

# Signature Order SigV

## pursuant to § 25 of the Signature Law

### Contents

- § 1 Fees for supervisory activities
- § 2 Financial resources of certification service providers
- § 3 Generation of signature creation data for secure electronic signatures
- § 4 Storage of signature creation data for secure electronic signatures
- § 5 Technical components and procedures of supervisory body
- § 6 Technical components and procedures of certification service providers which issue qualified certificates
- § 7 Technical components and procedures of users of secure electronic signatures
- § 8 Protection of technical components for secure electronic signatures on the certification service provider's premises
- § 9 Testing technical components and procedures for qualified certificates and secure electronic signatures
- § 10 Provision of signature and certification services for qualified certificates and secure electronic signatures
- § 11 Application for a qualified certificate
- § 12 Qualified certificates
- § 13 Directory and revocation services for qualified certificates
- § 14 Secure timestamping services
- § 15 Security and certification concept for qualified certificates
- § 16 Records
- § 17 Renewed electronic signature (follow-on signature)
- § 18 Supervision and accreditation
- § 19 Reference to notification
- § 20 Entry into force
- Appendix 1 Parameters for technical components and procedures for secure electronic signatures
- Appendix 2 Technical procedures and formats

### Fees for supervisory activities

**§ 1.** (1) Certification service providers shall be charged the following fees for the following specific services by the supervisory body and Telekom-Control GmbH:

1. Audit and registration of certification service provider on notification of commencement of activity (§ 6, para. 2 of the Signature Law):
  - a) for certification service providers which do not issue qualified certificates and do not supply secure electronic signature procedures: 100 euros
  - b) for certification service providers which issue qualified certificates or supply secure electronic signature procedures: 6,000 euros
2. Audit of certification service provider on notification of a further security and certification concept:
  - a) for certification service providers which do not issue qualified certificates and do not supply secure electronic signature procedures: 50 euros
  - b) for certification service providers which issue qualified certificates or supply secure electronic signature procedures:
    - aa) on notification of a further security and certification concept with changes with security implications: 4,000 euros

bb) on notification of a further security and certification concept with no changes with security implications:	1,000 euros
3. Audit of certification service providers on application for accreditation (§ 17 of the Signature Law):	6,000 euros
4. Audit of a certification service provider on notification of fundamental changes with security implications to an existing security and certification concept (§ 6, para. 5 of the Signature Law) for certification service providers which issue qualified certificates:	4,000 euros
5 a) Regular audit of certification service provider (§ 13, para. 1 of the Signature Law):	4,000 euros
b) Additional audit of certification service providers where it is established that the provisions of the Signature Law or the Orders issued on the basis thereof have been violated to more than just a minor degree:	6,000 euros
c) Audit of certification service providers in the event of changes with security implications to the security and certification concept which were not notified to the supervisory body:	6,000 euros
6. Notice of requirements in the event of shortcomings with security implications (§ 14, para. 6 of the Signature Law):	1,000 euros
7. Notice to certification service provider to cease activities (§ 14, para. 2 to 4 of the Signature Law):	1,000 euros
8. Supervision of cessation of certification service provider's activities (§ 12 of the Signature Law):	100 euros
9. Take-over of certification service provider's revocation service by the supervisory body (§ 12 and § 14, para. 5 of the Signature Law):	1 euro per certificate managed by the revocation service per year.
10. Keeping directories at the supervisory body (§ 13, para. 3 and § 17, para. 1 of the Signature Law):	500 euros per certification service provider per year.
11. Evaluating the equivalence of test reports from a government-recognised body in a third country (§ 24, para. 3 of the Signature Law):	6,000 euros.

(2) In order to cover the overhead costs of the supervisory and Telekom-Control GmbH, certification service providers which issue qualified certificates shall pay a fee of 2 euros per valid qualified certificate issued per year.

