

Digital Signature Act^{*)}

§1

Legislative Purpose and Scope

(1) 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.

(2) The application of other digital signature procedures is optional insofar as digital signatures according to this Act are not required by legal provisions.

§2

Definitions

(1) 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 owner of the signature key and the integrity of the data with the help of an associated public key provided with a signature key certificate of a certification authority or the authority according to §3 of this Act.

(2) 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.

(3) 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).

(4) 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.

§3

Competent Authority

^{*)} The notification requirements in Council Directive 83/189/EEC of 28 March 1983 laying down a procedure for the provision of information in the field of technical standards and regulations (OJ No L 109, p 8), last amended by Directive 94/10/EC of the European Parliament and the Council of 23 March 1994 (OJ No L 100, p 30) have been duly observed.

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.

§4

Licensing of Certification Authorities

(1) The operation of a certification authority shall require a licence from the competent authority. A licence shall be granted upon application.

(2) 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.

(3) Whosoever guarantees compliance, as a licensee, with the relevant legal provisions applicable to the operation of a certification authority shall be deemed to possess the necessary reliability. 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 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.

(4) 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.

(5) The competent authority shall issue the certificates for the signature keys used for affixing signatures to certificates. The provisions applicable to the issue of certificates by certification authorities shall apply accordingly to the competent authority. The competent authority shall keep the certificates which it has issued available for retrieval at all times and for everyone over publicly available telecommunication links. This shall also apply to information concerning addresses and call numbers of certification authorities, invalidation of certificates issued by the competent authority, cessation and prohibition of the exercise of the licensed activity and revocation of licences.

(6) Any public services rendered in accordance with this Act and the ordinance having the force of law pursuant to §16 shall be subject to costs (fees and expenses).

§5

Issue of Certificates

- (1) 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 owner of the signature key, for retrieval at all times and for everyone over publicly available telecommunication links.
- (2) 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.
- (3) At an applicant's request the certification authority shall indicate a pseudonym instead of the applicant's name in the certificate.
- (4) The certification authority shall take measures to prevent undetected forgery or manipulation of the data intended for certificates. 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.
- (5) 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 (1) sentence 2 above.

§6

Notification Requirement

The certification authority shall notify applicants according to §5(1) of the measures 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.

§7

Content of Certificates

- (1) The signature key certificate shall contain at least the following information:
 1. name of the owner of the signature key to which additional information must be appended in the event of possible confusion, or a distinctive pseudonym assigned to the owner of the signature key, clearly marked as such,

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

(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.

§8

Invalidation of Certificates

(1) The certification authority shall invalidate a certificate when the owner 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 invalidation is ordered by the competent authority pursuant to §13(5) sentence 2. The invalidation shall indicate the time at which it enters into effect. Retrospective invalidation shall not be permitted.

(2) Where a certificate contains third party information, this party may also request invalidation of the certificate.

(3) The competent authority shall invalidate certificates which it has issued according to §4(5) when a certification authority ceases operation or its licence is revoked.

§9

Time Stamp

Upon request the certification authority shall affix a time stamp to digital data. §5(5) sentences 1 and 2 shall apply accordingly.

§10

Documentation

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.

§11

Cessation of Operation

(1) Upon cessation of operation the certification authority shall notify the competent authority accordingly at the earliest possible time and shall ensure that the certificates valid at the time of cessation of operation are taken over by another certification authority or invalidated.

(2) It shall forward the documentation according to §10 to the certification authority taking over the certificates or otherwise to the competent authority.

(3) It shall notify the competent authority without undue delay of a bankruptcy petition or petition for institution of composition proceedings.

§12

Data Protection

(1) The certification authority may only collect personal data directly from the party concerned and only insofar as they are required for the purposes of a certificate. Collection of data from third parties shall be permitted only with the consent of the party concerned. The data may only be used for purposes other than those given in sentence 1 if this is permitted within the framework of this Act or another legal provision or if the party concerned has given its consent.

(2) Where the owner of a signature key uses a pseudonym, the certification authority shall upon request transmit data pertaining to his identity to the competent bodies insofar as this is required for the prosecution of criminal or administrative offences, for averting danger to public safety or order or for the discharge of legal functions by the federal and state authorities for the protection of the Constitution, the Federal Intelligence Service, the Federal Armed Forces Counter-Intelligence Office or the Customs Criminological Office. Such disclosures shall be documented.

(3) §38 of the Federal Data Protection Act shall apply subject to the proviso that verification may also be carried out when there is no indication of a violation of data protection provisions.

§13

Control and Enforcement of Obligations

(1) The competent authority may take measures vis-à-vis certification authorities to ensure compliance with this Act and the ordinance having the force of law. In particular, it may prohibit use of unsuitable technical components and may wholly or partially prohibit the exercise of the licensed activity for a temporary period of time. Parties who appear to have a licence according to §4 without this being the case may be prohibited from carrying out their certification activity.

(2) For purposes of monitoring according to (1) sentence 1 above certification authorities shall allow the competent authority to enter the production sites and business premises during normal business hours, shall upon request make available for inspection any relevant books, records, supporting documents, papers and any other documentation, shall disclose information and provide all necessary support. Whosoever is obliged to provide information may refuse to answer questions which would render himself or a person related by blood affinity as specified in §383(1) subparagraphs 1 to 3 of the Code of Civil Procedure liable to prosecution or proceedings under the Administrative Offences Act. Any person obliged to answer inquiries shall be advised of this right.

(3) In the event of non-fulfillment of obligations arising under this Act or the ordinance having the force of law or in the event of a reason for denial of a licence the competent authority shall revoke the licence when measures according to (1) sentence 2 above are unlikely to be successful.

(4) In the event of withdrawal or revocation of a licence or cessation of operation of a certification authority the competent authority shall ensure transfer of the activity to another certification authority or winding up of the contracts with the owners of signature keys. This shall also apply when a bankruptcy petition or a petition for institution of composition proceedings is filed and the licensed activity is discontinued.

(5) The validity of the certificates issued by a certification authority shall remain unaffected by revocation of a licence. The competent authority may order the invalidation of certificates when facts warrant the assumption that certificates have been forged or are not adequately protected against forgery or when technical components used for the signature keys reveal security flaws enabling digital signatures to be forged or signed data to be manipulated without detection.

§14

Technical Components

(1) 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.

(2) 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 owner of the signature key to whom the digital signature belongs to be established.

(3) 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.

(4) Technical components according to (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.

(5) 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 in another State party to the Agreement on the European Economic Area which ensure the same level of security shall be assumed to fulfil the technical security requirements according to (1) to (3) above. 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 (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.

§15

Certificates Issued by Other Countries

(1) 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.

(2) Paragraph (1) above shall also apply to other states insofar as supra-national or intergovernmental agreements have been concluded on the recognition of certificates.

§16

Ordinance Having the Force of Law

The Federal Government shall be empowered, by ordinance having the force of law, to issue the legal provisions required for implementation of §§ 3 to 15 with respect to

1. further details of the procedure pertaining to the granting, transfer and revocation of a licence and the procedure upon cessation of the licensed activity,
2. chargeable acts according to §4(6) and the level of the fee,

3. further details of the obligations of certification authorities,
4. validity periods of signature key certificates,
5. further details of the control over certification authorities,
6. detailed requirements applicable to technical components, their testing, and confirmation of compliance with the requirements,
7. the period after which a new digital signature should be affixed and the associated procedure.