

**EXPLANATIONS AND APPLICATION OF
REGULATION 7**

**OBLIGATION OF IDENTIFICATION
SERVICE PROVIDERS AND
CERTIFICATION AUTHORITIES
PROVIDING QUALIFIED
CERTIFICATES TO THE PUBLIC TO
SUBMIT NOTIFICATIONS TO FICORA**

CONTENTS

CONTENTS 1

1 LEGISLATION 2

1.1 LEGISLATIVE BASIS FOR REGULATION 2

1.2 EC LEGISLATION 2

1.3 OTHER RELEVANT STATUTES..... 2

2 PURPOSE AND VERSION HISTORY OF THE REGULATION 2

2.1 PURPOSE OF THE REGULATION 2

2.2 KEY AMENDMENTS AND VERSION HISTORY 3

2.3 DEFINITIONS..... 3

3 PARAGRAPH-SPECIFIC EXPLANATIONS AND APPLICATION INSTRUCTIONS 3

3.1 §1 SCOPE OF APPLICATION 3

3.2 §2 IDENTIFICATION SERVICE PROVIDER’S DECLARATION OF STARTING A BUSINESS 4

3.2.1 Assessment of the reliability of an identification service provider’s operations 4

3.2.2 Assessment of the information security of an identification method 6

3.3 §3 DECLARATION OF STARTING A BUSINESS BY A CERTIFICATION AUTHORITY PROVIDING QUALIFIED CERTIFICATES. 6

3.3.1 Assessment of the reliability of a certification authority’s operations 6

3.3.2 Assessment of the information security of a certification service 8

3.4 §4 DECLARATION OF OPERATIONAL CHANGES 8

3.5 §5 ANNUAL REPORT 9

3.6 §6 DECLARATION OF TERMINATION/TRANSFER OF OPERATIONS..... 10

3.7 §7 OTHER NOTIFICATIONS 10

4 REFERENCE LIST 11

1 LEGISLATION

The objective of this chapter is to provide regulation users with an overview of the statutes on which the regulation is based. Moreover, the chapter lists other appropriate legislation within this area.

1.1 Legislative basis for regulation

Regulation 7 B /2009 M is based on sections 10(4), 32(1) and 42(2) of the Act on Strong Electronic identification and Electronic Signatures (617/2009), hereinafter Identification Act [1]. The Act on Strong Electronic identification and Electronic Signatures entered into force on 1 September 2009, enforcing Directive 1999/93/EC of the European Parliament and of the Council [2].

According to section 10 of the Identification Act, Finland-based identification service providers must notify FICORA prior to starting operations. The notification obligation of a certification authority providing qualified certificates is determined in section 32 of the law. Section 16 of the law details identification service providers' obligation to notify of threats and disruptions concerning information security. Section 42 of the law determines FICORA's authorisation to issue technical regulations regarding reliability and information security requirements for service provider operations.

According to section 43 of the Identification Act, FICORA has the right to obtain information from identification service and qualified certificate providers. According to section 42 of the law, FICORA is responsible for supervising compliance with the law and the statutes issued thereunder. The statutes related to issuing technical regulations are sections 8(3), 10(4), 32(1) and 42(2) of the Act.

According to the transitional provision of the Identification Act's section 51(1), identification service providers must notify FICORA in accordance with section 10 within six months of the law entering into force. According to subsection 4 of the section, a certification authority providing qualified certificates that has provided notification in accordance with section 9(1) of the Act on Electronic Signatures, and continued operations without interruption until the Identification Act enters into force, is not obliged to issue a new notification in accordance with section 32(1).

1.2 EC legislation

Directive 1999/93/EC of the European Parliament and of the Council [2].

In Finland, this directive was enforced by the Act on Electronic Signatures (14/2003). The Identification Act replaced the Act on Electronic Signatures. Regulations concerning qualified certificates were also transferred to this law.

There are no EC regulations regarding identification services as regulation 7B/2009 enters into force.

1.3 Other relevant statutes

FICORA's regulation (FICORA 8) on the requirements for reliability and information security in the operation of certification authorities providing qualified certificates.

2 PURPOSE AND VERSION HISTORY OF THE REGULATION

The objective of this chapter is to provide regulation users with information on the goals and purpose of this regulation. The most significant amendments to the regulations and recommendations preceding this regulation are also detailed in this chapter.

2.1 Purpose of the regulation

Under sections 10(4) and 32(1) of the Identification Act, FICORA has issued the regulation FICORA 7B/2009 on the obligation of identification service providers and certification authorities providing qualified certificates to the public to submit notifications to FICORA. The content requirements of the notifications provided to FICORA by such certification authorities are detailed in regulation sections 2 to 7.

