requirements relating to the personnel, thus providing the competent authority with access to the personnel. The second scenario places the emphasis on specific organisational and technical requirements relating to the environment, which thus do not fall within the competent authority's scope of access.

**Scenario BSS_1:**
**Expert committee - personnel-related competence - appointment of members**

**Scenario BSS_2:**
Pool of certification authorities in accordance with DIN EN 45011 (in the field of the evaluation of security management systems) - organisation-related competence - accreditation of certification authorities in accordance with DIN EN 45011 (in the field of the evaluation of security management systems) with additional authorisation for confirmation in accordance with SigG/SigV

The first scenario meets the requirement stipulated in the Act for confirmation of the assessed security concept by a body which is independent of the assessment body, and is based on the standard auditing procedures for management systems. The second scenario bases recognition as a confirmation body on valid accreditation in accordance with DIN EN 45011, in the course of which proof of the required knowledge of the Digital Signature Act and Ordinance and the safeguard catalogue is also to be furnished. The first scenario is to be recommended, as it provides the greatest possible degree of transparency for this licensing procedure which forms the focus of public attention, avoids excessive regulation and ensures commensurability with requirements in that the establishment of an accreditation procedure for a small number of bodies is not initially necessary (see also Section 7.4.3.3).

#### 7.5.3.3 Recognition

The appointment of appraisors taking special account of specific conditions relating to the general environment is carried out for the specialised areas specified in the appurtenant applications, and is divided into three phases: preparation, appointment and decision.

1. **Preparatory phase for appointments**

- Application for appointment
- Confirmation of the application for appointment
- Assessment of application

2. **Appointment phase**

- Verification
  a) of compliance with organisational technical requirements
  b) of compliance with personnel qualification requirements

3. **Decision on appointment**

- Verification of submitted proof and decision on appointment
- Conclusion of an agreement with the organisation to which the appraisor belongs and with the appraisor directly
- Publication in the register
- Monitoring of appointed appraisors

The following requirements are to be imposed on the appraisors:

- knowledge in the fields of information and communications technology and IT security (minimum of 4 and 2 years´ experience in the fields of IT and IT security respectively),
- knowledge in the field of IT security concepts,

- knowledge of the procedures, structure and mode of functioning of quality and security management systems,
- knowledge of the Digital Signature Act and Ordinance and the safeguard catalogue,
- experience in the auditing and assessment of quality and security management, and
- furnishing of at least 2 to 3 references relating to security concepts (drafting/appraisal).

The information contained in the application for appointment must include the following:

- precise description of the specialised area to which the application for appointment relates,
- details of the appraisor´s professional career and experience in the specialised field to which the application for appointment relates,
- details of the appraisor´s involvement in relevant national and/or international standardisation and expert bodies,
- details of the appraisor´s experience in the fields of assessment and certification, quality management, IT security, and experience as an appraisor or in a comparable capacity,
- details of reference projects,
- undertaking by the appraisor to maintain confidentiality,
- undertaking to apply only those assessment methods and assessment means which are specified for the specialised area concerned at the time of appointment,
- undertaking by the appraisor to exchange experience with other involved parties, and
- a completed application form bearing the appraisor´s legally binding signature.

The applicant is to furnish the following proof:

- proof of qualifications and competence, and
- proof of fulfilment of the required general technical and organisational conditions.

The appraisor´s task is to assess the security concept and its implementation and to record the results of this assessment in a report. The appointment is limited to the individual concerned, and cannot be transferred. The appointment applies as long as the agreement exists between the competent authority and the appraising person; it may be cancelled on the grounds specified in this agreement. Activities which fall within the sphere of the appointment may only be carried out by the appraisor himself. Appraisors are bound to observe confidentiality on all information and documents of which they obtain knowledge in connection with their appraisal activities. Information relating to the appraisal work may be passed on to third parties only with the express consent of those concerned to which the information relates. This provision does not apply to information furnished to the expert committee.

