Digital Signature Ordinance

(Signaturverordnung - SigV)

On the basis of § 16 of the Digital Signature Act of 22 July 1997 (Federal Law Gazette I S. 1870, 1872), the Federal Government decrees as follows:

Contents

§ 1: Procedures for issuance, withdrawal and revocation of licenses

(1) 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.

(2) 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. 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.

(3) 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.

§ 2: Costs

(1) The following public services shall be subject to charges (fees and expenditures):

1. issuance of a license for the operation of a certification authority,
2. rejection of an application for issuance of a license,
3. withdrawal or revocation of a license,
4. complete or partial rejection of an objection,
5. issuance of certificates,
6. review of check reports and confirmations pursuant to § 15 (1),
7. checks pursuant to § 15 (2), if such checks reveal a not solely insignificant violation of the Digital Signature Act or of this Ordinance,
8. taking over of documentation pursuant to § 11 (2) of the Digital Signature Act.

Charges shall also be due if an application for issuance of a license, or an objection, is withdrawn after the commencement of official processing but before the conclusion of such processing.

(2) The following hourly rates shall be used as a basis for calculating fees for public services pursuant to (1) Nos. 1, 5, 6, 7 and 8:

1. Civil servants in the intermediate service (*mittlerer Dienst*) or persons in comparable positions: DM 85,
2. Civil servants in the higher intermediate service (*gehobener Dienst*) or persons in comparable positions: DM 105,
3. Civil servants in the higher service (*höherer Dienst*) or persons in comparable positions: DM 135.

One quarter of these hourly rates shall be charged for each commenced quarter hour. If public services are provided outside of the authority’s location, by employees of the competent authority, fees shall also be charged for travel time during regular working hours or for travel that entails separate expenses for the competent authority; fees shall also be charged for waiting time caused by the party liable for costs.

(3) § 15 of the Administrative Expenses Act (*Verwaltungskostengesetz*) shall apply to cases in which an application for issuance of a license is rejected or withdrawn or in which a license is withdrawn or revoked. A fee may be charged for complete or partial rejection of an objection; the amount of this fee shall be no larger than the fee charged for the disputed administrative action. For rejection or retraction of an objection directed solely against a decision on costs, a fee may be charged whose amount shall be no larger than 10% of the disputed amount.

§ 3: Application procedure for issuance of certificates

(1) 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.

(2) 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. 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 invalidation pursuant to § 8 (1). Possession of any professional

license or other license must be proven through submission of the relevant license document.

§ 4: Notification of the applicant

(1) The certification authority shall notify applicants, in the framework of § 6 Sentences 1 and 3 of the Digital Signature Act, concerning the following necessary measures to ensure the security of digital signatures:

1. 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.

2. 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.

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.

6. If data are required in signed form for a prolonged period, a digital signature shall again be appended, pursuant to § 18.

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.

(2) If an applicant already has a certificate no further notification is required.

§ 5: Generation and storage of signature keys and identification data

(1) 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.

(2) 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.

§ 6: Handover of signature keys and identification data

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.

§ 7: Validity period for certificates

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.

§ 8: Public register of certificates

(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 register for at least as long as the algorithm listed in the certificate and its pertinent parameters are considered suitable pursuant to § 17 (2).

(2) The competent authority shall keep certificates issued by it in a register pursuant to the provisions of § 4 (5) Sentence 3 of the Digital Signature Act, for the duration of the period mentioned in (1). This shall also apply to certificates for public signature keys of foreign supreme certification authorities, where foreign certificates are recognised. For foreign certificates contained in the register, the competent authority shall confirm such recognition by means of a digital signature. The competent authority shall publish in the Federal Gazette the electronic addresses from which the certificates can be retrieved, along with their relevant public keys, and shall directly notify the certification authorities of such electronic addresses.

(3) 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).

§ 9: Procedures for invalidation of certificates

(1) 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 invalidation of the certificates, at any time; the certification authority shall also provide an authentication procedure for this purpose.

(2) The certification authority shall invalidate 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.

(3) Invalidation of certificates must be clearly indicated, with inclusion of the relevant date and time, in the register pursuant to § 8 of the Digital Signature Act, and may not be rescinded.

§ 10: Reliability of personnel

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.

§ 11: Protection of technical components

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.

§ 12: Security concept

(1) 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. The concept shall be changed without delay in cases of security-relevant changes.

(2) The competent authority shall keep a catalogue of suitable security measures, and shall publish this catalogue in the Federal Gazette. These measures shall be taken into account in the preparation of the security concept. The catalogue shall be prepared in keeping with provisions of the Federal Agency for Security in Information Technology (*Bundesamt für Sicherheit in der Informationstechnik*). Experts from the areas of industry and science shall be consulted in this regard.

§ 13: Documentation

(1) 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; invalidation 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.

(2) 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.

§ 14: Cessation of operation

(1) If the certification authority wishes to terminate its operation, pursuant to § 11 (1) of the Digital Signature Act, it must notify the competent authority of this intention at least four months in advance.

(2) Prior to cessation of its operation, the certification authority shall carry out the following for each certificate that has not been invalidated 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 invalidated that at this time are not already invalidated or have not already expired. The signature key holders of the certificates subject to invalidation shall be given relevant proper notification.

(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.

(4) The certification authority that assumes documentation pursuant to § 11 (2) of the Digital Signature Act, or the competent authority, shall keep the certificates in a register pursuant to § 8 (1) and (3).

§ 15: Checks of the certification authorities

(1) 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.

(2) 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.

§ 16: Requirements pertaining to technical components

(1) 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.

(2) 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.

(3) The technical components required for display of data for signing must function in such a manner that the signing person can reliably determine what data is to receive the signature; that a digital signature is provided only at the initiation of the signing person; 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 verifying person can reliably establish what data has received the digital signature; that the verifying person 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.

(4) The technical components used to store certificates in verifiable form, pursuant to § 4 (5) Sentence 3 or § 5 (1) Sentence 2 of the Digital Signature Act, must function in such a manner that only authorised persons can make entries and changes; that the invalidation 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 invalidated, in the register of certificates. 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.

(5) 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.

(6) The competent authority shall keep a catalogue of suitable security measures and shall publish this catalogue in the Federal Gazette. The measures shall be taken into account in the design of the technical components. The catalogue shall be prepared in keeping with specifications of the Federal Agency for Security in Information Technology (*Bundesamt für Sicherheit in der Informationstechnik*). Experts from the areas of industry and science shall be consulted for this purpose.

§ 17: Testing of technical components

(1) 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 "E 4" test standard; otherwise, they must conform to the "E 2" 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).

(2) 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. This date should be at least six years after the time of assessment and publication. The suitability shall be redetermined on a yearly basis and as required. Suitability shall be considered present if, throughout a certain time period, any undetectable forging of digital signatures or manipulation of signed data can be ruled out with near certainty, by means in keeping with current scientific and technological standards. 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.

(3) 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.

(4) 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.

§ 18: New digital signature

If data is required in signed form for a period longer than that for which the algorithms and pertinent parameters used to generate and verify the data pursuant to § 17 (2) are considered to be suitable, the data shall be given a new digital signature prior to the time at which the suitability of the algorithms and pertinent parameters ends. This signature must include new algorithms or pertinent parameters, must include earlier digital signatures and must bear a time stamp.

§ 19: Entry into force

This Ordinance enters into force on 1 November 1997.