Issued:	Entry into force:	Validity:
20 May 2022	1 June 2022	until further notice

Legal basis:
Act on Strong Electronic Identification and Electronic Trust Services (617/2009), section 42, as amended with Act 230/2021

Provisions on sanctions for operations violating this Regulation are laid down in:

Act 617/2009, section 45, section 45 a

Implemented EU legislation:
-

Modification details:
This regulation repeals regulation Viestintävirasto 72 A/2018 (Regulation 72A/2018 on Electronic Identification and Trust Services)

Regulation on Electronic Identification and Trust Services (M72 B/2022)

Contents

Chapter 1 General provisions

1 Scope of application

1.1

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 the Finnish Transport and Communications Agency.

1.2

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.

1.3

This Regulation shall apply to the strong electronic identification schemes referred to in section 1 if they are notified to the European Commission and to the trust services referred to in section 2 and their conformity assessment, as well as to the certification of electronic signature or seal creation devices, unless otherwise provided in the eIDAS Regulation or the implementing acts of the Commission adopted thereunder.

2 Meaning

The objective of this Regulation is to:

1) promote the information security and technical interoperability of means for strong electronic identification and the services by providers of identification brokering 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) complete the requirements set for qualified electronic trust services and the independence and competence criteria of their compliance assessment insofar as they are not regulated by European Union legislation; and

4) complete the certification criteria of electronic signature or seal creation devices insofar as they are not regulated by European Union legislation.

3 Definitions

3.1

For the purposes of this Regulation:

1) *interface* means specifications and implementations in relation to data transfers between two different systems or parts thereof;

2) *digital certificate* means an electronic certificate the purpose of which is to demonstrate that the holder of the certificate is a certain person, organisation or system and to connect the authentication data to the holder.

3.2

This regulation also subscribes to the definitions specified in section 2 of the Identification and Trust Services Act, Article 3 of the eIDAS Regulation and section 1 of the appendix to the Commission implementing regulation (EU) 2015/1502, hereinafter referred to as *regulation on Level of Assurance in Electronic Identification,* laid down in point 3 of Article 8 of the eIDAS Regulation.

Chapter 2 Information security requirements of an identification service

4 Information security management system of the identification service provider

4.1 Information security management standard

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

4.2 Information security management scope

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

1) 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 steering of the provision of the identification service for the purpose of meeting information security requirements; and

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

5 Information security requirements of an identification scheme

5.1 The resistance of the identification scheme

5.1.1

The communications and information systems of the identification scheme and their operation must be planned, executed and maintained throughout the life cycle of the service so that the integrity and confidentiality of the identification service are protected. The identification service must be able to resist at least moderate or high-level threats and attack potential specified in section 2.3 of the appendix to the regulation on *Level of Assurance in Electronic Identification* in accordance with the assurance level of the identification service.

5.1.2

The encryption requirements concerning communications connections between identification service providers and the identification service and the relying party are specified in section 7. The encryption of other communications connections of the identification scheme and information systems and data must employ encryption methods specified in section 7 of the regulation, where technically applicable, unless the overall ability of the system to protect itself is otherwise realised by other security means.

5.2 Communications security

The identification scheme communications must be planned, executed and maintained with:

a) structural network security;

b) zoning of the communications network;

c) filtering rules according to the principle of least privilege;

d) administration of filtering and control systems;

e) secure administration connections; as well as

f) employing internationally or nationally recommended encryption methods.

5.3 Information systems security

The identification scheme information systems must be planned, executed and maintained with:

a) access control according to the principle of least privilege;

b) unique identification of the users of the systems;

c) hardening of the systems;

d) malware protection;

e) ability to trace security events and tracing procedure;

f) ability to detect security incidents and repair procedure; as well as

g) employing internationally or nationally recommended encryption methods.

5.4 Safety of operation

The identification scheme operation must be planned, executed and maintained with:

a) change management;

b) confidential data processing environment and storage based on data classification;

c) protecting remote use and administration from threats in the remote use environment;

d) software development and software vulnerability management;

e) backup procedures; and

f) employing internationally or nationally recommended encryption methods.

5.5 Administration and remote connections of the production network of the identification scheme

The production network together with its administration connections and remote access and remote administration referred to in subsections 5.2.e) and 5.4.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 administration in a terminal used for the administration, are

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

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

6 Information security requirements of the identification means

6.1 Identification means characteristics and its resistance

6.1.1

The authentication factors, authentication mechanism and security measures of the identification means must be planned, executed and maintained so that they protect the integrity and confidentiality of the identification means. The identification means must be able to resist at least moderate or high-level threats and attack potential specified in section 2.3 of the appendix to the regulation on *Level of Assurance in Electronic Identification* in accordance with the assurance level of the identification service.

The resistance must be based on a risk assessment including specific assessments of threats directed at an authentication mechanism and authentication factors based on possession, knowledge and inherence as well as assessment of security measures in place to protect against these threats.

