Regulation on Electronic Identification and Trust Services

Issued in Helsinki on 14 May 2018

The Finnish Communications Regulatory Authority (FICORA) has, under section 42 of the Act on Strong Electronic Identification and Electronic Trust Services (617/2009) of 7 August 2009, as amended in Act 533/2016, laid down as follows:

Chapter 1 General provisions

Section 1 Objective of the Regulation

The objective of this Regulation is to:

1) promote the information security and technical interoperability of means for strong electronic identification and identification broker services,

2) refine the criteria for the conformity assessment of strong electronic identification services as well as the criteria for the independence and competence of assessment bodies,

3) complement the requirements concerning qualified electronic trust services and the independence and competence criteria in relation to their conformity assessment in so far as they are not laid down in the legislation of the European Union, and

4) complement the certification criteria of electronic signature or electronic seal creation devices in so far as they are not laid down in the legislation of the European Union.

Section 2 Scope of application

This Regulation shall apply to the provision and conformity assessment of means for strong electronic identification and identification broker services referred to in the Act on Strong Electronic Identification and Electronic Trust Services (617/2009, hereinafter referred to as the *Identification and Trust Services Act*) that have been notified to FICORA.

This Regulation shall apply to the qualified trust services referred to in the Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (hereinafter referred to as the *EU Regulation on electronic identification and trust services*

or the *eIDAS Regulation*) and to their conformity assessment, as well as to the certification of electronic signature or seal creation devices.

This Regulation shall apply to the strong electronic identification schemes notified to the European Commission or the trust services referred to in section 2 above and their conformity assessment, as well as to the certification of electronic signature or seal creation devices, only if not otherwise provided by the eIDAS Regulation or the implementing acts of the Commission adopted thereunder.

Section 3 Definitions

For the purposes of this Regulation:

1) *interface* means specifications and implementations in relation to data transfers between two separate systems or parts of such systems;

2) *eIDAS interface* means the interface of a national node to the national node of another state.

Otherwise, the definitions of the Identification and Trust Services Act and the eIDAS Regulation shall apply in this Regulation.

Chapter 2 Information security requirements of an identification service

Section 4 Information security management requirements of an identification service provider

The identification service provider shall apply the ISO/IEC 27001 standard or another corresponding, well-known information security management standard to the management of the information security of its identification scheme. Information security management may also be based on the combination of several standards.

Information security management shall cover the following aspects concerning the provision of identification service:

1) the overall context of the identification service provider;

2) governance, organisation and maintenance of information security management;

3) management of information security risks related to the provision of the identification service;

4) resources allocated to information security, competences, staff awareness of information security, communication, documentation and the management of documented information;

5) planning and control of the provision of the identification service for the purpose of meeting information security requirements; and

6) evaluation of the efficiency and effectiveness of information security management.

Section 5 Technical information security measures of the identification scheme

The identification scheme shall be designed, implemented and maintained to take into account the following aspects of the scheme:

1) telecommunication security
    a) structural network security
    b) zoning of the communications network
    c) filtering rules according to the principle of least privilege
    d) administration of the entire life cycle of the filtering and control systems
    e) control connections
2) computer security
    a) access rights control
    b) identification of the users of the scheme
    c) hardening of the scheme
    d) malware protection
    e) tracing of security events
    f) security incident observation capability and recovery
    g) internationally or nationally recommended encryption solutions in other respects than those laid down in section 7
3) operator security
    a) change management
    b) processing environment of secret materials
    c) remote access and remote management
    d) management of software vulnerabilities
    e) backup copies

Production network together with its control connections referred to paragraph 1(1)(e) and remote access and remote management referred to in paragraph (1)(3)(c) above must be implemented in such a way that the information security threats caused by other services of the organisation,

such as e-mail or web browsing, or information security threats caused by other functions than those essential to management in a terminal used for the management, are

a) at substantial assurance level specifically assessed and minimised, and

b) at high level of assurance prevented when assessed as a whole.

Section 6 Information security requirements of the identification method

An identification means shall not be connected to an applicant before the applicant has passed initial identification or it has been otherwise ensured in the process of granting an identification means that the identification means is not available before the initial identification referred to in section 17 of the Identification and Trust Services Act has been performed.

The service provider shall ensure that secret information related to the identification means are not revealed to its staff under any circumstances.

The service provider shall not make copies of any secret information related to the identification means.

Section 7 Encryption requirements of the identification scheme and interfaces

Interfaces between identification service providers and interfaces between an identification service provider and an eService shall be encrypted. The following methods shall be used in the encryption, key exchange and sign-cryption:

1) **Key exchange**: In key exchange, DHE methods or ECDHE methods with elliptic curves shall be used. The size of the finite field to be used in calculations shall be at least 2048 bits in DHE and at least 224 bits in ECDHE.

