Law Governing Framework Conditions for Electronic Signatures and Amending Other Regulations

inofficial version for industry consultation
for official German text please refer to the Official Journal
(Bundesgesetzblatt – BGBl. Teil I S. 876 vom 21. Mai 2001)

. . .

The German Bundestag has adopted the following Law:

Article 1
Law Governing Framework Conditions for Electronic Signatures (Signatures Law - SigG)[1]

Contents

[1] Information requirements under Directive 98/34/EC of the European Parliament and the Council of 22 June 1998 on an information procedure in the field of norms and technical requirements (OJ EC No. L 204, p. 37 of 21 July 1998) last amended by Directive 98/48/EC of the European Parliament and the Council of 20 July 1998 (OJ EC No. L 217, p. 18 of 5 August 1998) have been observed.

Part One: General Provisions

Section 1: Purpose and Area of Application

(1) The purpose of this Law is to create framework conditions for electronic signatures.

(2) Where electronic signatures are not specifically required by law their use shall be voluntary.

(3) Legal provisions may require compliance with additional conditions for the use of qualified electronic signatures for public administrative activities. These conditions shall be objective, proportionate, and non-discriminatory, and shall relate only to the specific characteristics of the relevant applications.

Section 2: Definition of Terms

For the purposes of this Law

1. "Electronic signatures" shall be data in electronic form that are attached to other electronic data or logically linked to them and used for authentication;

2. "Advanced electronic signatures" shall be electronic signatures as in 1. above that
   a) are exclusively assigned to the owner of the signature code
   b) enable the owner of the signature code to be identified
   c) are produced with means which the owner of the signature code can keep under his sole control and
   d) are so linked to the data to which they refer that any subsequent alteration of such data may be detected;

3. "Qualified electronic signatures" shall be electronic signatures as in 2. above that
   a) are based on a qualified certificate valid at the time of their creation and
   b) have been produced with a secure signature-creation device;

4. "Signature codes" shall be unique electronic data such as private cryptographic codes that are used to create an electronic signature;

5. "Signature test codes" shall be electronic data such as public cryptographic codes that are used to test an electronic signature;

6. "Certificates" shall be electronic certificates assigning signature test codes to a person and confirming his or her identity;

7. "Qualified certificates" shall be electronic certificates pursuant to 6. above for natural persons that fulfill the requirements in Section 7 and are issued by certification-service providers who meet at least the requirements under Sections 4 to 14 or Section 23 of this Law and the provisions of the statutory ordinance pursuant to Section 24 that are based on this Law;

8. "Certification-service providers" shall be natural persons or legal entities who issue qualified certificates or qualified time stamps;

. . .

9. "Signature-code owners" shall be natural persons who own signature codes and to whom the appropriate signature test codes have been assigned in qualified certificates;

10. "Secure signature-creation devices" shall be software or hardware products used to store and apply the respective signature code, that meet or exceed the requirements of Section 17 or Section 23 of this Law and the provisions of the statutory ordinance pursuant to Section 24 that are based on this Law, and that are designed for qualified electronic signatures;

11. "Signature-application components" shall be software and hardware products designed to
    a) assign data to the process of producing or testing qualified electronic signatures or
    b) test qualified electronic signatures or check qualified certificates and display the results;

12. "Technical components for certification services" shall be software or hardware products designed to
    a) create signature codes and transfer them into a secure signature-creation device
    b) keep qualified certificates available for testing and, if necessary, downloading by the public, or
    c) produce qualified time stamps;

13. "Products for qualified electronic signatures" shall be secure signature-creation devices, signature-application components, and technical components for certification services;

14. "Qualified time stamps" shall be electronic certificates issued by a certification-service provider that meet or exceed the requirements under Sections 4 to 14 and Section 17 or Section 23 of this Law and the provisions of the statutory ordinance pursuant to Section 24 that are based on this Law, and that confirm that certain electronic data have been presented to it at a certain time;

15. "Voluntary accreditation" shall be a procedure to issue a permit that authorizes the operation of a certification service and confers specific rights and obligations.

Section 3: Competent Authority

The tasks of the competent authority under this Law and the statutory ordinance under Section 24 shall be performed by the authority named in Section 66 of the Telecommunications Act.

Part Two: Certification-Service Providers

Section 4: General Requirements

(1) The operation of a certification service shall not require approval under current law.

