Federal Electronic Signature Law

(Signature Law - SigG)

Section I

Purpose and definitions

Purpose and scope

§ 1. (1) The present federal law sets out the legal framework governing the creation and use of electronic signatures and the provision of signature and certification services.

(2) The present federal law shall apply in closed systems, insofar as the parties within the system have so agreed, and in open electronic transactions with courts and other authorities unless a law stipulates otherwise.

Definitions

§ 2. The following definitions shall apply for the purposes of the present federal law:

1. **Electronic signature**: electronic data attached to or logically linked with other electronic data which serve to authenticate, that is establishing the identity of the signatory.

2. **Signatory**: a natural person to whom the signature creation data and the corresponding signature verification data have been allocated and who creates an electronic signature either on his own or on a third party's behalf, or a certification service provider who uses certificates to provide certification services.

3. **Secure electronic signature**: an electronic signature which

a) is allocated solely to the signatory,

b) allows the signatory to be identified,

c) is created using devices under the signatory's sole control;

d) is linked with the data to which it refers to in a way which allows any subsequent change to the data to be identified and

e) is based on a qualified certificate and is created using technical components and procedures which comply with the security requirements of the present federal law and the orders issued on the basis thereof.

4. **Signature creation data**: unique data such as codes or private signature keys which are used by the signatory to create an electronic signature.

5. **Signature creation device**: configured software or hardware which is used to implement the signature creation data.

6. **Signature verification data**: data such as codes or public signature keys which are used to verify an electronic signature.

7. **Signature verification device**: configured Software or hardware which is used to process the signature verification data.

8. **Certificate**: electronic confirmation in which signature verification data are linked to a specific person whose identity is certified.

9. **Qualified certificate**: a certificate containing the information referred to in § 5 and issued by a certification Service provider which meets the requirements of § 7,

10. **Certification service provider**: a natural or juristic person or some other legally capable Institution which issues certificates or provides other signature and certification services.

11. **Signature and certification services**: the provision of signature products and procedures, the issuing, renewal and administration of certificates, the provision of directory-, revocation-, registration-, time stamping-, computing- and consultancy- services in connection with electronic signatures.

12. **Time stamp**: electronically signed confirmation from a certification service provider that specific electronic data were submitted at a specific time.

13. **Signature product**: hardware or software or the specific components thereof used to create and verify electronic signatures or used by a certification service provider to provide signature or certification services.

14. **Compromise**: breach of security measures or security technique so that the level of security set up by the certification service provider no longer applies.

Section 2

Relevancy in law of electronic signatures

General legal effects

§ 3. (1) Signature procedures with different levels of security and different classes of certificates can be used for legal or commercial transactions.

(2) The legal effects of an electronic signature and its use as evidence cannot therefore be excluded merely by reason of the fact that the electronic signature is only available in electronic form, is not based on a qualified certificate or on a qualified certificate issued by an accredited certification service provider or was not created using the technical components and procedures as defined in § 18.

Specific legal effects

§ 4. (1) A secure electronic signature meets the legal requirement for a hand-written signature especially the requirement for the written form as defined in § 886 of the Austrian Civil Code unless a different definition is laid down by law or by an agreement between the parties.

(2) A secure electronic signature does not have the legal effects of the written form as defined in § 886 of the Austrian Civil Code in the case of:

1. legal transactions under family and inheritance law which require the written form or a stricter formal requirement;

2. other declarations of intent or legal transactions which require official certification, judicial or notarial authentication or a notarial deed in order to be valid;

3. declarations of intent, legal transactions or petitions which require official certification, judicial or notarial authentication or a notarial deed in order to be entered in the land register, companies register or other official register or

4. declarations of guarantee (§ 1346 para. 2 of the Austrian Civil Code).

(3) The provisions of § 294 of the Code of Civil Procedure governing the presumption of authenticity of the content of a signed private deed shall apply to electronic documents bearing a secure electronic signature.

(4) The legal effects of paragraphs 1 and 3 shall not apply if it is proven that the security requirements of the present federal law and the orders issued on the basis thereof have not been complied with or the precautions taken in order to comply with the said security requirements have been compromised.