2) **Signature**: When using the RSA for electronic signatures, the key length shall be at least 2048 bits. When using the elliptic curve method ECDSA, the underlying field size shall be at least 224 bits.

3) **Symmetrical encryption**: The encryption algorithm shall be AES or Serpent. The key length shall be at least 128 bits. The encryption mode shall be CBC, GCM, XTS or CTR.

4) **Hash functions**: The hash function shall be SHA-2, SHA-3 or Whirl-pool. SHA-2 refers to functions SHA224, SHA256, SHA384 and SHA512.

Encryption settings shall be technically forced to the minimum levels listed above to avoid a situation where settings weaker than the minimum levels are adopted following connection handshakes.

If the TLS protocol is used, version 1.2 of TLS or newer shall be used. Version 1.1 of TLS may only be used if the user's terminal does not support newer versions.

The integrity and confidentiality of messages containing personal data shall be protected by encryption referred to paragraph 1 above and also at a message level in accordance with paragraph 1.

The integrity and confidentiality of the identification scheme record keeping shall be ensured. If the data protection is only based on encryption, requirements laid out in paragraph 1 above concerning signatures, symmetrical encryption and hash functions shall apply.

Section 8 Information security requirements concerning the interface between an identification means provider and an identification broker service provider

Encryption methods shall meet the requirements of section 7(1)–(4) above.

In identifying the parties and in relaying the data necessary for identification, metadata or similar procedures that ensure a corresponding level of information security shall be used.

All personal data shall be encrypted and signed at the message level.

Section 9 Information security requirements at the eService interface

The interface between an identification broker service provider and an eService shall meet the requirements of section 7(1)–(4) above.

An identification means provider and identification broker service shall ensure the confidentiality and integrity of personal data at the eService and user interface.

Section 10 Information security requirements at the national node interface

The interface between the provider of an identification broker service and the national node shall meet the requirements of section 7(1)–(4) above.

Section 11 Disturbance notifications by the identification service provider to FICORA

Notifications of a significant threats or disturbances provided to FICORA in accordance with section 16 of the Identification and Trust Services Act shall contain at least the following information:

1) the identification means or the broker service affected by the disturbance;

2) description of the disturbance and its known reasons;

3) description of the impact of the disturbance, including the impact on the issuance of new identification means, their users, relying parties, other parties of the trust network, and cross-border operations;

4) description of corrective measures; and

5) description of the provision of information on the disturbance to relying parties, identification means holders and the trust network as well as information on notifying other authorities.

In assessing the significance of a disturbance, the disturbance is deemed more significant if it relates to incorrectness or abuse of electronic identity or to an information security threat or disturbance that compromises the integrity and reliability of identification. The disturbance is also deemed more significant if it affects a trust network.

Chapter 3 Relaying information in a trust network

Section 12 Minimum set of data relayed in a trust network

The following minimum set of data shall be relayed at the interface between the identification means provider and the provider of an identification broker service:

1) in identification events concerning natural persons: at least the first name, family name, date of birth and the unique identifier of the person;

2) in identification events concerning legal persons: at least the first name, family name and the unique identifier of the natural person representing the legal person as well as the unique identifier of the organisation; and

3) an indication of whether the level of assurance is substantial or high.

The interface between the identification means provider and the provider of an identification broker service must enable the implementation of the relay of the following information:

1) an indication of whether the identification event concerns a public administration eService or a private eService;

2) in identification events concerning natural persons: forename(s) and surname(s) at the time of birth, place of birth, current address and gender;

3) in identification events concerning legal persons:

   a) current address;

   b) VAT registration number;

   c) tax reference number;

d) the identifier related to Article 3(1) of Directive 2009/101/EC of the European Parliament and of the Council[1];

e) Legal Entity Identifier (LEI) referred to in Commission Implementing Regulation (EU) No 1247/2012[2];

f) Economic Operator Registration and Identification (EORI) referred to in Commission Implementing Regulation (EU) No 1352/2013[3]; and

g) excise number provided in Article 2(12) of Council Regulation (EC) No 389/2012[4].

Section 13 Information required in cross-border identification operations

When using a Finnish identification means on a foreign eService, the same information shall be relayed at the interface between the identification means provider and the provider of an identification broker service as required by section 12 concerning national identification in a trust network. It shall be possible to pass on the information between the identification broker service and the national node. In addition, an indication of whether the identification event relates to a public administration eService or to a private eService shall be relayed.

When using a foreign identification means on a Finnish eService, the minimum set of information determined for international eIDAS interface shall be relayed at the interface between the national node and the provider of a broker service, and the interface shall be equipped for relaying the optional set of information determined for international eIDAS interface. The unique identifier of a person shall be relayed in the format in which the national node receives it from the international eIDAS interface. It shall be possible to pass on the information between the identification broker service and the eService. In addition, an indication of whether the identification event relates to a public administration eService or to a private eService shall be relayed.