(2) Only those who can prove that they have the necessary reliability and specialized knowledge may operate as certification-service providers. They shall also show that they have cover under Section 12 and fulfill the other conditions for the operation of a certification service under this Law and the statutory ordinance under Section 24 (1), (3), and (4). An applicant shall have the necessary reliability if he can guarantee that as certification-service provider he will observe the legal regulations governing this operation. The necessary specialized knowledge shall be available if the persons who will work in the certification-service office have the knowledge,

. . .

experience, and skills needed for this work. The other conditions for operating a certification service shall be met if the measures to fulfill the security requirements under this Law and the statutory ordinance under Section 24 (1), (3), and (4) have been presented to the competent authority in a secure concept, are appropriate, and have been implemented in practice.

(3) Anyone commencing to operate a certification service shall report this to the competent authority at the latest when commencing operation. The report shall include appropriate proof that the conditions under (2) have been met.

(4) It shall be ensured that the conditions under (2) can be fulfilled throughout the entire duration of operation as certification-service provider. Circumstances that render this impossible shall be reported to the competent authority without delay.

(5) The certification-service provider may transfer work under this Law and the statutory ordinance under Section 24 to third parties if this is included in his security concept under (2) Sentence 4.

Section 5: Issue of Qualified Certificates

(1) The certification-service provider shall reliably identify persons who apply for a qualified certificate. He shall confirm the assignment of a signature-test code to an identified person with a qualified certificate and ensure that this can be examined and downloaded by anyone at any time using public telecommunication links. A qualified certificate may only be kept accessible for downloading with the approval of the signature-code owner.

(2) If requested by an applicant, a qualified certificate may contain data on his authorization to act for a third party and occupational or other data on his person (attributes). In regard to the data on the authorization to act for a third party, the approval of this person must be proven; occupational or other data on the person must be confirmed by the office responsible for the occupational or other data. Data on the authorization to act for a third party may only be included in a qualified certificate if proof of this party's approval is given as stated in Sentence 2; occupation or other data on the person from the applicant may be included only if the approval is presented in accordance with Sentence 2. Other personal data may be included in a qualified certificate only with the approval of the person concerned.

(3) If requested by the applicant the certification-service provider shall use a pseudonym instead of his name in the qualified certificate. If a qualified certificate contains data on the authorization to act for a third party or occupational or other data on the person, the approval of the third party or the office responsible for the occupational or other data shall be required for the pseudonym to be used.

(4) The certification-service provider shall make arrangements to ensure that data for qualified certificates cannot be falsified or forged without detection. He shall also take steps to ensure that the signature codes are kept secret. Signature codes may not be stored outside the secure signature-creation device.

(5) For the purposes of certifying qualified electronic signatures, the certification-service provider shall employ reliable personnel and products that meet the requirements under Sections 4 to 14 and Section 17 or Section 23 of this Law and the statutory ordinance pursuant to Section 24.

(6) The certification-service provider shall obtain suitable proof that the applicant owns the relevant secure signature-creation device.

Section 6: Information Obligations

(1) The certification-service provider shall inform the applicant under Section 5(1) of the measures needed to increase the security of qualified electronic signatures and to test them reliably. He shall remind the applicant that data with a qualified electronic signature may have to be signed again lest the security value of the current signature be reduced by the passage of time.

(2) The certification-service provider shall inform the applicant that a qualified electronic signature has the same effect in legal transactions as a handwritten signature unless otherwise specified by law.

(3) To fulfill the information obligations under (1) and (2), the applicant shall be given a written information sheet and confirm by separate signature that he has read and taken note of this. If an applicant has already been informed pursuant to (1) and (2), further information shall not be necessary.

Section 7: Contents of Qualified Certificates

(1) A qualified certificate shall contain the following data and bear a qualified electronic signature:

1. The name of the signature-code owner, to which a supplement shall be added if there is a possibility of confusion with another name, or an unmistakable pseudonym assigned to the signature-code owner and recognizable as such;
2. The assigned signature-test code;
3. The designation of the algorithms with which the signature-test code of the signature-code owner and the signature-test code of the certification-service provider may be used;
4. The current number of the certificate;
5. The start and end of its validity;
6. The name of the certification-service provider and the state in which he is domiciled;
7. Information on whether the use of the signature code is limited to certain applications by nature or extent;
8. Information that this is a qualified certificate; and
9. If necessary, attributes of the signature-code owner.

