

Regulation

ON RELIABILITY AND INFORMATION SECURITY REQUIREMENTS FOR IDENTIFICATION SERVICE PROVIDERS AND CERTIFICATION SERVICE PROVIDERS OFFERING QUALIFIED CERTIFICATES

Issued in Helsinki on 20 October 2010

The Finnish Communications Regulatory Authority (FICORA) has, under Sections 8(3), and 42(2) of the Act on Strong Electronic Identification and Electronic Signatures of 7 August 2009 (617/2009), prescribed as follows:

1 §

Scope of application

This regulation applies to identification service providers offering services for strong electronic identification and certification service providers offering qualified certificates. These will later be referred to as the 'service provider'.

2 §

Information security management

Organizing information security

A service provider must determine in writing the organizing, responsibilities and reporting relations of information security. These must be maintained up-to-date and updates must be verified at least once a year. The responsibilities of persons with executive information security duties must be included in their job description.

Information security control documentation

A service provider must have a written view of its executives on the objectives, principles and implementation of information security. Personnel related to the provision of identification services or qualified certificate services must be informed of the view.

FICORA 8 C/2010 M

In addition, a service provider must keep written documents on how the special areas below have been taken into consideration to the extent that they apply to the service to be provided:

- 1) Administrative and organizational security;
- 2) personnel security;
- 3) physical security;
- 4) hardware and software security;
- 5) communications security;
- 6) information material security;
- 7) operations information security; and
- 8) interference in information security violations and misuse.

Risk management

A service provider must draw up a plan to assess the risks related to the service. A service provider must identify and assess information security risks in operations, data and systems that are essential to identification services and qualified certificate services. A service provider must have risk acceptance methods for those significant risks which avoid any control measures on the basis of risk evaluation. Risk management must be systematic, regular and documented.

Information security measures

On the basis of risk analysis results, a service provider must draw up a plan detailing measures, responsibilities and schedules in order to manage the identified risks. A service provider must regularly monitor the suitability of the measures for the purpose they are meant for.

A service provider must define sufficiently detailed instructions for individual procedures that are relevant to information security.

A service provider must ensure that the personnel responsible for offering identification and qualified certificates services are trained in accordance with given instructions.

A service provider must have a security classification for information material that is vital to the service offered.

A service provider must ensure that incidents that are significant to information security are identified. A service provider must react to identified problems.

Monitoring of information security management

At regular intervals, the implementation of the obligations in the regulation must be monitored, and always when needed.

3 §

Initial identification and registration of an applicant

An identification service provider must check the identity of the applicant of an identification device in accordance with Section 17 of the Act on Strong Electronic Identification and Electronic Signatures. A certification service provider offering qualified certificates must check the identity of the applicant of a qualified certificate in accordance with Section 35 of the Act. The objective of initial identification is to ensure that the information of the identification device or qualified certificate, and electronic services that they enable, is correct and reliable.

Initial identification must be performed in connection with the acquisition of the identification device or qualified certificate. The applicant's identity and other related information must be carefully verified before the identification device or qualified certificate is issued to the applicant for the first time.

An identification service provider must store the information on the initial identification of the applicant and the document used for the purpose.

If the identification method is based on a certificate or in case of qualified certificate, the service provider must collect and store the information related to the information content of the certificate. In case the certification service provider will not create a pair of keys, it must check that the applicant has in his or her possession a private key corresponding to the public key to be certified.

A certification service provider offering qualified certificates must enter the applicant's information into the register in connection to the acquisition of a qualified certified. The information to be entered into the register includes the applicant's name and sufficient information to distinguish between persons with the same name. In addition, any significant information on initial identification, necessary information on the documents used for the identification and other information essential to issuing a qualified certificate must be entered into the register.

4 §

Creation of identification devices and qualified certificates

An identification device or a qualified certificate can only be created if the application of the person applying for an identification device or qualified certificate fulfils the requirements set for the issuance of qualified certificates or identification devices. Identification devices or qualified certificates must not be created before the applicant has passed initial identification.

A service provider must store the information on the creation of identification devices and qualified certificates.

As they create identification devices and qualified certificates, service providers must ensure that their systems maintain the confidentiality and integrity of data.

The service must be sufficiently secure to ensure that only the holder of an identification device or qualified certificate has access to using an identification device or qualified certificate.

The algorithms and keys used for the identification method or a qualified certificate must be secure and meet the generally-accepted standards or recommendations.

5 §

Delivery of certificates

A service provider and certificate holder can agree on informing parties relying on the certificate of the certificate. If the service provider publishes the certificates in a public directory, the directory must be available round-the-clock.

A service provider must not copy any secret information related to the certificate, because they should only be used by the applicant and others should not be aware of it.

6 §

Service provision**Documents related to the service**

A service provider must maintain a certificate policy and certificate practice. Also, the identification service principles must be publicly available and updated.

The information security and certificate policy, identification principles, and information security and certificate practices of parties of cross-certification must correspond to one another.

Revocation of identification devices and qualified certificates and verification of validity

A service provider must handle any revocation requests for identification devices and signature devices without delay in such a manner that all requests are identified and handled with sufficient accuracy.

A service provider must store the information on suspending an identification device or signature device, reintroducing a device after suspension and revoking a device. This information must be available to parties relying on the service without delay after the service provider has been informed of the reason for revocation or suspension.

A service provider must be able to revoke all identification and signature devices. A service provider must inform the holder of an identification and a signature device of the revocation.

The parties relying on the certificate must be in a position to check the status of the certificate by means of a certificate revocation list service. A revocation list service can be real-time or regularly updated. The service provider must sign the revocation lists and revocation list replies. A signed revocation list or reply must include the date of publication of the list or the date of the reply.

Certification service provider's signature keys

A service provider must ensure that the private signature keys used for creating certificates cannot be reintroduced after their lifespan has come to an end.

FICORA 8 C/2010 M

A service provider must ensure that all private and secret keys used for creating and signing certificates are stored in a secure place. The environment for storage and back-ups must be secured and authorized persons only may perform these tasks.

Significant events in service provision

A service provider must store information on all events which are relevant to service provision.

Prevention of unauthorized use

A service provider must protect the identification device and qualified certificate against unauthorized use.

A service provider must ensure that secret information related to the qualified certificate or identification device are not exposed to its personnel in any circumstances.

7 §

Termination of operations

An identification service provider must inform FICORA, all persons involved in the identification activities, identification device holders, service providers using the identification service and other stakeholders related to identification activities, of the termination of operations. The identification service provider must also ensure that the harm caused to identification device holders and service providers using the identification service is minimised.

A certification service provider offering qualified certificates must inform FICORA, all persons involved in qualified certificate activities, qualified certificate holders and stakeholders related to its operations, of the termination of operations. The certification service provider must also ensure that the harm caused to qualified certificate holders and parties relying on qualified certificates is minimised.

8 §

Transitional provisions and entry into force

This regulation enters into force on 20 October 2010 and will remain in force until further notice. The regulation repeals FICORA's regulation 8 B/2009 M of 27 August 2009 M on the requirements for reliability and information security in the operation of certification authorities providing qualified certificates to the public.

9 §

Information and publication

This regulation is included in the Series of Regulations issued by the Finnish Communications Regulatory Authority and available from FICORA's Customer Service:

Office address	Itämerenkatu 3 A, HELSINKI
Postal address	P.O. Box 313 FI-00181 HELSINKI
Telephone	09 6966 500
Fax national	09 6966 410
website:	http://www.ficora.fi/
Business identification code	0709019-2

Helsinki 20 October 2010

Acting Director-General Jorma Koivunmaa

Director Timo Lehtimäki