2.2 Key amendments and version history

The following amendments were made to regulation 7A.

New statutes regarding the notification obligation of identification service providers were added to the regulation.

The reporting obligation of qualified certification authorities was slightly reduced with regard to interim reports and annual reports. Moreover, some minor changes were made to the other statutes concerning notification obligations.

An obligation for qualified certification authorities to notify FICORA, if they confirm that the certificates of a certification authority not based within the EEA are qualified certificates, was also added to the regulation.

The validity period of the regulation was amended to being valid until further notice.

2.3 Definitions

The terms used in the regulation and its application instructions correspond to the definitions of the Identification Act. In the regulation and its explanations, service provider refers to both identification service providers and certification authorities providing qualified certificates to the public. The Act is not available in English at the time the regulation and explanatory note are published.

3 PARAGRAPH-SPECIFIC EXPLANATIONS AND APPLICATION INSTRUCTIONS

This chapter covers paragraph-specific explanations and application recommendations.

3.1 §1 Scope of application

This FICORA regulation is applicable to both identification service providers and certification authorities providing qualified certificates related to electronic signatures.

Identification service provider means a service provider that provides strong electronic identification services for service providers using them, releases authentication devices for the public, or both. An identification service provider may thus provide release-of-authentication devices, other identification services, or both.

The Identification Act and, consequently, the regulation are not applied to internal identification within a community, or if a community uses its own identification method for identifying its customers within its services. Therefore, matters such as identification methods fall within the regulation's scope of application only to the extent that an identification service provider provides an identification method through an identification service, for other service providers to use in identifying their customers.

A certification authority is considered to be providing certificates to the public if it provides certificates to a user group that has not been restricted in advance. The regulations do not apply to providing certificates to a closed-off user group such as certificates provided for in-house use within a corporate group. Moreover, the regulation is not applied to voluntary civil contracts that have been made to determine rules for the use of electronic signatures within a certain, limited group of participants. An open user group would be constituted in a situation in which the party relying on the certificate did not have a contractual relationship with the certification authority or signatory.

The regulation is not applicable to the manufacture, importation or sale of authentication devices or electronic signature devices. The release of authentication devices can be separated from their manufacture, importation and sale in such a manner that a contractual relationship mostly exists between the releaser and device holder. In the case of electronic signatures, a revocation list maintained by the certification authority is one of the elements that make the activity a service, separating it from pure manufacture, importation and sales of the device.

3.2 §2 Identification service provider's declaration of starting a business

Prior to starting operations, a Finland-based identification service provider must provide FICORA with the information¹ on the basis of which FICORA can assess the legality of the identification service provider and the provided service. This notification must be submitted in writing. The written format requirement can also be fulfilled by providing an electronic notification in accordance with the Act on Electronic Services and Communications in the Public Sector (13/2003) [3].

The notification obligation is set for identification service providers based in Finland. Under law, a consortium of service providers that manages a service that should be considered a single identification service can also submit this notification.

FICORA assesses the fulfilment of the legal requirements set for the identification service provider and the provided service before they are entered in the FICORA register, in compliance with section 12 of the Identification Act. However, the identification service provider may initiate operations immediately after submitting the notification, before entry in the register.

If the notification is inadequate, FICORA must request the submitter of the notification to complete the notification. If the service or service provider do not fulfil the legal requirements, FICORA must, after receiving the notification, forbid the service provider from providing its service as a strong electronic identification service. If the inadequacy can be considered minor, FICORA may request that the service provider remedy this inadequacy within a set time.

3.2.1 Assessment of the reliability of an identification service provider's operations

An identification service provider must report the following information to FICORA for the assessment of the reliability of the service provider's operations:

Information on identification service provider

The identification service provider must report the following contact information to FICORA, as applicable:

- name of company / identification service provider
- business ID
- extract from the trade register
- postal address
- visiting address
- telephone number
- fax number
- contact person
- e-mail address
- link to website.

¹ According to the transitional provision of the Identification Act's section 50(1), identification service providers must notify FICORA of the start of operations within six months of the Act's enter into force.

In addition, the identification service provider must inform FICORA of contact information to a service, complying with section 25(1) of the Identification Act, where the holder of the authentication device may request revocation or prevention of the authentication device.

Information on principles of identification

The principles of identification determine how well an identification service provider fulfils the obligations determined in the Identification Act. The identification principles comprise:

- information on the implementation of initial identification
- service descriptions of the provided services
- information on the service provider's primary partners, and
- information on reviews conducted by notified bodies.