(2) Attributes may also be included in a separate qualified certificate (qualified attribute certificate). In a qualified attribute certificate, the data under (1) may be replaced with clear reference data from the qualified certificate to which it refers, where this is not needed to use the qualified attribute certificate.

Section 8: Invalidating Qualified Certificates

(1) The certification-service provider shall invalidate a qualified certificate without delay if a signature-code owner or his representative so demands, if the certificate was issued on the basis of false data on Section 7, if the certification-service provider has ceased to operate and the operation is not being continued by another certification-service provider, or if the competent authority orders the certificate invalidated in accordance with Section 19(4). The invalidation must state the time from which it applies. Invalidation with backdated effect is not permitted.

. . .

If a qualified certificate was issued with false data, the certification-service provider may also make this known.

(2) If a qualified certificate contains data under Section 5(2), the third party or the office responsible for the occupational or other data on the person may demand invalidation of the certificate in question under (1) if the conditions for the occupational or other data on the person cease to apply after being included in the qualified certificate.

Section 9: Qualified Time Stamps

If a certification-service provider issues a qualified time stamp, Section 5(5) shall apply mutatis mutandis.

Section 10: Documentation

(1) The certification-service provider shall document the security measures taken to observe this Law and the statutory ordinance under Section 24 Nos. 1 and 3, and document the qualified certificates issued in accordance with Sentence 2 so that the data and their correctness may be confirmed at any time. The documentation shall be made without delay, and in such a manner that it cannot subsequently be altered without detection. This shall particularly apply to the issuance and invalidation of qualified certificates.

(2) Upon request, the signature-code owner shall be given access to the data and the procedural steps concerning him.

Section 11: Liability

(1) If a certification-service provider infringes the requirements under this Law and the statutory ordinance under Section 24, or if his products for qualified electronic signatures or other technical security facilities fail, he shall reimburse a third party for any damage suffered from relying on the data in a qualified certificate or a qualified time stamp or on information given in accordance with Section 5(1) Sentence 2. Damages shall not be payable if the third party knew, or must have known, that the data was faulty.

(2) Damages need not be reimbursed if the certification-service provider has incurred no culpability.

(3) If a qualified certificate restricts the use of the signature code to certain applications by type or extent, damages shall be payable only within the limits of these restrictions.

(4) The certification-service provider shall be liable for third parties commissioned under Section 4(5) and when guaranteeing foreign certificates under Section 23(1) No. 2 as for his own actions. Section 831(1) Sentence 2 of the German Civil Code shall not apply.

Section 12: Cover

The certification-service provider shall be obliged to make appropriate cover provisions to ensure that he can meet his statutory obligations for reimbursement of damages caused by an infringement by him of the requirements or products of this Law or the statutory ordinance under Section 24, or if his products for qualified electronic signatures or other technical security facilities fail. The minimum amount shall be 500,000 deutschmarks for damages caused by an occurrence of the kind described in Sentence 1 for which he is liable.

Section 13: Cessation of Operations

(1) The certification-service provider shall report the cessation of his operations to the competent authority without delay. He shall ensure that the qualified certificates that are still valid when he ceases to operate will be taken over by another certification-service provider or invalidate them. He shall inform the signature-code owners concerned that he is ceasing to operate and that the qualified certificates are being taken over by another certification-service provider.

(2) The certification-service provider shall hand over the documentation under Section 10 to the certification-service provider who is taking over the certificates under (1). If no other certification-service provider takes over the documentation, the competent authority shall do so. In response to legitimate interest, the competent authority shall provide information on the documentation pursuant to Sentence 2 if this is technically possible and does not require an overproportionate amount of effort.

(3) The certification-service provider shall inform the competent authority without delay of an application to open insolvency proceedings.

Section 14: Data Protection

(1) The certification-service provider may only obtain data on persons directly from these persons and only to the extent necessary to issue a qualified certificate. Obtaining data from third parties shall only be permitted with the consent of the person concerned. The data may only be used for purposes other than those given in Sentence 1 if this Law permits or the person concerned gives his consent.

(2) In the case of a signature-code owner with a pseudonym, the certification-service provider shall hand the data on his identity to the competent authority upon request, where this is necessary for the prosecution of criminal acts or infringement of regulations, to avoid risk to public security or order or to fulfill the tasks legally required of the constitutional protection agencies of the federal government and the individual states, the Federal Secret Service, military defense, or the fiscal authorities, or insofar as the courts order this as part of proceedings pending and pursuant to the appropriate statutory provisions. The information shall be documented. The authority requesting the information shall inform the signature-code owner that his pseudonym has been revealed as soon as this will not restrict the performance of its legal duties, or if the interests of the signature-code owner in being informed outweigh the other considerations.

