Merchants and Trade - Act No 28/2001 on electronic signatures

Chapter I
Objectives and Scope

Article 1
Objectives

The objective of this Act is to provide for the legal effect of electronic signatures and to contribute to their secure and effective use by defining the requirements for qualified electronic signatures, qualified certificates and the activities of certification-service-providers.

Article 2
Scope

This Act applies to electronic signatures and the activities of certification-service-providers established in Iceland.
The Minister for Industry and Commerce shall be the responsible authority pursuant to this Act.

Chapter II
Definitions, Legal Effect and the Protection of Personal Data

Article 3
Definitions

For the purpose of this Act:
1. Electronic signature means data in electronic form which are attached to or logically associated with other electronic data and which are used to authenticate the origin of the latter data.
2. Advanced electronic signature means an electronic signature which
a. is uniquely linked to the signatory,
b. is capable of identifying the signatory,
c. is created using means that the signatory can maintain under his sole control, and
d. is linked to data in such a manner that any change of the data subsequent to signature is detectable;
3. Qualified electronic signature means an advanced electronic signature which is supported by a qualified certificate and created using a secure signature-creation device;
4. Signatory means a person who holds a signature-creation device and acts either on his own behalf or on behalf of another natural or legal person;
5. Signature-creation data means unique data, such as codes or private cryptographic keys, which are used by the signatory to create an electronic signature;
6. Signature-creation device means software or hardware used to create an electronic signature with the help of signature-creation data;
7. Secure signature-creation device means a signature-creation device which meets the requirements laid down in Articles 8 and 9 hereof;
8. Signature-verification-data means data, such as codes or public cryptographic keys, which are used for the purpose of verifying an electronic signature;
9. Signature-verification device means configured software or hardware used to verify the electronic signature with the help of the signature-verification data;
10. Certificate: means an electronic attestation which links signature-verification data to a person and confirms the identity of that person;
11. Qualified certificate means a certificate containing the data provided for in Article 7 and issued by a certification-service-provider who fulfils the requirements laid down in Chapter V hereof;
12. Certification-service-provider means an entity or a legal or natural person who issues certificates or provides other services related to electronic signatures

Article 4
Legal Effect of Electronic Signatures

In the event of a signature being a condition for legal effect pursuant to legislation, administrative requirements or for other reasons, a qualified electronic signature shall in all cases fulfil such requirements.
The provisions of Paragraph 1 do not preclude electronic signatures other than those stipulated therein from meeting the conditions for signatures pursuant to law, administrative instructions or other reasons.

Article 5
Protection of Personal Data

Certification-service-providers who issue certificates to the public may collect personal data only directly from the data subject, or with the explicit consent of the data subject. The data may only be collected or used insofar as it is necessary for the purposes of issuing and maintaining the certificate, except with the explicit consent of the data subject.

The processing of personal data by the certification-service-providers and surveillance of such processing shall be subject to legislation on personal privacy and processing of personal data. Certification-service-providers are subject to notification requirements pursuant to the said legislation.

Chapter III
Qualified Certificates

Article 6
Qualified certificate

The term "qualified certificate" or any other terms implying that the certificate is qualified may not be used unless the relevant certificate fulfils the requirements laid down in Article 7 and is issued by a certification-service-provider meeting the requirements laid down in Chapter V hereof.

Article 7
Content of Qualified Certificates

A qualified certificate must contain the following information and data:
1. an indication that the certificate is issued as a qualified certificate;
2. information on the identity of the certification-service-provider and the place of its establishment.
3. the name of the signatory or pseudonym; in the event of the signatory using a pseudonym, the pseudonym shall be clearly identified as such;
4. further information on the signatory if necessary for the intended purpose of the certificate;
5. signature-verification data which correspond to signature-creation data under the control of the signatory;
6. an indication of the beginning and end of the period of validity of the certificate;
7. the identity code of the certificate;
8. the advanced electronic signature of the certification-service-provider issuing the certificate;
9. information on limitations on the scope of use of the certificate and limits on the value of transactions for which the certificate can be used, if applicable.

The Minister may issue further instructions on the information to be included in qualified certificates in a government regulation.

Chapter IV
Secure-Signature-Creation Devices

Article 8
Requirements

Secure-signature-creation devices must ensure that the signature data:
a. can appear only once;
b. cannot be breached, taking into consideration normal security requirements, and
c. are reliably protected against use by parties other than the signatory.

Secure-signature-creation-devices shall also satisfactorily ensure the confidentiality of the signature-creation data and that the electronic signature is protected from forgery.

Secure signature-creation devices shall not permit alterations to the data to be signed or prevent such data from being seen by the signatory prior to signature.

Article 9
Approval

Requirements for the signature-creation device pursuant to Article 8 shall be regarded as fulfilled when:
a. a competent public or private body has confirmed that it fulfils the requirements of article 8. The Minister of Commerce may designate the bodies authorised to grant such confirmation by government regulation, or;
b. a competent public or private body within the European Economic Area has approved it.