(3) Insofar as the supervisory agency or Telekom-Control GmbH uses a confirmation agency or other non-official person or institution in the course of supervision under the Signature Law or the orders issued on the basis thereof, their fees shall be determined in accordance with § 53a AVG and levied on the certification service provider in question as cash disbursements as defined in § 76 AVG.

(4) The supervisory body shall issue a notice for the fees. The fees in accordance with paragraph 2 shall be collected on a pro rata basis in arrears for each quarter. Certification service providers which issue qualified certificates shall therefore notify the supervisory body by the 15<sup>th</sup> of each month of the number of qualified certificates issued which were valid on the first day of the month.

### **Financial resources of certification service providers**

**§ 2.** (1) The regular funds at the certification service provider's disposal for the purpose of exercising its activities shall be stated to the supervisory body on notification of commencement of activities in accordance with § 6, para. 2 of the Signature Law. Certification service providers which issue qualified certificates shall have minimum funds of 300,000 euros. These minimum funds shall be available in the form of own equity as defined in § 224, para. 3 A and B of the Commercial Code. Registered capital as defined in § 224, para. 3 A shall be understood to mean paid up capital as defined in § 23, para. 3 of the Federal Finance Act.

(2) Certification service providers which issue qualified certificates shall also prove to the supervisory body on notification of assumption of activities in accordance with § 6, para. 2 of the Signature Law that they have contracted liability insurance with minimum cover of 1,000,000 euros per claim.

(3) The Federal Republic, Provinces, associations of local authorities and communities with more than 50,000 inhabitants shall be exempt from the obligations set out in paragraphs 1 and 2.

### **Generation of signature creation data for secure electronic signatures**

**§ 3.** (1) The supervisory body's signature creation data shall comply with Appendix 1, point 1 (main system). The generation system must be isolated, designed solely for this purpose and suitably protected from unauthorised access and malfunction. The supervisory body shall generate a second system of signature creation

data (second key) and shall also create all its own electronic signatures with which it signs the directories kept by it with this second system as a back up. The signature verification data (public key) for the second system shall be signed with the supervisory body's signature creation data. The second system shall be kept under lock and key. The signature verification data for the second system shall only be used if the main system fails so that the signature and certification services of the supervisory body can continue uninterrupted. If the supervisory body also uses signature creation data other than those referred to in Appendix I, point I, the certificates containing the signature verification data in question shall be signed using the main system and shall be stored so that they can be retrieved electronically at all times. The supervisory body shall ensure that the signature creation data used by it and the signature verification data in the corresponding certificate can be used in tandem.

(2) The certification service provider's signature creation data must be generated in and must not leave its signature creation device. The signature verification data must be notified to the supervisory body in the certification service provider's security and certification concept. For the rest, the requirements governing other signatories' secure electronic signatures shall apply.

(3) The minimum length of the signature creation data for signatories' secure electronic signatures is laid down in Appendix I, point 2. The actual key length of the signature procedures provided shall be stated in the certification service provider's security concept, together with the upper and lower limits. The algorithms used must be published. The probability that the signature creation data for secure electronic signatures will only occur with the signatory must border on certainty and must allow the identity of the signatory to be concluded unequivocally using state-of-the-art technology. The repeated generation of signature creation data for secure electronic signatures should not reduce the quality of the key below the appropriate security level for the signature procedure in question.

(4) Repeated use of the signature creation data for secure electronic signatures shall not reduce the quality of the key. Applications which may reduce the quality of signature creation data (e.g. RSA applications on randomly selected data) must be effectively excluded. The signature creation data may only be used for their intended purpose.

(5) The signature creation data for secure electronic signatures must be generated on the basis of real random elements based in turn on technical random elements or signatory-related random elements. The number of bit positions in signature creation data influenced by real random elements is stipulated in Appendix I, point 3 (quality random elements). The suitability of the random elements must be adequately tested. Pseudorandom numbers must not be used as a starting point. If the generation system is used for the signature creation data of various signatories, the statistical random quality of the technical random elements used must be checked periodically (at least once a month). The test protocols must be recorded. If the results of the test are negative, the certificates based on the signature creation data in question, which have been issued since the last test with positive results shall be revoked.