(3) Where certification-service providers other than those named in Section 2 No. 8 issue certificates for electronic signatures, (1) and (2) shall apply mutatis mutandis.

Part Three: Voluntary Accreditation

Section 15: Voluntary Accreditation of Certification-Service Providers

(1) Certification-service providers may be accredited by the competent authority upon application; the competent authority may make use of private offices for the accreditation. Accreditation shall be given if the certification-service provider can show that the requirements under this Law and the statutory ordinance under Section 24 are fulfilled. Accredited certification-service providers will be given a quality sign by the competent authority. This shall be proof that the qualified electronic signatures (qualified electronic signatures with provider accreditation) based on their qualified certificates offer security that has been comprehensively tested technically and administratively. They shall be allowed to call themselves accredited certification-service providers and refer to the proven security in legal and business transactions.

(2) To fulfill the requirements under (1), the security concept under Section 4(2) Sentence 4 shall be comprehensively tested for its suitability and practical implementation and approved by an office under Section 18. The testing and approval shall be repeated after any changes that greatly affect security, and at regular intervals of time.

(3) The accreditation may be given with conditions attached where this is necessary to ensure fulfillment of the requirements under this Law and the statutory ordinance under Section 24 upon commencement of and during operations.

(4) The accreditation shall be refused if the conditions under this Law and the statutory ordinance under Section 24 are not fulfilled; Section 19 shall apply mutatis mutandis.

(5) If the requirements under this Law or the statutory ordinance under Section 24 are not fulfilled, or if there is reason to refuse accreditation under (5), the competent authority shall revoke the accreditation or, if the reasons were already given when the accreditation was accorded, withdraw it if measures under Section 19(2) would not appear likely to succeed.

(6) If an accreditation is revoked or withdrawn, or if an accredited certification-service provider ceases to operate, the competent authority shall ensure that his operations are taken over by another accredited certification-service provider or that the contracts with the signature-code owners can be handled. This shall also apply if the application is made to open insolvency proceedings, if the operations are not continued. If no other accredited certification-service provider is taking over the documentation in accordance with Section 13(2), the competent authority shall take it over. Section 10(1) Sentence 1 shall apply mutatis mutandis.

(7) In the case of products for electronic signatures, fulfillment of the requirements under Section 17(1 to 3) and the statutory ordinance under Section 24 shall be adequately tested with state-of-the-art science and technology and confirmed by an office under Section 18; (1) Sentence 3 shall apply mutatis mutandis. The accredited certification-service provider shall

1. Only use products and qualified electronic signatures in his certification operations that have been tested and approved pursuant to Sentence 1;
2. Only issue qualified certificates for persons who can prove that they have secure signature-creation devices that have been tested and approved in accordance with Sentence 1; and
3. Inform the signature-code owners of signature-application components that have been tested and confirmed in accordance with Sentence 1, within the framework of Section 6(1).

. . .

Section 16: Certificates from the Competent Authority

(1) The competent authority shall issue the accredited certification-service providers with the qualified certificates they need for their operations. The regulations for the issuance of qualified certificates by accredited certification-service providers shall apply mutatis mutandis for the competent authority. It shall invalidate qualified certificates it has issued if an accredited certification-service provider ceases to operate or if an accreditation is withdrawn or revoked.

(2) The competent authority shall ensure that

1. The names, addresses, and communication links of the accredited certification-service providers
2. The revocation or withdrawal of an accreditation
3. The qualified certificates it has issued and their invalidation and
4. The cessation of operations by an accredited certification-service provider and a ban on these

are available to be checked and downloaded at any time by anyone using public communication links.

(3) If necessary, the competent authority shall also issue the electronic certificates needed by the certification-service providers or producers for the automatic authentication of products under Section 15(7).

Part Four: Technical Security

Section 17: Products for Electronic Signatures

(1) To store signature codes and to produce qualified electronic signatures, secure signature-creation devices shall be used that will reliably identify forged signatures and false signed data and offer protection against unauthorized use of the signature codes. If the signature codes are themselves produced on a secure signature-creation device, (3) No. 1 shall apply mutatis mutandis.