Qualified certificates

§ 5. (1) A qualified certificate shall contain at least the following information:

1. an indication that it is a qualified certificate;

2. the unmistakable name of the certification service provider and its country of establishment;

3. the name of the signatory or a pseudonym, which must be indicated as such;

4. where necessary at the request of the applicant, information on a power of attorney or other significant legal attribute of the signatory;

5. the signature verification data allocated to the signatory;

6. the beginning and end of the period of validity of the certificate;

7. a uneque identification of the certificate;

8. where necessary, a restriction on the scope of the certificate and

9. where necessary, a limitation on the transaction value for which the certificate has been issued.

(2) Other important legal information may be included in a qualified certificate at the applicant' s request.

(3) Qualified certificates must bear the certification service provider' s secure electronic signature.

Section 3

Certification service providers

Activities of certification service providers

§ 6. (1) Certification service providers shall require no special permit to establish and exercise their activities.

(2) Certification service providers shall immediately notify the supervisory body (§ 13) of the establishing of activities and shall file a security policy and a certification policy for each signature and certification service provided, together with the technical components and procedures used, with the supervisory body by the time when activities are established or Services changed.

(3) The security policy of certification service providers which supply secure electronic signature procedures shall describe how they shall comply with the security requirements of the present federal law and the orders issued on the basis thereof.

(4) Certification service providers shall comply with the information presented in the security and certification policy both on assuming and during the exercise of their activities.

(5) Certification service providers shall notify the supervisory body immediately of any circumstances which preclude the clean exercise of their activities according to the security and certification policy.

(6) The security policy of certification service providers which issue certificates shall describe if and, where applicable, in what form directory and revocation Services are provided.

(7) Certificates for certification service providers shall only be used by them in the provision of certification services.

Certification service providers for qualified certificates

§ 7. (1) Certification service providers which issue qualified certificates shall:

1. demonstrate the reliability required for providing signature and certification services;

2. operate a fast, secure directory service and an instant, secure revocation service;

3. use quality-assured time data (time stamps) on qualified certificates and for directory and revocation Services and ensure in all cases that the time at which a qualified certificate was issued and revoked can be determined;

4. reliably check the identity and, where applicable, any significant legal attributes of the person for whom a qualified certificate is issued, using official identity papers with a photograph;

5. employ reliable personnel who have the specialist knowledge, experience and qualifications and, especially, the management skills and knowledge of secure signature technology and suitable security procedures needed for the services provided and apply suitable administrative and management procedures which comply with recognised standards;

6. have adequate financial resources to meet the requirements of the present federal law and the orders issued on the basis thereof and take precautions to satisfy compensation claims, for example by concluding liability insurance.

7. record all facts of importance to qualified certificates for a period of time commensurate with the purpose thereof including, if necessary, electronically so that certification can be proven, especially in judicial proceedings and

8. take precautions so that the signatory's signature creation data cannot be stored or copied either by the certification service provider or by third parties.

(2) Certification service providers which issue qualified certificates shall use reliable Systems, products and procedures which are protected against modification and which ensure technical and cryptographic security for signature and certification services to create and store certificates. Most importantly, it shall take suitable precautions to ensure that signature creation data are kept secret, that data for qualified certificates cannot be forged or falsified unnoticed and that these certificates are only publicly available on-line with the signatory's consent. Technical components and procedures which comply with the requirements of § 18 shall be used to supply the signature creation data and to create and store qualified certificates.

(3) The certification service provider's signature creation data shall be secured against unauthorised access.

(4) The fact that the conditions of para. 1 to 3 apply can be certified for secure electronic signatures during the voluntary accreditation procedure (§ 17).

(5) If the certification service provider supplies a secure electronic signature procedure that it is a secure electronic signature must be noted on the certificate or in a directory which is generally available on-line at all times.

(6) Certification service providers shall verify the secure signatures based on their qualified certificates at the request of the courts or other authorities.

Issuing qualified certificates

§ 8. (1) Certification service providers shall reliably establish the identity of the persons to whom qualified certificates are issued using official identity papers with a photograph and shall certify that specific signature certification data have been allocated to such persons by issuing a qualified certificate.

(2) An application for a qualified certificate may also be filed with a body instructed by the certification service provider. This body shall check the identity of the applicant.

(3) Certification service providers shall include information on the applicants' powers of attorney or other significant legal attributes on qualified certificates according to the certification policy if the applicant so requests provided these facts have reliably been proven to them or the other agencies (paragraph 2).

(4) Certification service providers may use a pseudonym in lieu of the signatory's name according to the certification policy, if the applicant so requests. The pseudonym shall not be offensive or obviously open to confusion with names or signs.