The signature-creation device shall be regarded as secure pursuant to Article 8 if it conforms to standards laid down by the Commission of the European Community for such devices and published in the Official Journal of the European Communities.

Chapter V
Requirements for Certification-Service-Providers Issuing Qualified Certificates

Article 10
Activity Requirements

A certification-service-provider issuing qualified certificates shall in its activities fulfil the requirements necessary to ensure a secure and reliable issuance of certificates.

A certification-service-provider shall to this end:
a. employ administrative and operational procedures of high quality;
b. employ personnel who possess the expert knowledge, experience and capability necessary for the activities; and
c. maintain sufficient financial resources to operate, taking into consideration the requirements laid down in this Act.

Article 11
Systems and Devices

The certification-service-provider shall in his operation use reliable systems and devices that are secure from changes and ensure the security of the coding and technical security.
The provisions in Paragraph 1 are regarded as met if the certification-service-provider uses systems that are approved in accordance with Article 9.
The certification-service-provider shall take measures to prevent the possibility of certificates being forged. In instances where the certification-service-provider creates the signature-creation data he shall ensure secrecy in the course of the production.

Article 12
Directory and Revocation Services

A certification-service provider issuing qualified certification shall establish and operate a prompt and secure system for the registration and revocation of certificates. He shall also ensure that the date and time when a certificate is issued or revoked can be determined precisely. Information on the limitations for the qualification of the certificate shall also be available, cf. Item 9 in Paragraph 1 of Article 7.

Article 13
Authentication of Signatory

A certification-service provider issuing qualified certificates shall verify in an appropriate manner the identity of the signatory and any further information on the signatory.
Information on the methods used pursuant to Paragraph 1 shall be available to the public.

Article 14
Storage of Information

A certification-service-provider issuing qualified certificates shall store all relevant information regarding the certificate for an appropriate length of time.
The certification-service-provider shall use reliable systems for the storage of certificates, so that:
a. no-one, with the exception of parties authorised to do so, can make changes to the certificates or add to them,
b. it is possible to verify that the information is correct,
c. the certificate is available to the public only if expressly permitted by the signatory, and
d. possible technical changes, which may compromise safety requirements, are easily recognisable to those who operate the system.
The certificates shall be stored in a manner whereby they can be verified.
The certification-service-provider may not store or copy the signature-creation data of the signatory.

Article 15
Information on terms, conditions etc.

Before a certification-service-provider enters into an agreement on the issuance of a qualified certificate he shall inform the signatory in writing and in a permanent manner of:
a. the terms and limitations on the use of the certificate,
b. any voluntary accreditation schemes in operation, and
c. procedures for complaints and dispute settlement.
Information pursuant to Paragraph 1 may be sent electronically, provided that it is in a legible form and in readily understandable language. This information shall, where applicable, be accessible on request to a third party who relies on certificates.

Article 16
Further rules

The Minister for Commerce may issue further instructions, in a government regulation, on requirements regarding certification-service-providers issuing qualified certificates pursuant to Chapter V hereof.

Chapter VI
Liability

Article 17

A certification-service-provider who issues a qualified certificate to the public or who guarantees such a certificate issued by others is liable for damage caused to any party who reasonably relies on a certificate, as regards:
a. the information on the certificate being correct on the date of issue,
b. the certificate containing all the information required in Article 7,
c. the signatory holding, at the time of issuance of the certificate, the signature-creation data corresponding to the verification data given in the certificate,
d. specific signature-creation data conforming solely to specific verification data and specific verification data conforming solely to specific signature-creation data when both are generated by the certification-service-provider, or
e. the certificate being appropriately filed in a revocation registry pursuant to Article 12.
The certification-service-provider is not liable pursuant to Paragraph 1 if he proves that the damages cannot be traced to any fault on his part.
If the use of the certificate is contrary to the limitations on the scope of the certificate or on the amount of the transaction and that information on such limitations is accessible, the certification-service-provider is not liable for such damage as may result from such use.

Chapter VII
Supervision of Certification-Service-Providers Issuing Qualified Certificates

Article 18
Supervision

The State Accreditation Agency is responsible for monitoring that the operation of certification-service-providers issuing qualified certificates conforms to the provisions hereof and regulations based on this Act, subject to Paragraph 2 of Article 5.
The State Accreditation Agency may prohibit operations and conditions that conflict with the provisions hereof and regulations based on this Act. Conditions may also be established for continued operation and respites granted for the fulfilment of such conditions.
The State Accreditation Agency may require reassessment of the systems, equipment and operating procedures of certification-service-providers issuing qualified certificates (re-assessment of information technology). The State Accreditation Agency may appoint the parties authorised to conduct such reassessment. The certification-service-provider shall pay all costs resulting from such reassessment.
The State Accreditation Agency may revoke the permission of a certification-service-provider to designate certificates issued by him as "qualified certificates" if he has grossly or repeatedly violated the provisions hereof or of regulations issued based on this Act.
The Minister may issue further instructions on the arrangement of supervision in a government regulation.