(2) The presentation of data to be signed requires signature-application components that will first clearly indicate the production of a qualified electronic signature and enable the data to which the signature refers to be identified. To check signed data, signature-application components are needed that will show

1. To which data the signature refers
2. Whether the signed data are unchanged
3. To which signature-code owner the signature is to be assigned
4. The contents of the qualified certificate on which the signature is based, and of the appropriate qualified attribute certificates, and
5. The results of the subsequent check of certificates under Section 5(1) Sentence 2.

Signature-application components shall, if necessary, also make the contents of the data to be signed or already signed sufficiently evident. The signature-code owners should use these signature-application components or take other suitable steps to secure qualified electronic signatures.

. . .

(3) The technical components for certification services shall contain provisions to

1. Ensure that signature codes produced and transferred are unique and secret and exclude storage outside the secure signature-creation device
2. Protect qualified certificates that are available to be tested or downloaded in accordance with Section 5(1) Sentence 2 from unauthorized alteration and unauthorized downloading, and
3. Exclude the possibility of forgery and falsification in the production of qualified time stamps.

(4) Confirmation shall be given by an office under Section 18 that the requirements under (1) and (3) No. 1 and the statutory ordinance under Section 24 have been fulfilled. To fulfill the requirements under (2) and (3) Nos. 2 and 3, a declaration by the manufacturer of the product for electronic signatures is sufficient.

Section 18: Recognition of Testing and Confirmation Offices

(1) The competent authority shall recognize a natural person or a legal entity upon application as confirmation office under Section 17(4) or Section 15(7) Sentence 1 or as a testing and confirmation office under Section 15(2) if it can prove it has the reliability, independence, and specialized knowledge needed to exercise these functions. The recognition may be limited in content, be preliminary, or be given for a limited period of time; conditions may also be attached.

(2) The offices recognized under (1) shall perform their tasks impartially, free of instruction, and conscientiously. They shall document the tests and confirmations and hand over this documentation to the competent authority if they cease to operate.

Part Five: Supervision

Section 19: Supervision Measures

(1) Supervision of observance of this Law and the statutory ordinance under Section 24 shall be the responsibility of the competent authority; it may use private entities to perform this supervision. A certification-service provider shall be subject to supervision by the competent authority when he commences to operate.

(2) The competent authority may take steps in regard to certification-service providers to ensure observance of this Law and the statutory ordinance under Section 24.

(3) The competent authority shall forbid a certification-service provider to operate temporarily, in part or wholly if facts justify the assumption that it

1. Does not have the reliability necessary to operate as certification-service provider;
2. Cannot prove that the specialized knowledge necessary for its operations is available;
3. Does not have the necessary cover;
4. Is using unsuitable products for electronic signatures;
5. Does not fulfill the other conditions to operate as certification-service provider under this Law and the statutory ordinance under Section 24

and if measures under (2) are not likely to succeed.

(4) The competent authority may order qualified certificates to be invalidated if facts justify the assumption that qualified certificates are forged or are not sufficiently secure against forgery, or that secure signature-creation devices have security defects that would enable qualified electronic signatures to be forged without detection or the falsification of data signed with these to go undetected.

(5) The validity of qualified certificates issued by a certification-service provider shall not be affected by a ban on his operations and cessation of operations or by withdrawal and revocation of an accreditation.

(6) The competent authority shall keep the names of the certification-service providers registered with it and of the certification-service providers that have ceased to operate under Section 13, or whose operations have been forbidden under Section 19(3), available for downloading through public communication links available to anyone.

Section 20: Obligatory Cooperation

(1) The certification-service providers and the third parties working for them under Section 4(5) shall permit the competent authority and the persons acting on its behalf to enter their premises and workshops during normal operating hours and upon request present for inspection the relevant books, records, vouchers, written material, and other documents in a suitable manner, including those in electronic form, and give information and the necessary support.

(2) The person obliged to give information may refuse to answer questions if this would expose him or a person connected with him as described in Section 383(1) Nos. 1 to 3 of the Order on Civil Proceedings to the risk of criminal prosecution or proceedings under the Law on Infringements of Regulations. He shall be informed of this right.