Revocation of certificates

§ 9. (1) Certification service providers shall revoke certificates immediately if:

1. the signatory or principal named in the certificate so requests;

2. the certification service provider leans of the death of the signatory or other change to facts confirmed in the certificate;

3. the certificate was obtained on the grounds of false information;

4. the certification service provider ceases operations and its directory and revocation services are not taken over by another certification service provider;

5. the supervisory body in accordance with § 14 orders that the certificate be revoked or

6. there is a danger that the certificate will be misused.

(2) If the facts referred to in paragraph l cannot be ascertained beyond doubt immediately, the certification service provider shall immediately suspend the certificate.

(3) The suspension and revocation must include the time and date on which they took effect. If a revocation service is supplied, the suspension and revocation shall take effect when entered in the corresponding directory. Retroactive suspends or retroactive revocations are not permitted. The signatory or successor in title shall be advised of the block or revocation immediately.

(4) Certification service providers shall keep a list of blocked and revoked qualified certificates available on line at all times.

(5) The supervisory body shall revoke a certification service provider' s certificate immediately if:

1. the certification service provider has been prohibited from exercising its activities and its directory and revocation Services have not been taken over by another certification service provider or

2. the certification service provider has suspended activities and its directory and revocation services have not been taken over by another certification service provider.

Timestamping Services

§ 10. If a certification service provider supplies timestamping services, it must set out the details thereof in the security and certification policy. Technical components and procedures which ensure that the time quoted is correct and authentic and which comply with the requirements of § 18 must be used for secure timestamping services.

Records

§ 11. (1) Certification service providers must record the security measures taken in order to comply with the present federal law and the orders issued on the basis thereof, as well as issuance, suspension or revocation of certificates. The data and the authenticity thereof and the date on which they were included in the records must be verifiable at all times.

(2) Certification service providers shall hand over the records in accordance with paragraph 1 at the request of the courts or other authorities.

Suspending activities

§ 12. Certification service providers shall immediately notify the supervisory body of the suspension of their activities. They shall also revoke the certificates which are valid when activities are suspended or ensure that at least their directory and revocation services are taken over by another certification service provider. Signatories shall be advised immediately of the suspension of activities and the revocation or take-over. The certification service provider shall ensure that revocation Services are maintained even if the certificates are revoked. If it fails to comply with this obligation, the supervisory body shall ensure that the revocation services are maintained at the certification service provider' s expense.

Section 4

Supervision

Supervisory body

§ 13. (1) The Telekom-Control-Kommission shall act as supervisory body (§ 110 of the Telecommunications Law). It shall be responsible for regular supervision of compliance with the provisions of the present federal law and the orders issued on the basis thereof.

(2) The supervisory body shall, inter alia:

1. check that the information in the security and certification policy has been put into practice;

2. if secure electronic signatures are supplied, monitor the use of suitable technical components and procedures (§ 18);

3. accredit certification service providers in accordance with § 17 and 4. Supervise the organisation of confirmation bodies (§ 19).

(3) The supervisory body shall ensure that a directory of valid, suspendeded and revoked certificates for certification service providers is generally available on-line at all times. The supervisory body shall also ensure that a directory of certification service providers established in Austria, certification service providers accredited by it and third country certification service providers whose certificates are guaranteed by certification service providers established in Austria in accordance with § 24 para. 2 number 2 is generally available on-line at all times. Other certification service providers established abroad shall also be included in this directory on request. The directory of certificates for certification service providers shall contain their qualified certificates for the provision of certification services. These certificates may also be issued by the supervisory body. The supervisory body shall attach its secure electronic signature to the directories which it maintains. The supervisory body's certificate shall be published in the Official Gazette of the *Wiener Zeitung.*

(4) The costs of the supervisory body's activities and the work carried out by Telekom-Control GmbH shall be covered by charging certification service providers fees as set out in an order. This revenue shall be collected by the supervisory body, which shall pay Telekom-Control GmbH or the confirmation body for the cost of the work carried out by them.

(5) The supervisory body may seek advice from suitable persons or institutions such as confirmation bodies (§ 19).

(6) In accordance with article 20 para. 2 of the Federal Constitution, the members of the supervisory body shall not be bound by any instructions in the exercise of their office. The supervisory body shall apply the 1991 AVG unless legislation stipulates otherwise. It shall decide in the last instance and may take recourse to the Administrative Courts.