The service description must indicate whether the identification service provider exclusively offers an authentication device release or other identification service, or both. The service description must also include information on whether the identification service provider's authentication devices can be used for making electronic signatures and which type of signatures are in question.

The principles of identification must also indicate how the identification service provider has arranged the possibility for authentication device holders to notify, in accordance with section 25 of the Identification Act, that the authentication device is lost, or that it has been used improperly or that it is being illegally possessed by others.

Information on personnel

The identification service provider must provide FICORA with the relevant information on its personnel and on persons used in providing the identification service as well as other information that can be used to assess the expertise, experience and competence of the identification service provider. The service provider must also submit a declaration to FICORA, stating that the organisation's accountable persons are reliable, fulfilling the requirements determined for identification service providers in section 9 of the Identification Act.

Information on information security principles

Included in the information to be submitted to FICORA, for assessing the information security of the identification service and the reliability of the service provider's operations, is a written opinion, accepted by the management, on the goals, principles and implementation of the service provider's information security activities. Moreover, the service provider must provide information on the standards with which it complies, and any possible statements by an accreditation body, if this information is not included in the identification principles. Based on this information, FICORA can determine whether sufficient attention has been paid to information security and whether the related responsibilities have been adequately defined.

Information on storage of information

A description of the procedures concerning the storage of information related to the identification event and device must also be attached to the report. This description must indicate, for instance, how the processing of information in various storage formats and ensuring its availability have been taken into account in all phases of the lifecycle of that information. Information material security is determined in more detail in regulation FICORA 8.

Other information relevant to the reliability of a service provider's operations

Identification service providers must possess adequate financial resources with respect to their activities, in order to organise their operations and cover possible liability for damages. Observed as a whole, the information provided must form an accurate and adequate picture of the service provider's financial resources, the financial risks related to the operations, and the risk management principles.

The sufficiency of the identification service provider's financial resources can be assessed, for instance, by means of the previous year's annual report, financial statements, and budget and

operating plans. As for fledgling businesses, the sufficiency of their financial resources can be assessed, for instance, by means of an operating plan and a result and balance budget, drafted for the first financial period, as well as a budget plan for the next two financial periods.

General information security requirements are determined in more detail in regulation FICORA 8.

3.2.2 Assessment of the information security of an identification method

The identification service provider must submit the following information to FICORA for the assessment of the identification method's information security.

Information on authentication device

The identification service provider must provide FICORA with a description of key lengths, algorithms, and other issues affecting the reliability of the authentication device.

Information on systems

The identification service provider must provide FICORA with information on/a description of the systems and products that are relevant to the identification service, including the revocation list service. This report must comprise information on the hardware and software used (inc. used key lengths, algorithms and purposes of use) as well as information on the standards with which the company complies and any possible statements by an accreditation body. Based on this information, FICORA can assess whether the information security and availability of the service provider's equipment have been ensured in the legally determined manner.

Structure of the certificate's data content

If an identification method is based on a certificate, the identification service provider must also provide FICORA with information on the structure of the certificate's data content. The structure of the certificate's data content must comply with the legal requirements in force.

3.3 §3 Declaration of starting a business by a certification authority providing qualified certificates

A certification authority providing qualified certificates to the public must, before starting operations², submit information to FICORA that FICORA can use to assess the authority's ability to serve as a qualified certificate provider as well as the legality of the provided certification service. FICORA assesses the fulfilment of the legal requirements set for the certification authority and the provided service before the certification authority is entered in the FICORA register, in compliance with section 32(4) of the Identification Act. However, the certification authority may initiate operations immediately after submitting the notification, before entry in the register.

If a certificate or the certification authority does not fulfil legal requirements, FICORA must immediately forbid the certification authority from offering its certificates as qualified certificates. A prohibition decision may be given, for instance, if FICORA is unable to assess the conformity of the certification authority's operations or its certificates due to the inadequacy of the information provided. Before the decision is issued, however, the certification authority is entitled to complement and/or correct the information it has provided in accordance with FICORA's requests.

3.3.1 Assessment of the reliability of a certification authority's operations

The following information must be submitted to FICORA for assessing the reliability of the operations of a certification authority providing qualified certificates to the public:

² According to the transitional provision of Identification Act's section 51(4), a certification authority that has issued notification in accordance with section 9(1) of the Act on Electronic Signatures, and continued operations without interruption until the Identification Act enters into force, is not obliged to submit a new notification.

Information on certification authority

The certification authority must report the following contact information to FICORA, as applicable:

- name of company / certification authority
- business ID
- extract from the trade register
- postal address
- visiting address
- telephone number
- fax number
- contact person
- e-mail address
- link to website.