(6) If the signature creation data for secure electronic signatures are generated by the certification service provider, then it shall take suitable precautions to ensure that the signature creation data or other data from which the signature creation data can be extrapolated are not disclosed and that these data are not stored outside the signatory's signature creation device. This shall also apply to the transmission of such signature creation data to the signatory's signature creation device and to the data to identify the signatory to the signature creation device (e.g. PIN). If the signature creation data are generated outside the signatory's signature creation device, the generation systems used shall be suitably protected from unauthorised access or malfunction. Access to the generation system shall be monitored, every user shall be identified and every use shall be registered.

(7) If the signature creation data for secure electronic signatures are generated in the signatory's signature creation device, then the certification service provider shall only supply or recommend technically suitable signature creation devices for generating and storing the signature creation data.

### **Storage of signature creation data for secure electronic signatures**

**§ 4.** (1) Signature creation data for secure electronic signatures shall be stored in such a way as to preclude its disclosure and ensure that the signatory has sole control of the use thereof. It is prohibited to duplicate signature creation data once they have been generated.

(2) Signature creation data for secure electronic signatures may be distributed to several signature creation devices for specific security purposes, in which case all the signature creation devices in question shall comply with the security requirements. The signatory shall be given instructions on the procedure needed to trigger the signature function (§10, para. 7).

### **Supervisory body: technical components and procedures**

**§ 5.** The systems (especially the products and procedures) used by the supervisory body shall comply with the security requirements for secure, electronic signatures. The supervisory body shall only use the algorithms listed in Appendix. 2.

## **Certification service providers issuing qualified certificates: technical components and procedures**

**§ 6.** (1) The current status of the systems (especially the products and technical procedures) used by certification service providers which issue qualified certificates shall be recorded in a verifiable manner. The presence of non-documented system elements or deviations from the records with security implications shall be tantamount to compromise of the security precautions. The same shall apply if these system elements are not required in order to provide signature or certification services. If the system elements used by the certification service provider in order to provide signature and certification services are also used for other activities, this shall not affect the working of the system elements used to provide the signature and certification services.

(2) The hash procedures specified in Appendix 2 section 2 shall be used in order to create secure electronic signatures. The algorithms used to generate the hash value shall be deemed secure until the date stipulated in Appendix 2 section 2. Pseudo random numbers may also be used to supplement the hash value. The algorithms listed in Appendix 2 section 3 shall be used to encrypt the hash value. The algorithms used to create signatures shall be deemed secure until the date stipulated in Appendix 2 section 3. Pseudo random numbers may also be used when applying signature algorithms which require random numbers (e.g. DSA).

(3) Certification service providers which issue qualified certificates must be able to verify electronic signatures securely. The procedures and algorithms used to verify signatures form a logical unit together with the procedures and algorithms used to create signatures and they shall be jointly documented.

## **Users of secure electronic signatures: technical components and procedures**

**§ 7.** (1) Signatories shall only use hash procedures and procedures to encrypt the hash value as stipulated in Appendix 2 sections 2 and 3.

(2) The technical components and procedures used by signatories in order to create secure electronic signatures must allow full display of the data to be signed. Only the formats recommended by the certification service providers shall be used for the data to be signed. The specifications for these formats shall be generally available. If dynamic changes or invisible data can be encoded in a format, then the codes in question must not be used. The certification service provider shall instruct users or provide them with methods which preclude dynamic changes or invisible data.