The appointment of appraisors is subject to the prospective appraisors furnishing and substantiating the required proof of compliance with the stipulated requirements. Appointment is subject to the basic qualification requirements for appraisors which are drawn up by the competent authority and declared binding, and to the mutual rights and duties stipulated by contractual agreement between the competent authority and the appraisor. The appointed appraisors undertake to provide the competent authority with proof of their qualification for the post of appraisor on a regular basis. In this connection, the competent authority should be provided with information relating, for example, to individual training and advanced training measures, participation in seminars, publications in specialist journals and lecturing and teaching work carried out after the appointment as an appraisor.

### 7.5.4 Parties involved

| Functions | Activities | Responsibility |
|---|---|---|
| Appointment of appraisors for security concepts | Implementation of the appointment procedure and conducting the technical discussion | Staff of the competent authority and expert committee |
| Appraisal of general conditions | Implementation of the appraisal procedure | Staff of the competent authority (may be delegated to accreditation body) |
| Assessment of security concepts | Security assessment | Appraisors |
| Confirmation of security concepts | Confirmation of proper implementation of the procedure and conformity of the results with legal requirements | Expert committee |

### 7.5.5 Methods, qualifications and competence for the appraisal of security concepts

The certification authority's security concept is intended to guarantee that the certification authority commences operation in a secure state and maintains this state in the course of operation.

#### 7.5.5.1 Establishment of a secure state

Appraisal of the certification authority (so-called security assessment) involves an assessment of reliability and specialised knowledge and an assessment of the security concept (see 7.4.3.2). The assessment of reliability and specialised knowledge covers the following formal aspects: organisational structure, certification personnel, documentation and updating service, records, certification procedures, quality management manual, confidentiality, publications, complaints, internal audit and periodical verification. The assessment of security concepts covers the following technical aspects:

a) the suitability and effectiveness of the security safeguards,

b) the use of suitable technical components,

c) the operational and organisational structure, and

d) the use of suitable mathematical/cryptographic processes.

In the interests of efficiency, it is expedient to have the formal and technical parts of the appraisal carried out at the same time by one and the same team. The table below shows the assignment of the technical aspects (column) to the contents (line) recommended in Section 5 of this Catalogue which are to receive due consideration in the security concept.

| | a) Suitability and effectiveness | b) Use of suitable technical components | c) Operational and organisational structure | | d) Use of mathematical /cryptographic processes |
|---|---|---|---|---|---|
| General information | Infrastructure | | | Personnel Organisation | |
| Structural analysis | | | Operational specification | | Mathematical/cryptographic specification |
| Security concept | Protection requirements Compliance<br>Emergency | Information and communica-tions technology (security) | | | |
| Other aspects | Law | | | | |

In assessing security concepts, the following three specialised areas are to be covered:

1. functions of the certification authority, covering the areas of mathematics/cryptography and operational specification,
2. security concept, covering the areas of organisation/personnel, IT systems and operational environment, and
3. law.

The assessment should be carried out by a team consisting of at least two independent experts. All the above-stated specialised areas are to be covered in full by the members of the team. One person may be responsible for several specialised areas. The obligation on the part of the appraisors appointed for the individual specialised areas to participate in a regular exchange of experience and findings is intended to establish and maintain an appropriate standard of quality. The criteria, procedures and resources to be applied in connection with the assessments are stipulated by the competent authority.

#### 7.5.5.2 Maintenance of a secure state

The security concept specifies all the measures and safeguards which are implemented in order to fulfil the security requirements. This is the document which stipulates the security policy and describes the organisational structure, procedures, processes and resources which are required in order to implement the safeguards, the so-called security management system. Consequently, the entire scope of security-related activities and objectives of an organisation can be referred to as security management. This security management thus embraces the activities of planning, control and assessment with regard to the security safeguards within a certification authority. The suitability and effectiveness of the specified and implemented security safeguards is verified via an assessment of the security management system.

The assessment of a security concept includes an evaluation of the suitability and effectiveness of the specified and implemented security safeguards; two basic questions require to be answered in this connection:

1. Do the specified safeguards fulfil the security requirements?
2. Have the adopted safeguards been implemented correctly?

These questions imply two opposite but not mutually exclusive approaches: top-down, i.e. an evaluation of the complete, unambiguous and consistent derivation of the safeguards from the security requirements as stipulated in the Digital Signature Act and Ordinance, and bottom-up, i.e. an evaluation of the implementation of the described safeguards. As the assessment of management systems focuses on an analysis of all relevant processes, an all-embracing evaluation of the management system taking due account of the interactions and combined effects of all security safeguards is the only expedient approach.