(7) The activities of the supervisory body pursuant to the present federal law shall be kept separate, from an organisational and financial point of view, from its activities under other federal laws.

Supervisory measures

§ 14. (1) The supervisory body shall impose measures on certification service providers to ensure that obligations pursuant to the present federal law and the orders issued on the basis thereof are fulfilled. More importantly, it may prohibit a certification service provider from using inappropriate technical components and procedures or exercising all or some of its activities. In addition, the supervisory body may revoke certification service providers' or signatories' certificates or order that the certification service provider revoke signatories' certificates.

(2) Unless corrective measures are prescribed in accordance with paragraph 6, a certification service provider shall be prohibited from exercising all or some of its activities if:

1. it or its staff do not demonstrate the reliability needed for the signature or certification services provided;

2. it or its staff do not have the necessary specialist knowledge;

3. it does not have sufficient financial resources at its disposal;

4. it fails to put the information set out in the security or certification policy into practice during the exercise of its activities,

5. it fails to provide or provide properly the prescribed directory or revocation services or fails to comply with or adequately comply with its blocking or revocation obligations (§ 9) or

6. it fails to comply with the notification obligation according to § 6 para. 2.

(3) Unless corrective measures are prescribed according to paragraph 6, certification service providers which issue qualified certificates shall be prohibited from exercising all or some of their activities if the other conditions governing the exercise of such activities pursuant to the present federal law or the orders issued on the basis thereof are not met.

(4) Unless corrective measures are prescribed according to paragraph 6, certification service providers which provide secure electronic signature procedures shall be prohibited from exercising all or some of their activities if the technical components and procedures used do not comply with the security requirements according to §18.

(5) If the supervisory body prohibits a certification service provider from exercising its activity, it must ensure that the certification service provider' s and signatories' certificates are revoked or arrange for the signature and certification services provided or at least the directory and revocation services to be taken over by another certification service provider, insofar as the certification service providers involved agree to the take-over. Signatories shall be advised of the ban and the revocation or take-over immediately. The certification service provider shall ensure that revocation services are maintained even if the certificates are revoked. If it fails to perform this obligation, the supervisory body shall ensure that the revocation services are maintained at the certification service provider' s expense.

(6) The supervisory body shall refrain from prohibiting the activities of a certification service provider if corrective measures can be ordered which are sufficient to ensure compliance with the provisions of the present federal law and of the orders issued on the basis thereof. More importantly, it may impose terms and conditions or threaten action if the shortcomings identified by it are not rectified by a reasonable deadline which it shall set.

Involvement of Telekom-Control GmbH

§ 15. (1)The Supervisory body may call on the Services of Telekom-Control GmbH (§ 108 of the Telecommunications Law) during the exercise of its supervisory activities.

(2) Telekom-Control GmbH shall, inter alia:

1. support the supervisory body in the day-to-day supervision of certification service providers and auditing of the technical products, procedures and other devices used for the purpose of providing signature and certification services and the qualifications of the personnel;

2. register certification service providers who submit notification of establishing of activities;

3. keep directories of certificates for certification service providers and of certificates of certification service providers (§ 13 para. 3) and a directory of accredited certification service providers (§ 17 para. l);

4. if the activities of a certification service provider are suspended or prohibited, maintain revocation Services not taken over as described in §§ 12 or 14 para. 5,

5. at the demand of the supervisory body, determine compliance with the conditions for voluntary accreditation (§ 17);

6. help to establish the equivalence of test reports from third countries as defined in § 24 para. 3 and

7. If there is good cause suspecting non-compliance with the security requirements of the present federal law or the orders issued on the basis thereof or at the request of a certification service provider, order directly a temporary ban on the activities of the certification service provider or provisional measures as defined in § 14 para. 1.

(3) Telekom-Control GmbH shall take all the organisational measures needed to ensure that it is able to fulfill its duties and support the supervisory body in the performance of its duties. It may seek advice from suitable persons or institutions such as confirmation bodies (§ 19). The technical aspects of its duties shall agree with a confirmation body (§ 19). The personnel of Telekom-Control GmbH shall be

bound by the instructions of the chair or a member named in the rules of procedure for the purposes of its activities for the supervisory body.

(4) The jurisdiction of the ordinary courts not withstanding, customers or parties representing interests may submit litigation or complaints to which no satisfactory solution can be found with the certification service provider, especially concerning the quality of a certification service, to Telekom-Control GmbH. Telekom-Control GmbH shall make every effort to find a solution which satisfies both parties within a reasonable period of time. Certification service providers are obliged to take part in such procedures and provide all the Information needed to assess the situation. Telekom-Control GmbH shall lay down guidelines for the implementation of this procedure, which shall be published in a suitable form.