(3) Entry of an authorisation code must be needed in order to trigger the signature function in the signatory's signature creation device. The signatory must be told how many signatures are triggered when the signature creation device receives the signatory's authorisation (e.g. PIN, fingerprint). The authorisation code must be designed and effective barring mechanisms used in order to exclude the practical possibility of an unauthorised person's acquiring the authorisation code. The same authorisation code shall not be used for different applications (e.g. signature and ATM functions). Signature creation devices which allow several applications (e.g. multi-application cards or multi-application terminals) may only be used if the measures and methods used to prevent various applications from being triggered with the same authorisation code are described in the security concept. The authorisation code entered shall not be stored by the system elements used. There must be no simplified input in the case of repeated input of the authorisation code. The authorisation code may be distributed to several system elements for special security purposes. The signatory must be instructed in the measures needed to trigger the signature function (§ 10, para. 7).

(4) The formats listed in Appendix 2 section 4 are particularly suitable as signature formats.

(5) If the recipient of an electronically signed declaration wishes to verify the secure signature in a secure manner, he must use the verification devices described as suitable for secure signature verification in the security concept of the certification service provider which issued the certificate. These verification devices shall comply with the requirements of § 18, para. 4 of the Signature Law.

## **Protection of technical components for secure electronic signatures on the certification service provider's premises**

**§ 8.** Certification service providers shall take suitable precautions to protect signature creation data and the technical components used to create certificates and ensure that directory and revocation services can be retrieved, from compromise and unauthorized access. Unauthorised access must be recognisable.

## **Testing the technical components and procedures for qualified certificates and secure electronic signatures**

**§ 9.** (1) Suitable protection profiles from the Common Criteria for Information Technology Security Evaluation (ISO 15408) recognised by a confirmation body shall be used in order to test the technical components and procedures for qualified certificates and secure electronic signatures.

(2) Technical components and procedures may also be tested under § 7, para. 2, § 10 and § 18 of the Signature Law using the criteria of the Information Technology Security Evaluation Criteria (ITSEC) and, where applicable, in accordance with the Security Requirements for Cryptographic Modules (FIPS 140-1) or British Standard (BS) 7799. If ITSEC is used, assurance level E 3 with security mechanisms with "high" minimum strength must be applied for generating and storing signature creation data and for generating secure electronic signatures and, where necessary, for secure signature verification; assurance level E 2 with security measures with "high" minimum strength must be applied for other technical components and procedures.

(3) The certificate of compliance with security requirements for technical components and procedures must state for which applications, under which conditions and until when it is valid. A copy of the test report and the certificate shall be passed to the supervisory body.

## **Provision of signature and certification services for qualified certificates and secure electronic signatures**

**§ 10.** (1) If the installations of a certification service provider which issues qualified certificates are configured as separate organisational or technical units, security measures shall be taken to ensure that the transmission of data between separate units does not compromise signature or certification services.

(2) The certification service provider's technical installations shall be configured so that functions and applications belonging to signature and certification services provided are kept separate from other functions and applications. There must be no possibility of the signature and certification services being affected by other functions and applications. This shall apply to regular operations, special operating situations as well as when not in operation. Special operating situations (e.g. maintenance) must be recorded.

(3) Certification service providers which issue qualified certificates shall take suitable precautions to ensure that the installations used to provide signature and certification services are protected from unauthorised access.

(4) Certification service providers which issue qualified certificates shall not employ staff in the provision of signature and certification services who have been sentenced to more than one year's imprisonment for criminal offences committed with intent or to more than three months' imprisonment for criminal offences against property or against the reliability of documents and evidence. Sentences redeemed in accordance with the 1972 Redemption Law or subject to restricted disclosure shall not be taken into account. The certification service provider shall check the reliability of the staff at least every two years.

(5) The technical staff of certification service providers which issue qualified certificates shall have sufficient specialist knowledge in the following areas:

1. General computing training.
2. Security technology, cryptography, electronic signatures and public key infrastructure.
3. Technical standards, especially evaluation standards.
4. Hardware and software.

The certification service provider must explain how the staff has acquired sufficient technical knowledge if requested to do so by the supervisory body (which relevant courses at recognised educational establishments or which relevant specialist activities). Training in the areas in question must last at least one year. This knowledge may be acquired, for example, by completing a course at a suitable institute of higher technical education or technical College or by completing a suitable university course. This training may be replaced by at least three years' suitable practical experience.