## 7.6 Procedure for the recognition of evaluation bodies and confirmation bodies for technical components

### 7.6.1 Intended objective

§ 14 (5) SigG states the following preconditions for the recognition of confirmation authorities:

- the security certificates or other types of confirmations issued by other bodies must ensure a comparable level of security, and
- the technical requirements, tests and test procedures forming the basis for the bodies´ test reports must be equivalent to those of confirmation bodies which have already been recognised.

The explanatory note on § 14 (5) SigG points out that the requirement for products and recognised product evaluations from other European states to be accorded equal status constitutes a precondition for the recognition of assessments.

### 7.6.2 Subject matter

§ 14 (4) SigG states that the technical components are to be adequately tested against current engineering standards and their compliance with requirements is to be confirmed by a body recognised by the competent authority.

The explanatory note on § 14 (4) SigG points out that, in addition to the BSI, the competent authority may also recognise other bodies, provided that the security certificates issued by such bodies ensure the necessary level of security. To enable ascertainment of the comparability and equivalence of the basic preconditions, the applied procedures and the determined results, the following points are to be assessed:

1. stipulations of the confirmation bodies regarding the evaluation results and evaluation procedures for technical components,
2. working practices of the confirmation bodies, and
3. stipulations of the confirmation bodies regarding the content and form of issued certificates or confirmations.

The explanatory note on § 14 (5) SigG points out that products and recognised product evaluations within the meaning of subsection 4 from the stated European states are accorded equivalent status. To enable ascertainment of the comparability and equivalence of the basic preconditions, the applied procedures and the determined results, the following points are to be assessed:

1. stipulations of the evaluation bodies regarding the results and procedures for the development of technical components,
2. working practices of the evaluation bodies, and
3. stipulations of the evaluation bodies regarding the content and form of issued evaluation reports.

In particular, proof is to be furnished of the required knowledge of the Digital Signature Act and Ordinance and of the safeguard catalogue.

The Federal Agency for Security in Information Technology is available as a recognised evaluation and confirmation body for technical components, for example; at least two private security certification bodies should be recognised.

### 7.6.3 Description of procedure and actions involved

#### 7.6.3.1 Confirmation bodies

The procedure for the recognition of confirmation bodies which, in the case of a positive final decision, concludes with recognition of the body concerned as an approved body for the confirmation of technical components in accordance with the Digital Signature Act and Ordinance, is based on the standard procedures in the field of accreditation.

**Scenario BSK_1:**
**Security certification bodies with valid accreditation (in the field of ITSEC certification) and additional authorisation to provide confirmation in accordance with SigG/SigV**

Confirmation of the requirements for technical components clearly covers both confirmation of a proper evaluation process (security certificate) and confirmation of compliance with the requirements of the Act and the Ordinance (conformity with the law). Accreditation establishes the basis for comparability and equivalence of the applied procedures and the determined results. As the BSI is explicitly named as an evaluation and confirmation body, the procedures which have already been established at the BSI serve as a basis for the recognition of other bodies.

The following preconditions apply:

- fulfilment of the general criteria for operation of security certification authorities in accordance with DIN EN 45011 and the technical requirements which apply to the specialised field concerned,
- where appropriate, participation in the exchange of experience and findings, and
- a knowledge of the Digital Signature Act and Ordinance and of the safeguard catalogue.

The information contained in the application must include the following:

- a precise description of the field to which the application for accreditation relates, and
- a completed application form bearing a legally binding signature.

The following proof is to be furnished:

- proof of the required level of qualification and competence, and
- proof of compliance with general technical and organisational requirements.

#### 7.6.3.2 Evaluation bodies

The procedure for the recognition of evaluation bodies which, in the case of a positive final decision, concludes with recognition of the body concerned as an approved body for the evaluation of technical components in accordance with the Digital Signature Act and Ordinance, is based on the standard procedures in the field of accreditation.

