No 780 16 August 2011

REGULATION
on electronic signatures.

CHAPTER I

Scope and definitions

Article 1

Scope.

This regulation applies to the information to be included in qualified certificates, requirements of certification service providers who issue qualified certificates, requirements for secure signature creation devices, the mechanism for the registration, notifications and disclosures of certification service providers and the mechanisms of regulation of certification service providers issuing qualified certificates.

An electronic signature made using a qualified certificate does not constitute confirmation of the time of signature creation.

Article 2

Definitions

The following definitions shall apply in this Regulation:

Certificate policy: A set of rules that indicates the applicability of a certificate to a particular class of application and/or technical solutions where security requirements are comparable. A certificate policy shall also reveal the proposed mechanism for the issue and handling of electronic certificates. A certificate policy also includes rules on the requirements for security and supervision.

Certification service provider: An entity that issues certificates, or a third party that engages in the issue of qualified certificates on such entity's behalf , as provided in Article 17 of Act No. 28/2001 on electronic signatures, or provides other services related to electronic signatures

In all other respects, definitions of terms are subject to the provisions of Act No. 28/2008.

CHAPTER II

Content of qualified certificates

Article 3

Content and information in a qualified certificate

It is permitted to specify that a certificate is qualified if the certificate meets the conditions of Article 7 of Act No. 28/2001 and is issued by a certification service provider who meets the provisions of Chapter V of the Act and the conditions of rules established on the basis of the Act.

A qualified certificate shall include the word *fullgilt* in a legible form. It should also be noted that the certificate meets the provisions of law and rules that apply to the issue of qualified certificates.

Certificates are regarded as meeting the requirements of this Article if they meet the conditions of standards and other normative documents listed in Annex I to this Regulation.

Article 4

ID number and name of signatory

A qualified certificate issued in Iceland shall, in a separate name field of the certificate, specify the full name of the signatory from the National Register or a pseudonym.

A qualified certificate issued in Iceland shall, in a separate number field of the certificate, specify the ID number of the signatory. If the signatory is not domiciled in Iceland, a similar unique number issued by the National Register pursuant to the rules applicable to such issuance at any time shall be specified.

In the event of the signatory using a pseudonym in a qualified certificate, the pseudonym shall be clearly identified as such in the certificate. The certification service provider shall verify the identity of a signatory using a pseudonym and his connection with the pseudonym, as further specified in Article 14 of this Regulation.

Article 5

Additional information

A qualified certificate may provide further information on the signatory than the information specified in Article 4, such as information to the effect that the certificate is also a professional certificate, in which case the apparent authority of the signatory shall be further specified, or a further description of the type of signature permitted with the certificate in question. The validity of signatures pursuant to this Article is subject to general rules on apparent authority and its revocation.

Article 6

Verification of a qualified electronic signature

A qualified certificate shall include verification data corresponding to the signature data under the control of the signatory and which is used to verify his electronic signature.

Article 7

Period of validity of certificates and their revocation

A qualified certificate shall indicate the beginning and end of the period of validity of the certificate. The revocation service of the certification service provider is subject to the provisions of Chapter III of this Regulation.

Article 8

Identity code of certificates

A qualified certificate shall have a unique number which constitutes the identity code of the certificate, so that the certificate can always be identified.

Article 9

Information on certification service providers

In order to make it possible to verify that a qualified certificate originates from a certification service provider, the certificate shall include the advanced electronic signature of its issuer.

Article 10

Limitations on the use of qualified certificates

Qualified certificates are without limitations as regards electronic signatures unless such limitations have been specifically imposed.

A certification service provider who wishes to impose limitations on the scope of qualified certificates, or the amount of a trade for which the certificate can be used, shall include information on such limitations in the certificate.

CHAPTER III

Requirements for certification service providers, registration and revocation services etc.

Article 11

Requirements for certification service providers issuing qualified certificates

A certification service provider issuing qualified certificates shall in its activities ensure a secure and reliable issuance of qualified certificates and conduct his business in all respects in compliance with Act No. 28/2001 and rules grounded in that Act.

A certification service provider is required to employ sound management and business practices. To this end, the certification service provider shall, among other things, prepare a quality and security manual laying down the procedures and work descriptions for the business activity.

Also, the certification service provider shall prepare a training programme to ensure that employees working under the responsibility of the certification service provider possess adequate skills and receive appropriate training in line with the scope of their tasks and responsibility.

A certification service provider shall ensure that his equity and financing of liabilities relating to his business activities are adequate, taking into account:

a. the estimated size of the customer base and income generated by the business,
b. whether there are any limitations on the use of qualified certificates,
c. the certification service provider's estimated liability for damages.

A certification service provider shall conduct regular internal audits in accordance with the quality and security management rules used in his business.