(5) § 13 para. 7 governing separate organisational and financial arrangements shall also apply to the activities of Telekom-Control GmbH. implementing supervision.

Implementation of supervision

§ 16. (1) Certification service providers shall grant persons acting on behalf of the supervisory body access to business and operating premises during business hours, submit or have ready for inspection the relevant books and other records and documentation, including the records according to § 11, and provide information and any other support needed. Current statutory rights to observe secrecy or remain silent shall remain unaffected.

(2) Security Service officials shall assist with the implementation of supervision within the limitations of their statutory remit if requested to do so by the supervisory body and the persons acting on its behalf.

(3) Supervision according to para. l and 2 shall be carried out with as little inconvenience as possible to the parties concerned and without attracting any unnecessary attention to ensure that the security of the signature and certification services are not breached.

Voluntary accreditation

§ 17. (1) Certification service providers which provide secure electronic signature procedures and which prove to the supervisory body that they comply with the requirements of the present federal law and the orders issued on the basis thereof before establishing their activities as accredited certification service providers shall be accredited by the supervisory body on request. Accredited certification service providers may describe themselves as such with the consent of the supervisory body. This description may only be used with signature and certification services and signature products if the security requirements according to § 18 are met. The supervisory body shall ensure that accredited certification service providers are included in a directory which is generally available on-line at all times.

(2) Voluntary accreditation of a certification service provider shall be included in the qualified certificate or made available in some other suitable manner.

(3) The supervisory body shall ensure that the certification service providers accredited by it are monitored on a regular basis.

Section 5

Technical security requirements

Technical components and procedures for secure signatures

§ 18. (1)Technical components which allow the forgery of signed data to be reliably recognised and reliably prevent unauthorised use of signature creation data procedures shall be used to generate and store signature creation data and create secure signatures.

(2) The technical components and procedures used to create a secure signature must also ensure that the data to be signed is not changed. They must also allow the data to be signed to be displayed to the signatory before the signature procedure is triggered. The probability that signature creation data will only occur once must be near certainty, the data must be adequately secured against derivation and their confidentiality must be guaranteed.

(3) Technical components and procedures which prevent forgery or falsification of the certificates shall be used to create and store qualified certificates.

(4) Technical components and procedures used to verify securely signed data shall ensure that:

1. the signed data have not been changed;

2. the signature is verified reliably and the result of the verification is displayed correctly,

3. the person conducting the verification can establish the data to which the electronic signature relates;

4. the person conducting the verification can establish the signatory to whom the electronic signature has been allocated, whereby the use of pseudonyms must be indicated and

5. changes to the signed data with security implications can be recognised.

(5) The technical components and procedures for generating secure signatures must be constantly and adequately verified using state-of-the-art technology. Compliance with security requirements must be certified by a confirmation body (§ 19).

Confirmation body

§ 19. (1) The duties allocated to a confirmation body pursuant to the present federal law and the orders issued on the basis thereof may only be carried out in an institution suitable for the purpose.

(2) An institution is suitable for carrying out the duties allocated to a confirmation body if it:

1. demonstrates the required reliability;

2. employs reliable personnel with the specialist knowledge, experience and qualifications, especially knowledge of electronic signatures, suitable security procedures, cryptography, communications and smart card technology and the technical evaluation of these components needed for these duties;

3. has sufficient technical installations and resources and adequate solvency and

4. guarantees the necessary independence, neutrality and impartiality.

(3) The Federal Chancellor shall stipulate that an institution is suitable as a confirmation body in an order issued in agreement with the Minister of Justice. The order in question shall only be issued at the request of the institution in question and it shall only be found suitable if it complies with the requirements in paragraph 2 regarding its statutes or memorandum and articles of association, organisation and security and financing concept.

(4) A confirmation body may obtain test reports on technical components or procedures from other institutions or agencies to perform the tasks incumbent upon it according to the present federal law of the orders issued on the basis thereof.

Section 6

Users' rights and obligations

Certification service provider's general duty to provide Information

§ 20. (1) Certification service providers shall advise applicants for certificates clearly and comprehensibly of the content of the security and certification policy in writing or using a permanent data carrier before a contract is concluded. When qualified certificates are issued, certification service providers shall also advise certificate holders of the conditions of use of the certificate such as restrictions on its scope or transaction value, and shall refer to voluntary accreditation (§ 17) or any special procedures for settling disputes.