**Scenario PSK_1:**
Manufacturer carries out development and evaluation

**Scenario PSK_2:**
**Test laboratory with valid accreditation (in the field of ITSEC evaluation)**

**Scenario PSK_3:**
Manufacturer produces with approved QM system in compliance with ITSEC standards and evaluates according to alternative

In contrast to the confirmation of technical components, recognition is not explicitly required for the purposes of evaluating technical components. However, in view of the existing evaluation and certification scheme in accordance with ITSEC, it is appropriate for evaluation to be carried out by a test laboratory which is duly accredited for the purposes of ITSEC evaluations. When test reports from test laboratories with valid accreditation are not stipulated as an essential requirement for the purposes of recognising confirmation bodies, appropriate precautions are to be implemented when tests are also carried out by non-accredited laboratories.

The following preconditions apply:

- fulfilment of the general criteria for operation of security certification authorities in accordance with DIN EN 45011 and the technical requirements which apply to the specialised field concerned,
- where appropriate, participation in the exchange of experience and findings,
- a knowledge of the Digital Signature Act and Ordinance and of the safeguard catalogue, and

- a knowledge of mathematics/cryptography.

The information contained in the application must include the following:

- a precise description of the field to which the application for accreditation relates, and
- a completed application form bearing a legally binding signature.

The following proof is to be furnished:

- proof of the required level of qualification and competence, and
- proof of compliance with general technical and organisational requirements.

#### 7.6.3.3 Recognition

In both cases, the accreditation process is divided into three phases: preparation, appraisal and decision.

1. **Preparation for the accreditation process**

- Submission of inquiry to the competent accreditation body for the field concerned
- Preliminary discussion
- Application for accreditation
- Confirmation of the application for accreditation
- Examination of application
- Appraisal contract with costing

2. **Accreditation appraisal**

- Selection of appraisors in consultation with the applicant
- Appointment of appraisors
- Expert examination of the application documents
- Appraisal
  a) of conformity with the DIN EN 45000 series and
  b) of technical competence on the basis of special technical criteria
- Drafting of the appraisal report

3. **Decision on accreditation**

- Assessment of the appraisal results and decision on accreditation
- Conclusion of an accreditation contract
- Issuing of the accreditation certificate
- Publication in the register
- Monitoring of accredited bodies and extension of accreditation

DEKITZ is presently available as an accredited body for security certification authorities; an extension of the scope of the agreement between BAPT, BSI and DEKITZ on cooperation in the performance of accreditation procedures for test laboratories and security certification authorities would be appropriate. BSI and DEKITZ are available as accredited bodies for test laboratories; the adoption of a joint accreditation procedure by BAPT, BSI and DEKITZ would be particularly expedient.

### 7.6.4 Parties involved

| Functions | Activities | Responsibility |
|---|---|---|
| Recognition of evaluation and confirmation bodies for technical components | Accreditation procedure | Accreditation bodies for test laboratories and security certification authorities for technical components |
| Evaluation of technical components | ITSEC evaluation | ITSEC test laboratory |
| Confirmation of technical components | Confirmation of proper implementation of the procedure and conformity of the result with legal requirements | ITSEC certification authority |

**ANNEX Initialisation phase of the certification body**

CA: Submission of written licence application to CO and verification of completeness of the submitted documents by RA

CA: Verification of operator's reliability, i.e. compliance with the relevant legal requirements

CA: Verification of the personnel's specialised knowledge, i.e. possession of the required knowledge, experience and skills

CO: Verification of preconditions for issuing of the licence with regard to the operator's reliability and specialised knowledge

CA: Verification of other pertinent preconditions, i.e. specification of the intended measures to fulfil the security requirements in the security concept

ABS/CBS: Assessment and confirmation of the security concept and its implementation

EBT/CBT (optional): Evaluation and confirmation of the deployed technical components in accordance with ITSEC

CA: Submission of the security concept and the results of the assessment/confirmation to the CO

RA: Decision on licence - Issuance in accordance with official notification - Complaints procedure in case of rejection or revocation - Invoicing of costs

RA: Issuance/revocation of certificates, i.e. generation/erasure of CA signature key by the CA and certification/revocation of the CA signature key by the CO

CA: Renewed assessment after changes of relevance to security and at 2-yearly intervals at the latest by ABS

RA: Random checks by CO in suspected cases of failure to comply with requirements and at appropriate intervals