In respect of point (c) of the fourth paragraph of this Article 11, a certification service provider shall supply information on the estimated total amount of damages, whether any limitations are established regarding the minimum liability of the certification service provider for each event of damage and whether professional liability insurance has been obtained for the business activity. Information pursuant to this paragraph, and changes in such information, shall be sent to the Consumer Agency [*Neytendastofa*].

Article 12

System and devices

A certification service provider shall in his operation use trustworthy systems and devices that are protected against modifications and ensure cryptographic and technical security.

The provisions of the first paragraph are considered fulfilled if the certification service provider uses systems that are approved in accordance with Article 9 of Act No. 28/2001.

A certification service provider shall take measures to prevent the possibility of qualified certificates being forged. A certification service provider who prepares signature-signing material shall guarantee confidentiality in the production process.

Article 13

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 qualified certificates. Information on revoked qualified certificates shall be updated daily, at a minimum.

A certification service provider shall ensure that the time when a certificate was issued, when it was revoked and when it was listed in a certificate revocation list can be determined precisely.

A certification service provider shall also document and have available information on limitations on the validity of qualified certificates, such as limitations on scope and amount of trades for which the certificate can be used, if any.

Article 14

Authentication of Signatory

A certification service provider issuing qualified certificates, or a party acting on his responsibility and under his authority, shall at the outset of business verify the identity of the signatory and any further information on the signatory required for documentation pursuant to this Regulation.

On the first issuance of a qualified certificate by a certification service provider or a party acting under his authority in the delivery of qualified certificates, a signatory shall prove his identity by the presentation of

a. a passport, or
b. a driver's licence, or
c. an ID card issued by the National Register of Iceland.

Article 15

Information Storage.

A certification service provider shall use trustworthy systems for the storage of qualified certificates, so that

a. only authorised persons can make entries and changes to the qualified certificates,
b. information can be checked for authenticity,
c. certificates are publicly available for retrieval in only those cases for which the certificate-holder’s consent has been obtained, *and*
d. possible technical changes which may compromise security requirements are apparent to the operator.

Qualified certificates shall be stored in such a manner that they can be verified. A certification service provider may not store or copy the signature-creation data of the signatory.

A certification service provider shall preserve copies of verified identification documents presented pursuant to Article 14 in a secure and accessible manner.

The obligation to preserve data on natural persons and legal persons which have been identified for the purposes of issuing qualified certificates is effective for 20 years from the time that the qualified certificate is revoked. The preservation and obligation to disclose data is in other respects subject to legislation applicable to the preservation of such data at any time.

Article 16

Certificate policy

A certification service provider shall publish his certificate policy in an accessible manner, including all information on the implementation and arrangements for the identification of natural persons and legal persons in respect of the issue of qualified certificates.

The certificate policy of a certification service provider shall indicate the means by which the certification service provider uses a system that fulfils the provisions of Article 15 and the means by which he ensures the preservation of data in such a manner that it is always possible to verify the data of qualified certificates, particularly so as to make it possible to supply evidence of certification in the course of legal proceedings before a court of law.

In addition, a certificate policy shall indicate the arrangements for preservation of data if a new party takes over the operation of a certification service provider or in the event of other unforeseen circumstances, e.g. if the business is discontinued or operations cease in another manner.

Article 17

Liability of certification service providers

The liability of certification service providers is subject to the provisions of Chapter VI of Act No. 28/2001.

Article 18

Information on terms, process of complaints etc.

A certification service provider shall provide customers entering into an agreement on

the issue of qualified certificates, in writing and in a permanent manner, with information pursuant to Article 15 of Act No. 28/2001.

A certification service provider offering a procedure for complaints and resolution of disputes without the intervention of a court of law shall publish the rules of procedure in an accessible manner. The Consumer Agency shall confirm the rules of procedure and ensure that they comply with general principles that apply to persons engaging in the resolution of disputes outside the courts of law.

CHAPTER IV

Secure-Signature-Creation Devices

Article 19

Basic requirements concerning the security of signature creation devices, confidentiality and the protection of data

A qualified electronic signature is valid only if it is created by a secure signature creation device meeting the basic requirements of Act No. 28/2001 and supported by a qualified certificate.

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 must not be used to alter the data to be signed, or prevent such data from being presented to the signatory prior to the signature process.

Article 20

Standards and other normative documents

A signature creation device will always be regarded *prima facie* as secure pursuant to the provisions of this Article if it complies with standards and other normative documents in respect of which the European Commission has issued resolutions and references and which are published in the Official Journal of the European Communities. A list of the names of standards and other normative documents are included in an annex to this Regulation. The Minister will update this list on the recommendation of the Consumer Agency.

Article 21

Acceptance of signature creation device

The requirements for signature creation devices pursuant to Articles 19 and 20 of this Regulation shall be regarded as fulfilled when the device has been accepted by a competent body as compliant with the requirements of Article 8 of Act No. 28/2001, cf. points (a) and (b) of the first paragraph of Article 9 of the same Act.