(6) Signature creation data generated on the certification service provider's premises shall only be handed to the signatory and the possibility of using the signature creation data before it is handed to the signatory shall be excluded. The certification service provider shall ensure under all circumstances that the signatory's signature creation data and the signature verification data on the corresponding certificate can be used in tandem.

(7) Before the signature creation data is used for the first time, the certification service provider shall give the signatory clear, generally comprehensible instructions in writing or on a permanent data carrier on all the security-related measures relating to use of the data (e.g. security of the authorisation code, testing prevention of unauthorised use, using directory and revocation services, possibility of displaying data to be signed, use of suitable formats).

## **Application for a qualified certificate**

**§ 11.** (1) The certification service provider shall establish the identity of the applicant using valid, official identity papers with a photograph. The application for a qualified certificate must be signed by the applicant *manu propria*. A copy of the identity papers submitted shall be taken and filed with the application. If the application bears the applicant's secure electronic signature, his identity need not be established anew.

(2) The application for a qualified certificate shall contain, inter alia:

1. the name, date and place of birth and the address of the applicant, the issuing authority and date of issue and the number of the identity papers with photograph submitted;
2. where applicable, information on whether the certificate should contain any restrictions on its scope or on the value of transactions;
3. where applicable, information on whether powers of attorney or other significant legal attributes on the part of the applicant, such as a legal professional or other permit or other information is to be included on the qualified certificate.

(3) If information on powers of attorney is to be included on a qualified certificate, the power of attorney must be reliably proven and the third party's consent must be submitted in writing or with a secure electronic signature attached. The said third party shall be instructed on the content of the qualified certificate in writing or on a permanent data carrier and informed of the possibility of revocation in accordance with § 9, para. 1, number 1 of the Signature Law. A legal professional or other permit must also be reliably proven before being included on a qualified certificate. If the signatory is subject to official supervision with respect to a registered professional qualification, the body responsible for the supervision shall be instructed on the content of the qualified certificate in writing or on a permanent data carrier.

### **Qualified certificates**

**§ 12.** (1) If a certification service provider issues certificates other than qualified certificates, it must use separate signature creation data for the signature relating to the qualified certificate.

(2) The formats listed in Appendix 2 are particularly suitable as formats for qualified certificates. The same applies to the coding schemes in qualified certificates.

(3) The period of validity of a qualified certificate shall not exceed three years and shall also not exceed the period of suitability of the technical components and procedures used or the concomitant parameters in accordance with appendices 1 and 2.

(4) It shall be permitted pending expiry of a qualified certificate to re-certify the same content and the same signature verification data, but not the period of validity, and thereby issue a new certificate. In all other cases, certificates with the same signature verification data and different contents shall be tantamount to compromise of the certificates in question.

(5) A certification service provider shall be entitled, with the agreement of another certification service provider, to certify its certificate or the certificates issued by it. The certificates issued in this way shall not contain any modifications. The certification service provider shall also provide directory and revocation services and, where necessary, recognize the revocations of the other certification service provider immediately.

### **Directory and revocation services for qualified certificates**

**§ 13.** (1) The formats listed in Appendix 2 are particularly suitable as formats for directory and revocation services. Directory and revocation services may also be supplied in different formats. The certification service provider shall ensure that the formats of the revocation services can be taken over by the supervisory body. If the directory and revocation services of another certification service provider are taken over, they must continue to be supplied in the same formats.

(2) The certification service provider shall tell signatories and third parties with respect to whom information on the signatory's power of attorney has been included on a qualified certificate, which forms of communication they may use at any given time in order to arrange for the immediate revocation of the certificate. Provision must be made for an authentication procedure for this purpose, although it must always be possible to demand the revocation of a qualified certificate on hard copy.