Part Six: Final Regulations

Section 21: Fines

(1) A person infringes regulations who deliberately or negligently

1. Operates a certification service in violation of Section 4(2) Sentence 1, or in connection with a statutory ordinance under Section 24 Nos. 1, 3, and 4;
2. In violation of Section 4(3) Sentence 1 or Section 13(1) Sentence 1 does not report his operation, reports it incorrectly, or not within the required time;
3. In violation of Section 5(1) Sentence 1 in connection with a statutory ordinance under Section 24 No. 1 does not identify a person, or does so incorrectly, or not within the required time;
4. In violation of Section 5(1) Sentence 2 and in connection with a statutory ordinance under Section 24 No. 1 does not keep a qualified certificate available for testing;
5. In violation of Section 5(1) Sentence 3 makes a qualified certificate available for downloading;
6. Includes information in a qualified certificate in violation of Section 5(2) Sentences 3 or 4;
7. In violation of Section 5(4) Sentence 2 and in connection with a statutory ordinance under Section 24 No.1 fails to take certain steps or does not take them correctly;
8. Stores a signature code in violation of Section 5(4) Sentence 3;

. . .

9. In violation of Section 10(1) Sentence 1 and in connection with a statutory ordinance under Section 24 No.1 fails to document a security measure or a qualified certificate or does so incorrectly or not within the required time;
10. In violation of Section 13(1) Sentence 2 and in connection with a statutory ordinance under Section 24 No.1 fails to ensure that a qualified certificate is taken over by another certification-service provider and fails to invalidate a qualified certificate or does not do so at the right time; or
11. In violation of Section 13(1) Sentence 3 in connection with a statutory ordinance under Section 24 No.1 fails to inform a signature-code owner or does so incorrectly or not within the required time.

(2) Violation of the regulations may carry a fine of up to one hundred thousand deutschmarks in cases in (1) Nos.1, 7, and 8, and in the other cases a fine of up to twenty thousand deutschmarks may be imposed.

(3) The administrative authority as defined under Section 36(1) No.1 of the Law on Infringements of Regulations shall be the Regulatory Authority for Telecommunications and Posts.

Section 22: Costs and Contributions

(1) The competent authority shall charge costs for the following official duties (fees and expenditure):
1. Measures as part of the voluntary accreditation of certification-service providers under Section 15 and the statutory ordinance under Section 24;
2. Measures as part of the issue of qualified certificates under Section 16(1) and the issue of certificates under Section 16(3).
3. Measures as part of the recognition of testing and confirmation offices under Section 18 and the statutory ordinance under Section 24.
4. Measures as part of the supervision under Section 19(1to 4) in conjunction with Section 4(2 to 4) and the statutory ordinance under Section 24.

Costs shall also be charged for the administration expenditure incurred if the authority uses private offices to perform the supervision. The Law on Administrative Costs shall apply.

(2) Certification-service providers who have reported the commencement of operations under Section 4(3) shall pay a levy to the competent authority to cover the administrative expenditure for the continuous fulfillment of the conditions under Section 19(6); this shall be charged as an annual contribution. Certification-service providers accredited under Section 15(1) shall pay a levy to the competent authority to cover the administrative expenditure for the continuous fulfillment of the conditions under Section 16(2); this shall be charged as an annual contribution.

Section 23: Foreign Electronic Signatures and Products for Electronic Signatures

(1) Electronic signatures for which a foreign qualified certificate has been issued by another member state of the European Union or signatory to the Treaty on the European Economic Area shall be the equivalent of qualified electronic signatures if they correspond to Article 5(1) of Directive 1999/93 EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures (OJ EC 2000 No. L 13, p. 2) in the current version. Electronic signatures from third countries shall be the equivalent of qualified electronic signatures if the certificate is issued publicly as a qualified certificate by a certification-service

provider in that country and is designed for an electronic signature in the meaning of Article 5(1) of Directive 1999/93 EC, and if

1. The certification-service provider fulfills the requirements of the Directive and is accredited in a member state of the European Union or another signatory to the Treaty on the European Economic area, or if
2. A certification-service provider domiciled in the EU and meeting the requirements of the Directive guarantees the certificate, or if
3. The certificate or the certification-service provider is recognized under a bilateral or multilateral agreement between the European Union and third countries or international organizations.

(2) Electronic signatures under (1) shall be the equivalent of qualified electronic signatures with provider accreditation under Section 15(1) if they can prove that they offer equivalent security.

(3) Products for electronic signatures shall be recognized if it has been established in another EU Member State or another signatory to the Treaty on the European Economic Area that they meet the requirements of Directive 1999/93 EC in its current version. Products for qualified electronic signatures tested under Section 15(8) shall be regarded as the equivalent of products for electronic signatures from a country named in Sentence 1 or a third country if they can prove that they offer the same security.