---

[1] Directive 2009/101/EC of the European Parliament and of the Council of 16 September 2009 on coordination of safeguards which, for the protection of the interests of members and third parties, are required by Member States of companies within the meaning of the second paragraph of Article 48 of the Treaty, with a view to making such safeguards equivalent (OJ L 258, 1.10.2009, p. 11).

[2] Commission Implementing Regulation (EU) No 1247/2012 of 19 December 2012 laying down implementing technical standards with regard to the format and frequency of trade reports to trade repositories according to Regulation (EU) No 648/2012 of the European Parliament and of the Council on OTC derivatives, central counterparties and trade repositories (OJ L 352, 21.12.2012, p. 20).

[3] Commission Implementing Regulation (EU) No 1352/2013 of 4 December 2013 establishing the forms provided for in Regulation (EU) No 608/2013 of the European Parliament and of the Council concerning customs enforcement of intellectual property rights (OJ L 341, 18.12.2013, p. 10).

[4] Council Regulation (EU) No 389/2012 of 2 May 2012 on administrative cooperation in the field of excise duties and repealing Regulation (EC) No 2073/2004 (OJ L 121, 8.5.2012, p. 1).

Section 14 Data transfer protocol and other requirements

The identification means provider, the provider of the identification broker service, the eService provider and the national node operator shall negotiate the properties of their mutual interfaces (other than those laid down in this Regulation) and the respective protocol to be employed.

Chapter 4 Assessment criteria related to the identification service

Section 15 Assessment criteria

The identification service assessment shall cover the requirements concerning the following:

1) certain properties of the functions affecting the provision of the identification service (the identification scheme), namely:
    a) information security management
    b) record keeping
    c) facilities and staff
    d) technical measures
2) the identification method, meaning certain properties of the identification means, namely:
    a) application and registration
    b) identity proofing and verification of the applicant
    c) identification means characteristics and design
    d) issuance, delivery and activation
    e) suspension, revocation and reactivation
    f) renewal and replacement
    g) authentication mechanisms.

The assessment of the aspects referred to in paragraph 1 above shall be based on the requirements of the Identification and Trust Services Act and this Regulation, the rules and guidelines of the EU or other international body, published and universally or regionally applied information security guidelines, or widely adopted information security standards or procedures.

Section 16 Declaration of compliance with other requirements

The identification service provider shall provide proof, by means of either a written self-declaration or an assessment referred to in section 15 above, of its compliance with the following requirements related to the reliability of

the identification service provider and the information provided on the identification service:

1) published notices and user information, such as identification principles, price lists and terms and conditions

2) established organisation

3) preparedness to bear risks of damage

4) sufficient financial resources

5) responsibility for subcontractors

6) planning for the termination of operations.

Section 17 National node assessment criteria

Assessment of the information security of a national node shall be based on the standard ISO/IEC 27001 and the European Commission Implementing Regulation (EU) 2015/1501[5].

Chapter 5 Competences of the identification service assessment body

Section 18 Requirements concerning an external assessment body of the identification service

The independence and competences of an assessment body, referred to in section 33 of the Identification and Trust Services Act, may be proven through one of the following:

1) accreditation based on standard ISO/IEC 27001 or other proof of the competence to perform assessments according to the standard;

2) competence proven according to an internationally renowned self-regulation arrangement based on WebTrust guidelines;

3) accreditation based on the PCI DSS payment card standard or other proof of the competence to perform assessments according to the standard;

4) competence proven according to the ISACA standards and IT management framework; or

5) compliance with other, comparable rules, guidelines or standards on general information security management or sector-specific regulation or standardisation or providing proof of competences required therein.

[5] Commission Implementing Regulation (EU) 2015/1501 of 8 September 2015 on the interoperability framework pursuant to Article 12(8) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market

Proof of the competence to assess identification schemes also requires demonstrating how, and to what extent, the rules, guidelines or standards referred to in paragraph 1 above concern the identification scheme.

Section 19 Requirements concerning an internal notified body of the identification service

The independence of an internal notified body, referred to in section 33 of the Identification and Trust Services Act, may be proven through one of the following:

1) compliance with the IIA standards for professional practice (independence and objectivity of internal auditing, including organizational independence);

2) compliance with the ISACA standards and IT management frameworks;

3) compliance with the BIS (Bank for International Settlements) internal audit guidelines;

4) compliance with the regulations and guidelines on internal auditing of the FIN-FSA Regulations and Guidelines;

5) compliance with instructions or regulations issued by the corresponding supervisory authorities of other EEA Member States; or

6) compliance with other comparable standards concerning public control or overall independent internal audit management.