Article 19
Registration and Supervision Fee

A certification-service-provider intending to issue qualified certificates shall send notification of his operation to the State Accreditation Agency [Löggildingarstofa]. Following such notification, the certification-service-provider may issue qualified certificates. The notification shall contain the information necessary to demonstrate that the certification-service-provider fulfils the conditions hereof for his operation, including information on the operation, organisation, system and equipment. Amendments and new information shall be sent promptly to supervisory bodies.
A certifcation-service-provider who issues qualified certificates shall pay a fee in the amount of ISK 1,000,000 per year to fund the cost of supervision pursuant to this Act. In the event of a certification-service-provider starting or ceasing operation during the payment year, the minimum fee shall be determined in proportion to the time of operation during the year. The supervision fee shall be directly payable to and collected by the State Accreditation Agency. Claims in respect of supervision fees are enforcible by attachment without prior court judgement, ruling or mediation.
The due date of the supervision fee is 1 February of each year for the preceding calendar year.
The Minister may establish further instructions on the method of registration, notification and reporting in a government regulation.

Article 20
Checks, Access and Confidentiality

The State Accreditation Agency shall be provided with all information and explanations necessary for the supervision. The State Accreditation Agency may establish deadlines for the delivery of information or explanations. The State Accreditation Agency may also require certification-service-providers and parties in their service to appear before it to provide information and explanations regarding the issue of certificates or other services connected with electronic signatures.
The State Accreditation Agency is entitled, in the course of its supervisory duties, to gain access to the premises of the certification-service-provider, or other premises where activities falling under this Act are carried out, without court intervention, where it may take the supervisory measures it regards as necessary and require the employees on the premises to provide the necessary assistance. In the event of obstruction of its supervisory activities, the State Accreditation Agency may request the assistance of the Police.
The authority of the State Accreditation Agency to require information or access to operating premises and technical equipment can not be restricted by reference to rules on confidentiality.
The employees of the State Accreditation Agency are bound by confidentiality. They shall not, subject to liability, disclose to any third party confidential matters that come to their attention in the course of their work regarding the business and operations of a certification-service-provider, related parties or others. The same applies to experts in the employ of the State Accreditation Agency in the course of their supervisory work under this Act. This confidentiality shall remain in force after termination of employment.

Article 21
Daily Fines

The State Accreditation Agency may impose daily fines on a certification-service-provider following a specified grace period, if the provider does not supply requested information, comply with the Agency's calls for corrective action or respond to the requirements of the supervisory body in other respects.
The amount of the daily fines shall be determined on the basis of the scope of the operation of the certification-service-provider and the nature of the offence. Daily fines may range from ISK 10,000 to ISK 1 million per day. They shall be paid until the fulfilment of the requirements of the State Accreditation Agency. Uncollected daily fines shall not be revoked on fulfilment of the requirements of the State Accreditation Agency except by specific decision of the Agency.

Daily fines are enforceable by attachment and shall accrue to the State Treasury net of collection costs. A decision of the State Accreditation Agency on the daily fines cannot be appealed to the Minister.

Chapter VIII
Miscellaneous Provisions
Article 22
Certification-service-providers Established Outside Iceland

Certificates issued by certification-service-providers established outside Iceland shall be regarded as qualified certificates pursuant to this Act if:

a. the certification-service-provider meets the provisions of this Act and has been approved by a voluntary accreditation scheme in the European Economic Area.

b. the certification-service-provider established in the European Economic Area and meeting the provisions of this Act guarantees the certificate,

c. the certificate is issued by a certification-service-provider established in a country in the European Economic Area and meets the requirements of the said country for qualified certificates or

d. the certificate or certification-service provider are approved in Iceland, the European Union, states outside the European Union or international organisations, in bilateral or multilateral agreements.

Article 23
Penalties

Offences against this Act are punishable by fines, unless a more severe punishment is indicated pursuant to other legislation. Both legal entities and individuals may be subjected to fines for offences against this Act. The criminal liability of legal entities is subject to Chapter II A of the Icelandic Penal Code.

Article 24
Entry into force

This Act shall enter into force immediately.

It is enacted taking into consideration the decision of the EEA Joint Committee No. 66/2000, amending Annex XI (Telecommunication Services) to the EEA Agreement of 2 May 1992, and in order to incorporate into Icelandic law the provisions of DIRECTIVE 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community Framework for Electronic Signatures.

Interim Provision

The provisions of Chapter VII hereof shall be reviewed when two years have passed from the entry into force of this Act, based on the experience of the supervision and its scope. Special consideration shall be given to whether there is reason to review the provision on the supervision fee.