ZS: Renewed submission to CO

## Literature

[DIN 45001] DIN EN 45001 Allgemeine Kriterien zum Betreiben von Prüflaboratorien (September 1989)

[DIN 45004] DIN EN 45004 Allgemeine Kriterien für den Betrieb verschiedener Typen von Stellen, die Inspektionen durchführen (June 1995)

[DIN 45011] DIN EN 45011 Allgemeine Kriterien für Stellen, die Produkte zertifizieren (May 1990)

# 8. Standards and guidelines

| JTC | ISO/IEC | WG | SC 27 | NI 27 | Status | Relevant to SigG | Contents |
|---|---|---|---|---|---|---|---|
| 1.27.01 | 8372 | 2 | | | IS | | Modes of operation for a 64-bit block cipher algorithm |
| 1.27.02 | 10116 | 2 | N 1494 | 279-96 | DIS | | Modes of operation for an n-bit block cipher algorithm |
| 1.27.03.01 | 9798-1 | 1 | N 1496 | 281-96 | IS | | Entity authentication, Part 1, general model |
| 1.27.03.02 | 9798-2 | 2 | N 68A | 77-94 | IS | | Entity authentication, Part 2, symmetric encipherment algorithms |
| 1.27.03.03 | 9798-3 | 2 | N 1669 | 126-97 | IS | | Entity authentication, Part 3, asymmetric techniques |
| 1.27.03.04 | 9798-4 | 2 | N 952 | 183-94 | IS | | Entity authentication, Part 4, cryptographic check function |
| 1.27.03.05 | 9798-5 | 2 | N 1671 | 165-97 | DIS | | Entity authentication, Part 5, ZKN techniques |
| 1.27.04 | 9797 | 2 | N 790 | 169-93 | IS | | Data integrity, block cipher |
| 1.27.06.01 | 13888-1 | 2 | N 1503 | 37-97 | DIS | * | Non repudiation, Part 1, general model |
| 1.27.06.02 | 13888-2 | 2 | N 1679 | 129-97 | 5.CD | * | Non repudiation, Part 2, symmetric techniques |
| 1.27.06.03 | 13888-3 | 2 | | 16-97 | DIS | * | Non repudiation, Part 3, asymmetric techniques |
| 1.27.07.01 | 9796-1 | 2 | | | IS | * | DS giving message recovery, redundancy |
| 1.27.07.02 | 9796-2 | 2 | N 1683 | 183-97 | DIS | * | DS giving message recovery, hash-function |
| 1.27.07.03 | 9796-3 | 2 | N 1563 | 292-96 | WD | * | Mechanisms using a check function |
| 1.27.07.04 | 9796-4 | 2 | N 1564 | 193-97 | 1. WD | * | Discrete logarithm based mechanisms |
| 1.27.08.01 | 14888-1 | 2 | N 1687 | 185-97 | 3.CD | * | DS General Model |
| 1.27.08.02 | 14888-2 | 2 | N 1513 | 115-97 | 3.CD | * | DS identity based (GQ) |
| 1.27.08.03 | 14888-3 | 2 | | 7-97 | 3.CD | * | DS certificate based (DSA) |
| 1.27.09.01 | 10118-1 | 2 | N 828 | 130-94 | IS | * | Hash functions, Part 1, general |
| 1.27.09.02 | 10118-2 | 2 | N 829 | 129-94 | IS | * | Hash functions, Part 2, n-bit block cipher |
| 1.27.09.03 | 10118-3 | 2 | | 17-97 | DIS | * | Hash functions, Part 3, dedicated hash functions |
| 1.27.09.04 | 10118-4 | 2 | N 1696 | 198-97 | DIS | * | Hash functions, Part 4, modular arithmetic |
| 1.27.10 | 9979 | 1 | N 1395 | 169-96 | | | Directory of cryptographic algorithms |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 1.27.13 | 15816 | 1 | N 1666 | 107-97 | CD | | Security information objects |
| 1.27.14.01 | 13335-1 | 1 | | 171-97 | CD | | Guidelines for the management of IT Security, Concepts and Models |
| 1.27.14.02 | 13335-2 | 1 | N 1523 | 43-97 | WD | | Guidelines for the management of IT Security, Managing and Planning |
| 1.27.14.03 | 13335-3 | 1 | N 1325 | 273-96 | WD | | Guidelines for the management of IT Security, Techniques for the Management |
| 1.27.14.04 | 13335-4 | 1 | N 1354 | | | | Guidelines for the management of IT Security, Selection of Safeguards |
| 1.27.14.05 | 13335-5 | 1 | N 1356 | | | | Guidelines for the management of IT Security, External Connections |