(2) The information referred to in paragraph l shall also be made available on request to third parties who can prove a prima facie legal interest in the said information.

(3) Certification service providers shall also advise certificate holders as to which technical components and procedures are suitable for the signature procedure used and, where applicable, which technical components and procedures and other devices comply with the requirements governing the

generation and verification of secure signatures. Furthermore, certificate holders must also be told of the potential legal effects of the signature procedure used the signatory's duties and the certification service provider's specific liability. Certificate holders shall also be told that (and, where applicable how) a new electronic signature is to be applied before the security value of the present signature is eroded with the passage of time.

Signatory's duties

§ 21. The signatory shall take good care of the signature creation data, prevent unauthorised access to the signature creation data as far as can reasonably be expected and refrain from passing on the signature creation data. He shall ask for the certificate to be revoked if the signature creation data are mislaid, if there is reason to believe the signature creation data have been compromised or if the facts certified in the certificate have changed.

Data protection

§ 22. (1)Certification service providers shall only use the personal data which are needed to perform the service provided. These data shall only be obtained directly from the person in question or, with his consent, from a third party.

(2) If a pseudonym is used, the certification service provider shall transmit data on the signatory's identity insofar as there is prima facie evidence of an overriding legitimate interest in establishing his identity as defined in § 8 para. l number 4 and para. 3 of the Data Protection Law. The transmission shall be recorded.

(3) The certification service provider' s duty to provide information and assist the courts and other authorities shall remain unaffected.

Certification bodies' liability

§ 23. (1)Certification service providers which issue qualified certificates or which guarantee such certificates according to § 24 para. 2 number 2 shall be liable vis-à-vis persons who rely on the certificate for ensuring that:

1. all the information on the qualified certificate was accurate at the time of issue,

2. the signatory referred to on the qualified certificate was in possession of the signature creation data which correspond to the signature verification data given on the certificate when the certificate was issued,

3. the signature creation data and the signature verification data allocated to them correspond when the products and procedures supplied or recommended as suitable by the certification service provider are used in tandem,

4. the certificate will be revoked immediately if there is cause to do so and that revocation services are available and

5. the requirements of § 7 have been complied with and technical components and procedures in accordance with § 18 have been used to generate and store the signature creation data.

(2) Certification service providers which supply secure electronic signature procedures shall also be liable for ensuring that the products, procedures and other devices which they supply or recommend as suitable to creating electronic signatures and to displaying the data to be signed only use technical components and procedures according to § 18.

(3) Certification service providers shall not be liable if they can prove that neither they nor their employees were to blame for the infringement of the obligations according to paragraphs l and 2. If the injured party can demonstrate that there is a probability that the obligations according to paragraph l and 2 were violated or the precautions taken to comply with the security requirements of the present federal law or the orders issued on the basis thereof were compromised, then it will be assumed that this was the cause of the damage. This assumption is refuted if the certification service provider can demonstrate that there is a probability that the damage was not caused by violation or compromise of the obligations and precautions referred to in the second paragraph.

(4) If the scope of a qualified certificate is restricted, the certification service provider shall not be held liable for damage caused by failure to comply with this restriction during use of the certificate. If the qualified certificate contains a specific transaction value capping the use of the certificate, the certification service provider shall not be held liable for damage caused by exceeding this transaction value.

(5) The certification service provider' s liability according to paragraphs l to 3 may not be excluded or limited in advance.

(6) The provisions of the Austrian Civil Code and other legislation which stipulate that damage is to be compensated to a different degree or by other persons shall remain unaffected

Section 7

Recognition of foreign certificates

Recognition

§ 24. (1)Certificates issued by certification service providers established in the European Community, the validity of which can be verified from Austria, shall be tantamount to Austrian certificates. Qualified certificates issued by the said certification service providers shall have the same legal effects as qualified Austrian certificates.

(2) Certificates issued by certification service providers established in third countries, the validity of which can be verified from Austria, shall be recognised in Austria. Qualified certificates shall be tantamount for legal purposes to qualified Austrian certificates if:

1. the certification service provider complies with the requirements of § 7 and is accredited under a voluntary accreditation system in a Member State of the European Union;

2. a certification service provider established in the European Community which complies with the requirements of § 7 guarantees the certificate under liability law or

3. the certificate is recognised as a qualified certificate or the certification service provider is recognised as an issuer of qualified certificates under a bilateral or multilateral agreement between the European Community on the one hand and third countries or international organisations on the other hand.