The certification authority must also inform FICORA of contact details for a service where the signatory may request that the qualified certificate be revoked. Provisions of this service are included in section 36 of the Identification Act.

Information on provided services

The report must include information on the provided services that are related to electronic signatures and qualified certificates. The certification authority must inform FICORA of its procedures, and provide information on the implementation of these procedures and the provided services that are related to qualified certificate services.

The reported information includes at least the following: the information issued to the qualified certificate applicant upon registration, information on the terms and conditions of qualified certificate use, determined by the certification authority, as well as the certificate policy and certificate practice statement (CPS). The certificate policy and certificate practice statement can be used to assess whether the lawful procedural requirements for certification authorities providing qualified certificates are realised in the certification authority's operations.

Information on personnel

The certification authority must provide a report on the personnel it utilises, including competence and task descriptions. Task descriptions can be allocated to various task categories (e.g. system administrator, certificate issuer) by means of, for instance, an organisational description and general competence requirements. The certification authority must also provide information on the distribution of its certification-related activities among, for instance, subcontractors, and the aforementioned information on the personnel the subcontractors use in performing the certification authority's tasks. Activities outsourced by the certification authority may include:

- registration
- creation of qualified certificates
- distribution of qualified certificates
- management of revocation list requests
- revocation list service.

Information on information security principles

Based on the information security policy and principles, FICORA can determine whether sufficient attention has been paid to information security and whether the related responsibilities have been adequately defined.

Other relevant information

Certification authorities must possess adequate financial resources with respect to their activities in order to organise their operations and cover possible liability for damages. Observed as a whole,

the provided information must form an accurate and adequate picture of the certification authority's financial resources, the financial risks related to the operations, and the risk management principles.

The sufficiency of the certification authority's financial resources can be assessed, for instance, by means of the previous year's annual report, financial statements, and budget and operating plans. As for fledgling businesses, the sufficiency of their financial resources can be assessed, for instance, by means of an operating plan and a result and balance budget, drafted for the first financial period, as well as a budget plan for the next two financial periods.

3.3.2 Assessment of the information security of a certification service

The certification authority providing qualified certificates to the public must provide FICORA with the following information for assessing the information security of the certification service:

Information on systems

The certification authority must provide FICORA with information on/a description of the systems and products that are relevant to the provision of qualified certificates. This report must comprise information on the hardware and software used (inc. the key lengths and algorithms used) as well as information on the standards with which the company complies and any possible statements by an accreditation body. This information can be used to assess whether the systems used by the certification authority are reliable in the sense required under the legislation in force.

Standards and technical specifications related to electronic signatures, qualified certificates, and certification authorities' operations have been prepared by CEN/ISSS, ETSI and IETF, among others. These documents cover the data content of the qualified certificate, the certificate policy for certification authorities providing qualified certificates, a secure signature creation device, and the certification authority's secure systems as well as other such matters.

3.4 §4 Declaration of operational changes

The identification service provider and the certification authority providing qualified certificates to the public must, on their own initiative, report any substantial changes in their operations or the information provided under sections 2 to 3, to FICORA.

Public register maintained by FICORA

The identification service provider and the certification authority providing qualified certificates to the public must always inform FICORA of any changes to the information in the public register maintained by FICORA. These changes must be reported a month before they enter into effect.

FICORA keeps at least the following information on identification service providers in its public register:

- name of identification service provider
- contact information for identification service provider (name, postal address, website, phone number)
- provided services
- termination of the identification service provider's operations
- contact information for a service where the authentication device holder may notify that the device be revoked or its use prohibited.

FICORA keeps at least the following information, on certification authorities providing qualified certificates, in its public register:

- name of qualified certificates

- contact information for certification authority (name, postal address, website, phone number)
- certification policy employed in granting qualified certificates (OID number)
- termination of the certification authority's operations
- contact information for a service where the signatory may request revocation of the qualified certificate.

Changes related to the information security of a service

The identification service provider and the certification authority providing qualified certificates to the public must inform FICORA of any changes concerning the information security and reliability of identification or certification operations.

Changes which service providers must report to FICORA include:

- changes to revocation list services and systems used for creating certificates:
 - significant hardware updates
 - software version updates, and
 - replacing software with other software.

Changes related to the reliability of a service provider

The identification service provider and the certification authority providing qualified certificates to the public must provide FICORA with reports on any significant changes in the service provider's personnel, utilised persons and general reliability. These include:

- outsourcing of operations
- transfer of outsourced operations to another actor
- changes in key personnel
- moving operations to other facilities

Moreover, the identification service provider and the certification authority providing qualified certificates to the public must provide FICORA with all accounts that indicate a substantial deterioration in the service provider's financial standing or a substantial increase in financial risks. These accounts must be delivered to FICORA immediately after their completion. Factors indicating a substantial deterioration in financial standing or substantial increase in financial risks include:

- order to enter service provider into liquidation
- significant credit losses
- bankruptcy of the parent company
- restructuring of service provider's debts, liquidation, or bankruptcy
- substantial increase in costs of liability coverage system (e.g. insurance).