(3) The directory and revocation services must be adequately protected against forgery, fraud and unauthorised calls. Care must be taken to ensure that only authorised persons can make entries in and amendments to the directories. It must not be possible to reverse a suspension or revocation without this being noticed.

(4) Revocation services shall be updated during business hours within no more than 3 hours of learning of the grounds for revocation. Business hours shall be from 09.00 to 17.00 hours on weekdays and from 09.00 to 12.00 hours on Saturdays. However, the certification service provider shall ensure that demands for qualified certificates to be revoked can be received automatically and the suspension effected outside business hours.

(5) The hours during which directory services are available must be stated in the security concept. Availability must be assured at least during the business hours referred to in paragraph 4. Revocation services shall be available constantly. A continuous interruption to directory or revocation services of more than 30 minutes during the period of availability shall be recorded as a malfunction. A back-up system shall be provided for as long as the revocation service is being maintained or has failed. If the back-up system also fails, the supervisory body shall be notified within one calendar day and shall restore the revocation service within three calendar days. Revocation services must generally be freely accessible; they may be used free of charge without the need for identification.

(6) A certification service provider shall manage the directory and revocation services at least until the date of the follow-on signature needed (§ 17), after which the certification service provider shall allow qualified certificates to be verified in individual cases up to expiry of the deadline stipulated in § 16, para. 2. The same shall apply where the management of the revocation services is taken over by the supervisory body because a certification service provider's activities have been suspended or prohibited.

(7) The period of time for which a suspension can apply shall be stated in the security concept. This period shall not exceed three working days. A suspension may be lifted during this period. A suspension which has been lifted does not affect the validity of the certificate. If the suspension is not lifted by the said deadline, the certificate must be revoked. If a certificate is revoked because of a suspension, the suspension alone shall be tantamount to revocation.

(8) If the signatory's signature creation data are divulged or if they reoccur as signature creation data or in another form, the signature creation data have been compromised and the signatory's certificate must therefore be revoked. The revocation must be demanded by the signatory (§ 9, para. 1, number 1 of the Signature Law) or effected ex officio by the certification service provider (§ 9, para. 1, number 6 of the Signature Law) as soon as it becomes aware that the data have been compromised.

s

### **Secure time-stamping services**

§ 14. (1) Only qualified certificates may be used to provide secure time-stamping services. They shall only be used for this purpose and this use shall be noted on the certificate.

(2) The date and time certified shall be Central European Time, taking account of summer time. Other time zones shall be expressly stipulated. The time quoted by the time-stamping service provider shall be accurate to within one minute.

(3) The hours during which secure time-stamping services are available shall be stated in the security concept of certification service providers which offer this service.

### **Security and certification concept for qualified certificates**

§ 15. (1) The security and concept shall include at least the following:

1. Name of the certification service provider.
2. Address of the certification service provider and country of establishment.
3. Type, scope and provision of signature and certification services provided.
4. Application procedure.
5. Where applicable, type of pseudonyms and information on power of attorney or other important legal attributes of signatory and method of inclusion in the certificate.
6. Business hours.
7. Generation of certification service provider's signature creation data.
8. Format of certification service provider's signature creation data.
9. Signature verification data; where necessary, certification service provider's certificate.
10. Generation of signatory's signature creation data.
11. Format of signatory's signature creation data.
12. Procedure used to create signatures provided (hash procedure and procedure for encoding hash value).
13. List of signature products used, provided and recommended.
14. Authorisation code security.
15. Formats applicable for documents to be signed and, where applicable, methods for preventing dynamic changes.
16. Formats and period of validity of certificate.
17. Technical standards, access methods and times when directory and revocation services are updated and available, including period of time of block.
18. Where applicable, times at which time-stamping services are available.
19. Comprehensible and generally understandable methods for secure signature verification.
20. Format of records of security measures and special operating situations.
21. Follow-on signature period and procedure.