Section 24: Legal Regulations

The federal government shall be empowered to issue the regulations necessary to implement Sections 3 to 23 by statutory ordinance on

1. The details of the duties of the certification-service providers in regard for the commencement of operations and during operation and upon cessation of operation under Section 4 (2 and 3), Sections 5, 6(1), and Sections 8, 10, 13, and 15
2. The items on which fees are payable and the rates for these fees, and the level of contributions and the procedure for levying these charges by the competent authority; the assessment of the contributions must be based on the administrative expenditure (personnel and material) and the investment where this has not already been covered by a fee
3. The details of the contents and period of validity of qualified certificates under Section 7
4. The reserves permitted to meet the obligations for cover provisions under Section 12, as well as their volume, level, and contents
5. The detailed requirements for products for qualified electronic signatures under Section 17(1 to 3) and the testing of these products, and the confirmation that the requirements have been fulfilled, under Section 17(4) and Section 15(7)
6. The details of the procedure for recognition and the work of testing and confirmation offices under Section 18
7. The period after which data with a qualified electronic signature under Section 6(1) Sentence 2 must be signed again and the procedure for doing this
8. The procedure to establish the equivalent security of foreign electronic signatures and foreign products for electronic signatures under Section 23.

Section 25: Transitional Regulations

(1) The certification offices approved under the Signatures Law of 28 July 1997 (BGBl. I, pp. 1870, 1872), amended by Article 5 of the Law of 19 December 1998 (BGBl. I, p. 3836), shall be regarded as accredited within the meaning of Section 15. They shall present proof of cover in accordance with Section 12 to the competent authority within three months of this Law coming into force.

(2) The certificates issued by certification offices under (1) up to the time when this Law comes into force under Article 5 of the Signatures Law of 28 July 1997 (BGBl. I, pp. 1870, 1872), amended by Article 5 of the Law of 19 December 1998 (BGBl. I, p. 3836), shall be the equivalent of qualified certificates. Owners of certificates under Sentence 1 shall be informed in an appropriate manner within six months of this Law coming into force, by the certification office in accordance with Section 6(2) Sentences 1 and 2.

(3) The recognition by the competent authority of testing and confirmation offices under Section 4(3) Sentence 3 and Section 14(4) of the Signatures Law of 28 July 1997 (BGBl. I, pp. 1870, 1872), amended by Article 5 of the Law of 19 December 1998 (BGBl. I, p. 3836), shall remain valid if they are in accordance with Section 18 of this Law.

(4) Technical components whose compliance with the requirements in Section 14(4) of the Signatures Law of 28 July 1997 (BGBl. I, pp. 1870, 1872) has been tested and confirmed shall be products for qualified electronic signatures under Section 15(7) of this Law.

Article 2
Conversion of Regulations to Euro

The Signatures Law of . . . (BGBl. I, pp. . .) shall be amended as follows:

1. In Section 12 Sentence 2 "500,000 deutschmarks" shall be replaced by "250,000 euros."
2. In Section 21 the words "a hundred thousand deutschmarks" shall be replaced by the words "fifty thousand euros" and the words "twenty thousand deutschmarks" by the words "ten thousand euros."

Article 3
Adjustment of Federal Law

(1) In Section 15 Sentence 2 of the Ordinance on the Issue of Public Orders of 9 January 2001 (BGBl. I, p. 110) the words "signature in the meaning of the Signatures Law" shall be replaced by the words "a qualified electronic signature under the Signatures Law."

(2) In Section 7(3) of the Ordinance on Social Insurance of 15 July 1999 (BGBl. I, p. 1627) the words "digital signature under Section 2(1) of the Signatures Law (Article 3 of the Law of 22 July 1997, BGBl. I, pp. 1870, 1872)" shall be replaced by the words "a qualified electronic signature under the Signatures Law."

Article 4
Return to a Uniform Order of Regulations

The parts of the statutory ordinance based on Article 3(1 and 2) and amended therein may be amended by statutory ordinance on the basis of the relevant authorizations.

Article 5
Coming into Force / Annulment of Legislation

This Law, with the exception given in Sentence 2, shall enter into force on the day after its publication; at the same time, the Signatures Law of 28 July 1997 (BGBl. I, pp. 1870, 1872), amended by Article 5 of the Law of 19 December 1998 (BGBl. I, p. 3836), shall be annulled. Article 2 shall enter into force on 1 January 2002.