| 1.27.16.01 | | 3 | N 1401 | | WD | | Evaluation criteria, Part 1 |
| 1.27.16.02 | | 3 | N 1402 | | WD | | Evaluation criteria, Part 2 |
| 1.27.16.03 | | 3 | N 1403 | | WD | | Evaluation criteria, Part 3 |
| 1.27.16.04 | | 3 | N 1404 | | | | Evaluation criteria, Part 4 |
| 1.27.18.01 | 11770-1 | 1 | N 1529 | 257-96 | DIS | | Key management, Part 1, Framework |
| 1.27.18.02 | 11770-2 | 2 | N 1213 | 32-96 | IS | | Key management, Part 2, symmetric techniques |
| 1.27.18.03 | 11770-3 | 2 | | 276-96 | DIS | | Key management, Part 3, asymmetric techniques |
| 1.27.19.01 | 14516-1 | 1 | N 1358 | 81-95 | | * | TTP General overview |
| 1.27.19.02 | 14516-2 | 1 | | 8-97 | | * | TTP Technical Aspects |
| | | | N 1442 | 210-96 | | | ISO/TC68 Catalogue of Security Related Standards |
| | | | N 1185 | 187-95 | | | Comprehensive Approach of ZK techniques |
| | | | N 1160 | 142-95 | DIS | | Code of Practice for information security management |
| | | | N 359 | 139-95 | | | DS with limited message recovery |
| | 11568-3 | | | | | | Banking - Key Management techniques for symmetric ciphers |
| | 9594-8 | | X.509v3 | | | * | Certificate extensions and CRL extensions |
| | RFC 1421 | | PEM | | | * | Message Encryption and Authentication Procedures |
| | RFC 1422 | | PEM | | | * | Certificate based key-management |
| | RFC 1423 | | PEM | | | * | Algorithms, Modes and Indicators |
| | RFC 1424 | | PEM | | | * | Key certification and related services |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | PKCS #1-#11 | | | | | * | Public Key cryptography Standards |
| | 7810 | | | | IS | * | Identification Cards - Physical Characteristics |
| | 7813 | | | | IS | * | [ISO] Identification cards - Financial transaction cards |
| | 7816-1 | | | | IS | * | Identification cards - Integrated circuit(s) cards with contacts - Part 1: Physical characteristics |
| | 7816-2 | | | | IS | * | Identification Cards - Integrated circuit(s) cards with contacts - Part 2: Dimension and location of contacts |
| | 7816-3 | | | | IS | * | Identification Cards - Integrated circuit(s) cards with contacts - Part 3: Electronic signals and transmission protocols |
| | 7816-4 | | | | IS | * | Identification Cards - Integrated circuit(s) cards with contacts - Part 4: Interindustry commands for interchange |
| | 7816-5 | | | | IS | * | Identification Cards - Integrated circuit(s) cards with contacts - Part 5: Numbering system and registration procedure for application indicators |
| | 7816-6 | | | | IS | * | Identification Cards - Integrated circuit(s) cards with contacts - Part 6: Interindustry data elements |
| | 7816-8 | | | | IS | * | Identification Cards - Integrated circuit(s) cards with contacts - Part 8: Security related interindustry commands |
| | 10373 | | | | IS | * | Identification cards - Test methods, ISO/IEC IS 1993 |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | **CEN ENV** | | | | | | |
| | 1375-1 | | | | | * | Identification card system - Intersector integrated circuit(s) card additional formats - Part 1: ID-000 card size and physical characteristics |
| | **DIN EN** | | | | | | |
| | 45001 | | | | | * | General criteria for the operation of test laboratories |
| | 45004 | | | | | * | General criteria for the operation of different types of bodies which carry out inspections |
| | 45011 | | | | | * | General criteria for bodies which certify products |