22. Protection of technical components from unauthorised access.

23. Protection of certification service provider's installations from unauthorized access.

(2) The security and certification concept shall be submitted to the supervisory body in electronic form (RTF, PDF, ASCII or Postscript format) and signed with the certification service provider's electronic signature. The certification service provider shall ensure that the security and certification concept and a summary of the concept can generally be retrieved electronically at all times in RTF, PDF, ASCII or postscript format.

## **Records**

**§ 16.** (1) The records in accordance with § 11 of the Signature Law, including records of malfunctions and special operating situations as well as of instructions given to the certificate holder in accordance with § 20 of the Signature Law shall be kept in electronic form. If signature creation data are generated outside the signatory's signature creation device, this shall also apply to the time at which the signature creation data are handed to the signatory. A secure electronic signature and secure timestamp (§ 14) shall be attached to the data contained in the records of certification service providers which issue qualified certificates.

(2) The records in accordance with paragraph 1 shall be kept safe for at least 33 years from the date of the last entry and must be legible and available during the said period.

## **Renewed electronic signature (follow-on signature)**

**§ 17.** The period of time after which a new secure electronic signature must be attached due to the threat of reduced security shall be stated in the certification service provider's security and certification concept, which shall make provision for follow-on signing before expiry of the deadlines given in the Appendices for the security of the signature creation procedure used. A timestamp shall be used when attaching a new signature.

## **Supervision and accreditation**

**§ 18.** (1) Certification service providers shall notify commencement of their activities in accordance with § 6, para. 2 of the Signature Law in electronic form. Unless specific contents of the notification require a different format, RTF, PDF, ASCII or Postscript format shall be used. The notice must be electronically signed. The supervisory body must be able to satisfy itself that the data is genuine and may therefore order the certification service provider or an authorised agent to attend. If the certification service provider issues qualified certificates, the supervisory body shall ensure that the certification service provider's signature creation data and the signature verification data on the corresponding certificate can be used in tandem.

(2) Notices shall contain the following in particular:

1. The security and certification concept.
2. An explanation of specific threats and risks with security implications on the certification service provider's premises.
3. Proof of financial resources and liability insurance.
4. Proof of the specialist know-how of the technical personnel.

(3) The orders of para. 1 are also applicable for notices of further security and certification-concepts as well as for notices of security-relevant changes of existing security and certification-concepts.

(4) The certification service provider shall be audited at least every two years or whenever changes with security implications are made to the security and certification concept. The supervisory body shall also be entitled to conduct random audits of the certification service provider at any given time. The supervisory body shall also carry out such an additional audit if it has good cause to suspect shortcomings with security implications.

(5) The supervisory body, its offices and the persons and installations employed by it shall be subject to official secrecy as defined in article 20, paragraph 3 of the Federal Constitution.

(6) Only details which have been checked for accuracy shall be included in the directories kept by the supervisory body. One of the formats listed in Appendix 2 shall be used for these directories. The supervisory body shall have a generally accessible homepage stating its address, signature verification data and the formats of and methods of accessing the directories kept by it.

(7) In case of voluntary accreditation according to §17 signature law the application for accreditation replaces the notice of commencement of activities of the certification provider.

(68 The description of accredited certification service providers in accordance with § 17 of the Signature Law shall contain the words "Accredited certification service provider". Accredited certification service providers shall be entitled to use the national coat of arms with the motto "Accredited certification service provider".

### **Reference to notification**

**§ 19.** This order has been notified to the European Commission (Notification no. 99/0448/a) in compliance with the terms of Directive of the European Parliament and Council no. 98/34/EC on a procedure for the provision of information in the field of technical standards and regulations as published in Directive 98/48/EC.

# Appendix I

## Parameters for technical components and procedures for secure electronic signatures

### 1. Supervisory body's signature creation data

The supervisory body's signature creation data must use a main system which complies with the RSA procedure (for encoding the hash value).

If other signature creation data are also used by the supervisory body (§ 3, para. 1, penultimate sentence), they must be signature creation data for secure electronic signatures.