The conditions for the appointment of a competent body pursuant to this Article are subject to the criteria laid down in Commission Decision 2000/709/EC on the minimum criteria to be taken into account by Member States when designating bodies in accordance with Article 3(4) of Directive 1999/93/EC of the European Parliament and of the Council on a Community framework for electronic signatures. The Minister may provide further for the bodies authorised to issue confirmation of compliance under this Article.

The Consumer Agency shall review information and confirmation that the audit and certification of a signature creation device complies with basic requirements, standards and other approved normative documents in accordance with the provisions of this Regulation and has been carried out by a competent body meeting the conditions of this Article. The Consumer Agency may request any documents and information that it considers necessary to assess the competence, qualifications and independence of bodies carrying out primary audits and regular audits pursuant to the provisions of this Regulation.

CHAPTER V

Registration, supervision fee and supervision of certification service providers issuing qualified certificates

Article 22

Registration

A certification service provider intending to issue qualified certificates shall send notification of his operation to the Consumer Agency [Neytendastofa].

The notification of a certification service provider shall be accompanied by all documents and information that the Consumer Agency considers necessary for its supervision. An initial notification shall, at a minimum, be accompanied by the following documents:

1. Formal information concerning the notifying party.
   1.1. A certificate of registration from the Company Register or the relevant register of the company.

1.2. A copy of the company's articles of association and information on its board of directors.

2. Information on the financial foundation of business operations.
   2.1. A statement from an auditor indicating, *inter alia*, that budgets and data show the availability of sufficient capital. The following supporting documents shall be submitted:
      2.1.1 The initial balance sheet and annual financial reports of the preceding two years, when available.
      2.1.2 Operating budget for the year
      2.1.3 Description of long-term financing, detailing how it will be ensured that the company's cash flow will support the operations being notified over the next 3 - 5 years, at a minimum, and other necessary information on the certification service provider's business plan.
      2.1.4 Copy of professional liability insurance policy.
3. Organisation of operations:
   3.1. Certification Practice Statement.
   3.2. Certificate policy.
   3.3. Security policy.
   3.4. Copy of subscription agreement with signatories and information on limitations of the use of qualified certificates, where applicable.
   3.5. Information on management and working procedures, revealing how good management procedures will be maintained, and on the organisation of the operations, including information on security matters and the means of ensuring business continuity in the operations. The above information shall be accompanied by an overview of the operation's quality and security management system, such as a quality handbook containing the principal procedures and job descriptions and other documents that are relevant to the management and operating procedures of the certification service provider.
   3.6. A training programme containing, *inter alia*, basic requirements of employee education and information on the methods used by the certification service provider to obtain confirmation of employee qualifications.
4. Systems and devices
   4.1. System and device specifications
      4.1.1 Requirements and working procedures on the means of identifying a signatory.
      4.2.1 Information on secure storage systems and verification of data.
   4.2. An overview and listing of the standards and normative documents used.
   4.3. Information on internal audit.
   4.4. Confirmation by competent authority of compliance with requirements for secure signature creation devices, cf. Articles 8 and 9 of Act No. 28/2001.

A certification service provider shall send promptly to the Consumer Agency information on all changes relating to the operations and other updating of documents pursuant to subsections 2.1.4 and sections 3-4 of the second paragraph of this Article.

A certification service provider shall also supply the Consumer Agency with all

information and explanations that the Agency considers necessary for its supervision.

The Consumer Agency may approve a request for certain documents pursuant to this Article to be made available to the Agency only in the business establishment of the certification service provider in the case of important confidential documents which are subject to secrecy and which, for security reasons, would be improper to surrender.

Article 23

Supervision fee

A certification service provider who issues qualified certificates shall pay a fee in accordance with the provisions of law to fund the cost of supervision.

Article 24

Supervision by the Consumer Agency

The Consumer Agency shall monitor the operation of certification service providers. The supervision, procedure, administrative actions and sanctions are subject to the further provisions of Act No. 28/2001. The Consumer Agency may require reassessment of the systems, equipment and operating procedures of certification service providers issuing qualified certificates. The Consumer Agency shall appoint the parties authorised to conduct such reassessment. The certification service provider shall bear the cost of such reassessment.

CHAPTER VI

Entry into force, etc.

Article 25

This Regulation is established on the basis of the second paragraph of Article 7, subsection (a) of the first paragraph of Article 9, Article 16, the ninth paragraph of Article 18 and the fourth paragraph of Article 19 of Act No. 28/2001 on electronic signatures and is effective immediately.

Ministry of Economic Affairs, 16 August 2011

On behalf of the Minister

Helga Jónsdóttir

Kjartan Gunnarsson