(3) If a government-recognised body has been set up in a Member State of the European Union or in a third country for the purposes of proving security requirements for secure electronic signatures, certification by the said body of compliance with the security requirements governing the generation of secure electronic signatures shall be tantamount to the certificates issued by a confirmation body (§ 19) insofar as the supervisory body establishes that the technical requirements, audits and test procedures on which the said body bases its assessrnents are equivalent to those of confirmation bodies.

Section 8

Final provisions

Signature order

§ 25. The Federal Chancellor shall issue the orders needed to implement the present federal law according to state-of-the-art science and technology and in agreement with the Minister of Justice. These orders shall stipulate:

1. the flat-rate, cost-covering fees for the Services of the supervisory body and Telekom-Control GmbH and how the said fees are to be levied;

2. the level of financial resources needed in order to meet the requirements of the present federal law and the orders issued on the basis thereof and cover the certification service providers' liability risk and shall set a minimum sum insured for liability insurance;

3. the reliability of the certification service provider and its staff (§§ 7 para. l and

14 para. 2);

4. the requirements for technical components and procedures and the technical products and other resources needed in order to apply §§ 7 para 2, 10 and 18, the method of auditing the technical components and procedures in accordance with § 18 and the method of issuing confirmation of compliance with these requirements;

5. the time during which revocation services must continue to be maintained by the supervisory body (§ 12 and § 14 para. 5);

6. the scope and requirements of and tolerances for secure time stamps;

7. the period of validity and the renewal of qualified certificates and the time and procedure for attaching a new electronic signature (follow-on signature),

8. the form, presentation and availability of the certification policy (e.g. plaintext);

9. the length of time records must be kept (§11) and

10. the format for the description ofaccredited certification service providers.

Administrative provisions

§ 26. (1)Any person who misuses another person's signature creation data without the signatory's knowledge and consent is guilty of an administrative violation punishable by a fine of up to ATS 56,000.

(2) A certification service provider is guilty of an administrative violation punishable by a fine of up to ATS 112,000 if it:

1. violates its duty to revoke a certificate in contravention of § 9 para. 1;

2. violates its duty to keep records in contravention of § 11;

3. refuses to allow the books, records and documentation referred to in § 16 para 1. to be inspected or fails to provide the necessary information in contravention of § 16 para. 1 or

4. fails to instruct the certificate holder in contravention of § 20 para. 1 and 3.

(3) A certification service provider is guilty of an administrative violation punishable by a fine of up to ATS 224,000 if it:

1. fails to notify assumption of activities or to submit a safety or certification policy in contravention of § 6 para. 2;

2. fails to notify the supervisory body of any facts which no longer allow proper activities in accordance with the security and certification concept in contravention of § 6 para. 5;

3. fails to maintain a suitable revocation service or suitable directories in contravention of § 7 para. l number 2;

4. fails to take suitable precautions to ensure that the signatory's signature creation data cannot be stored or copied either by the certification service provider or by third parties in contravention of§ 7 para. l number 8,

5. fails to use, supply or recommend suitable technical components and procedures for secure electronic signatures in contravention of § 18 or

6. continues to exercise its activities despite being prohibited from doing so by the supervisory body (§ 14 para. 2 to 4).

(4) There is no administrative violation according to para. 1 to 3 if the act in question constitutes an offence which can be prosecuted in the courts or attracts more serious sanctions under other administrative regulations.

(5) If the criminal offence is recognised, the items used to commit it may be declared forfeit.

Entry into force and references

§ 27. (1)The present federal law shall enter into force on l" January 2000.

(2) References herein to the provisions of other federal laws shall be understood as references to the currently valid version thereof.

Implementation

§ 28. The following persons shall be responsible for the implementation of the present federal law:

1. §§ 3,4 and 23: the Minister of Justice;
2. §§ 13 to 17: the Minister of Science and Transport;
3. §§ 22 and 26: the Federal Chancellor;
4. §§ 7 para. l number 6 and 13 para. 4: the Federal Chancellor in agreement with the Minister of Justice and the Minister of Finance and
5. the remaining provisions: the Federal Chancellor in agreement with the Minister of Justice.