### 2. Signature creation data for secure electronic signatures

The length of the key for signature creation data for secure electronic signatures must be at least:

- RSA procedure: 1023bits
- DSA procedure: 1023bits
- DSA variations based on elliptical curves: 160 bits.

Leading zero bits are not included in the key length. In all events, the key length is fundamental to the secret part of the signature creation data.

### 3. Random elements in signature creation data for secure electronic signatures

At least the following number of bit positions in signature creation data for secure electronic signatures must be influenced by real random elements:

RSA and DSA procedures: 1023bits

DSA variations based on elliptical curves: 160 bits

These are defined as high quality random procedures.

If further key elements (e.g. leading or trailing bit) are incorporated in fixed or random form during generation in order to guarantee the uniqueness of the signature creation data, this shall not reduce the number of bit positions influenced by quality random elements.

### 4. Security period

Where the algorithms listed are used, the key lengths for signature creation data listed under points 1 to 3 shall be deemed secure for the purposes of secure electronic signatures until 31.12.2005.

## Appendix 2

### Technical procedures and formats

#### 1. Supervisory body's technical procedures

The supervisory body shall use the SHA-1 procedure for the hash procedure and the RSA procedure for encoding the hash value (main system), it is prohibited to use the Chinese Remainder Theorem (CRT). If the supervisory body also uses other signature creation data (§ 3, para. 1, penultimate sentence), the procedures used to encode the hash value must be procedures for secure electronic signatures.

#### 2. Hash procedure for secure electronic signatures

The following hash procedures are recognized as secure:

- a) RIPEMD-160,
- b) SHA-1 function.

These hash procedures shall be deemed secure for the purposes of electronic signatures until 31.12.2005.

Other hash procedures are deemed to be equivalent if these procedures exhibit at least the same security and are recognized and published as such by a confirmation body.

f

#### 3. Signature creation procedure (encoding the hash value) for secure electronic signatures

The following signature creation procedures are considered secure:

- a) RSA,
- b) DSA,
- c) DSA variations based on elliptical curves:
  - ISO/IEC 14883-3, Appendix A.2.2 ("Agnew-Mullin-Vanstone analogue"),
  - IEEE standard P1363, section 5.3.3 ("Nyberg-Rueppel version"),
  - IEEE standard P 1363 [5], section 5.3.4 ("DSA version").

Where possible, internationally recognized methods should be used for the purposes of implementation. The algorithms listed shall be deemed secure for the purposes of electronic signatures until 31.12.2005.

Other signature creation procedures are deemed to be equivalent if these procedures exhibit at least the same security and are recognized and published as such by a confirmation body.

#### 4. Formats for secure electronic signatures

The formats used for secure electronic signatures should comply with an internationally recognized standard or recognized recommendation (e.g. PKCS#7 Cryptographic Message Syntax Standard).

#### 5. Formats for qualified certificates

The European Electronic Signatures Standardization Initiative (EESSI) is currently working out formats and standards for the presentation of qualified certificates and the content thereof. In the meantime, it is recommended that internationally recognized standardization proposals be used (e.g. X.509 v3 certificate or X.509 v2 CRL for use in the Internet). The details of the format must be presented in the security and certification concept: The format must be described using a formal notation (e.g. CCITT or ITU-T Recommendation X.208: Specification of Abstract Syntax Notation One - ASN.1 - 1988). The same applies to the "qualified" label coding on a qualified certificate.

#### 6. Formats for directory and revocation services for qualified certificates

The directory and revocation services should be kept in an internationally recognized format. The following international standards are recommended for access to the directory and revocation services:

- a) 1988 CCITT (ITU-T) X. 500 / ISO IS9594,
- b) RFC 2587 Internet X.509 Public Key Infrastructure LDAPv2 Schema,
- c) RFC 2459 Internet X.509 Public Key Infrastructure Certificate and CRL Profile,
- d) RFC 2589 Lightweight Directory Access Protocol (LDAPv3) Extensions for Dynamic Directory Services.