3.5 §5 Annual report

The identification service provider and the certification authority providing qualified certificates to the public must provide FICORA with an annual report detailing the extent of the provider's previous year's operations falling under the law's scope of application. The annual report must be delivered within two months of the end of the calendar year.

The identification service provider must also provide FICORA with the number of the granted authentication devices and identification incidents. The certification authority providing qualified certificates to the public must provide FICORA with the number of qualified certificates granted and revoked during the year and the certificates valid at the end of the year.

Moreover, the service providers must provide FICORA with statistics on detected problematic situations as well as other information relevant to their operations, including the number of customer complaints (possibly separate statistics on invoicing complaints and complaints concerning service errors or disruptions).

3.6 §6 Declaration of termination/transfer of operations

With regard to the monitoring of the identification service provider and the certification authority providing qualified certificates to the public, it is essential that FICORA receive notice of the termination or transfer to another service provider of that service provider's operations at as early a stage as possible. The primary means of striving to anticipate termination comprises the reporting obligation on operational changes. In addition to reports on changes, however, the service provider must separately inform FICORA of the termination of identification service or qualified certificate provision, or the transfer of these operations to another service provider in connection with, for instance, a transfer of business operations.

The identification service providers' declaration must also include information on how the service provider has informed or intends to inform the holders of authentication devices, service providers using the identification service, and other cooperation partners related to the service provider's operations, of the termination or transfer of operations.

The certification authorities' declaration must include information on how the certification authority has informed or intends to inform the assisting personnel, signatories and other cooperation partners related to certification operations, of the termination or transfer of operations.

3.7 §7 Other notifications

The identification service provider and the certification authority providing qualified certificates to the public must inform FICORA, without unwarranted delay, of any significant threats or faults to which the service is subject as well as of the measures performed in order to rectify these.

Under this regulation, information security refers to the administrative and technical measures used to ensure that certain information can only be accessed by authorised parties, that information cannot be modified by anyone other than the authorised parties, and that information and information systems are available to the authorised parties. Since availability forms part of the information security of services, FICORA must also be informed of any fault and error situations affecting service availability.

Matters of which the service provider must inform FICORA include:

- failures in the functionality of revocation lists
- intrusions into the service provider's systems
- disclosure of the certification authority's certificate signature key
- any serious cases detected of misuse of authentication and signature devices
- serious internal misuse.

The notification must include detailed descriptions of the following matters, among others:

- time of incident
- how and by whom was the incident detected
- causes leading to the incident
- the extent and effects of the incident
- planned/performed corrective measures, and repair schedule, and
- contact information for the person responsible for handling for the incident.

If all of this information is not readily available, it can be submitted afterwards to FICORA. The key issue is that FICORA be informed of the incident without delay.

The certification authority providing qualified certificates must notify FICORA if they confirm that the certificates of a certification authority not based in the EEA in accordance with section 31(1)(3) of the Act are qualified certificates. This notification must include the name and contact information of the certification authority that is not based in the EEA, as well as information on those certificates of the non-EEA certification authority which the Finland-based certification authority confirms to be qualified certificates.

4 REFERENCE LIST

- [1] The Act on Strong Electronic identification and Electronic Signatures (617/2009), available in Finnish and Swedish
<http://www.finlex.fi/fi/laki/alkup/2009/20090617>
<http://www.finlex.fi/sv/laki/alkup/2009/20090617>
- [2] Directive 1999/93/EC of the European Parliament and of the Council, issued on 13 December 1999, on community framework for electronic signatures.
<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31999L0093:FI:NOT>
<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31999L0093:EN:NOT>
- [3] Act on Electronic Services and Communications in the Public Sector (13/2003),
<http://www.finlex.fi/fi/laki/ajantasa/2003/20030013>
<http://www.finlex.fi/fi/laki/kaannokset/2003/en20030013.pdf>
- [4] ETSI TS 101.862 Qualified Certificate Profile
<http://pda.etsi.org/pda/queryform.asp>
- [5] RFC 3039 Internet X.509 Public Key Infrastructure Qualified Certificates Profile
<http://www.ietf.org/rfc/rfc3039.txt>
- [6] Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
<http://www.ietf.org/rfc/rfc3280.txt>