Proof of the competence to assess identification schemes also requires demonstrating how, and to what extent, an internal audit arranged according to the rules, guidelines or standards referred to in paragraph 1 above concern the identification scheme.

Chapter 6 Qualified trust services

Section 20 Assessment criteria for a qualified trust service provider

In addition to the requirements laid down in the eIDAS Regulation, a qualified trust service provider shall meet the requirements of standard EN 319 401.

In addition to the requirements of paragraph 1, a qualified trust service provider issuing certificates shall also meet the requirements of standard EN 319 411-1.

In addition to the requirements laid down in paragraphs 1 and 2 above, a qualified trust service provider issuing qualified certificates or qualified website certificates for electronic signatures or seals shall also meet the requirements of standard EN 319 411-2.

In addition to the requirements of the above paragraphs 1 and 2, a qualified trust service provider issuing qualified time stamps shall also meet the requirements of standard EN 319 421.

Compliance may be proven through observation of the standards referred to in paragraphs 1 to 4 above or through other means to achieve corresponding level of reliability.

Section 21 Assessment criteria for a qualified trust service

Certificates issued by a qualified trust service shall, in addition to the requirements of the eIDAS Regulation concerning certificates of electronic signatures and seals as well as website certificates, meet the requirements of standards EN 319 412-1, EN 319 412-2, EN 319 412-3, EN 319 412-4 and EN 319 412-5, as applicable.

The protocol and time stamp profile employed by a qualified time stamp service shall comply with standard EN 319 422.

Compliance may be proven through observation of the standards referred to in paragraphs 1 to 2 above or through other means to achieve corresponding level of reliability.

Chapter 7 Conformity assessment bodies of trust services

Section 22 Evaluation of the competence of assessment bodies

For the conformity assessment bodies of trust services, a prerequisite for complying with the requirements of section 33, paragraphs 1(3) and 1(4) of the Identification and Trust Services Act is that the assessment body meets the requirements of standard EN 319 403 or other corresponding requirements.

For the conformity assessment bodies of trust services, a prerequisite for complying with the requirement of section 33, paragraph 1(2) of the Identification and Trust Services Act is that the assessment body is sufficiently competent to perform assessments according to the criteria for trust service providers listed in section 20 above and the criteria for trust services listed in section 21 above.

Chapter 8 Certification of qualified electronic signature or electronic seal creation devices

Section 23 Requirements for electronic signature or seal creation devices

Requirements for chip-based electronic signature or seal creation devices that are in the physical possession of a user are laid down in the European Commission Implementing Decision (EU) 2016/650[6].

Section 24 Requirements for certification bodies

A prerequisite for complying with the requirements of section 36 of the Identification and Trust Services Act is sufficient competence and resources for verifying the requirements of the eIDAS Regulation and the Commission Implementing Decision referred to in section 23 above in the device to be certified.

Compliance with the requirements referred to in paragraph 1 above may be demonstrated through accreditation or other independent investigation. Competence may also be demonstrated through an inclusion in SOGIS-MRA (*Senior Officers Group for Information Systems, Mutual Recognition Agreement*), an agreement between certain certification bodies of EU or EEA Member States.

Chapter 9 Provisions on entry into force

Section 25 Transitional provisions and entry into force

This Regulation enters into force on 22 May 2018 and will remain in force until further notice.

This Regulation repeals the Regulation 72/2016 M on Electronic Identification and Trust Services issued by the Finnish Communications Regulatory Authority on 2 November 2016.

If the TUPAS protocol is used at the identification service interfaces, all the requirements of chapter 2, sections 7(4) and 8(3) concerning the encryption of personal data at the message level and the requirement of section 9(2) of the protection of personal data at the eService and user interface shall be met by 1 October 2019 at the latest. The identification service provider shall define an implementation that meets all the requirements of this Regulation by 1 October 2018 at the latest and make the altered interfaces available in the trust network and to relying parties by 1 March 2019 at the latest.

---

[6] COMMISSION IMPLEMENTING DECISION (EU) 2016/650 of 25 April 2016 laying down standards for the security assessment of qualified signature and seal creation devices pursuant to Articles 30(3) and 39(2) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market

A plan for the technical implementation of relaying the information referred to in section 12(2) must be made by 1 October 2018 at the latest.

Section 26 Information and publication

This Regulation is included in the Series of Regulations issued by the Finnish Communications Regulatory Authority and it can be obtained from the FICORA Customer Service Office:

Visiting address	Itämerenkatu 3A, Helsinki
Postal address	P.O. Box 313, FI-00181 Helsinki
Telephone	+ 358 295 390 100
Fax	0295 390 270
Website	http://www.ficora.fi/
Business ID	0709019-2

Issued in Helsinki on 14 May 2018

Kirsi Karlamaa
Director-General

Jarkko Saarimäki
Director