6.1.2

The features and security measures of the identification means must prevent the possibility that the compromise of one authentication factor would compromise the reliability of other authentication factors. The security measures protecting the identification means must separate and protect the authentication factors especially if they are used on the same terminal device.

6.1.3

The identification means and authentication must employ internationally or nationally recommended encryption methods. The communications connection between the identification means and the identification scheme must employ encryption methods specified in section 7 of the regulation, where technically applicable, unless resistance of the system assessed as a whole is otherwise realised by other security means.

6.2 Specific security measures

6.2.1

The identification service must present the user with information during the identification event, based on which the user may ensure that the identification request received in the identification means by the user is connected to the user's event. This information must be presented in identification means that have the technical ability to do so.

6.2.2

The identification service must present the identification means user with information concerning the relying party, for whom the identification is carried out, during the identification event. This information must be presented in identification means that have the technical ability to do so.

6.2.3

In this regulation, single sign-on refers to the identification service offering authentication to more than one relying party based on a single authentication of the holder using strong electronic identification means.

In planning, executing and maintaining single sign-on, the identification service must take care of the security measures based on the management of the length, transfer and ending of the session related to single sign-on and ensure that information concerning relying parties specified in section 6.2.2 is presented to the user.

6.3 Connecting identification means to a person

6.3.1

The authentication factors of the identification means must be bound to the identification means holder in the identification scheme.

6.3.2

An identification means shall not be bound 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 functional before the initial identification referred to in section 17 of the Identification and Trust Services Act has been performed.

6.4 Processing identification means holder-specific data

6.4.1

The identification service provider shall ensure that secret data related to an identification means is not revealed to its staff under any circumstances.

6.4.2

The identification service provider shall not make copies of any secret data related to an identification means.

7 Identification scheme interface encryption requirements

7.1 Communications encryption methods

7.1.1

Interfaces between identification service providers and interfaces between an identification service provider and relying parties shall be encrypted. The following methods shall be used in the encryption, key exchange, digital certificates and signing:

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 2,048 bits in DHE and at least 224 bits in ECDHE.

2) **Signature or asymmetric encryption:** When using the RSA for electronic signatures or encryption, the key length shall be at least 2,048 bits. When using the ECDSA or EdDSA methods with elliptic curves, the size of the finite field must be at least 224 bits.

3) **Symmetrical encryption:** The encryption algorithm must be AES, Serpent or ChaCha20. The key length shall be at least 128 bits. The encryption mode must be CBC, CCM, GCM or CTR.

4) **Hash functions:** The hash function or authentication code must be SHA-2, SHA-3, Whirlpool or Poly1305.

7.1.2

In addition to methods and values mentioned in section 7.1.1, methods and values that have been assessed as secure in use specified in subsections 1–4 in the current versions of the following documents may also be complied with:

a) Kryptografiset vahvuusvaatimukset luottamuksellisuuden suojaamiseen - kansalliset turvallisuusluokat (Dnro 190/651/2015) instruction (in Finnish) issued by the Crypto Approval Authority operating within the Finnish Transport and Communications Agency; or

b) SOG-IS Crypto Evaluation Scheme Agreed Cryptographic Mechanisms of the SOGIS-MRA (*Senior Officers Group for Information Systems, Mutual Recognition Agreement*), an agreement between certain certification bodies of EU or EEA Member States.

7.1.3

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.

7.2 Communications encryption protocol

If the TLS protocol is used, version 1.2 of TLS or newer shall be used.

8 Authenticating parties to the communications

8.1 Verification of the parties to the communications connection

The authenticity and integrity of the digital certificates or keys used to encrypt the communications or messages as well as their holders must be verified in establishing communications connections between identification services and identification services and relying parties.

The authentication must be based on a qualified electronic signature or a qualified electronic seal in compliance with the eIDAS Regulation or a direct bilateral procedure. Authentication may not only be based on a generally trusted digital certificate.

8.2 Certificate and key renewal

The digital certificates and keys referred to in section 8.1 above must be regularly renewed.

In order to ensure the authenticity and integrity of new digital certificates and keys, the renewal must be carried out in one of the following ways:

a) in accordance with the procedure in section 8.1;

b) by providing new keys via a communications connection, whose integrity and confidentiality has been ensured by binding the parties' communications to digital certificates or keys provided in accordance with section 8.1; or

c) by signing a new key using a key provided in accordance with section 8.1 or a key chained from such a key.

9 Integrity and confidentiality of authentication messages

9.1 Protecting messages between identification services and relying parties

9.1.1

The integrity and confidentiality of authentication messages containing personal data must be protected in communications between identification services and between identification services and relying parties in one of the following ways:

a) by ensuring the integrity and confidentiality of the communications connection by binding the parties' communications to digital certificates or keys provided in compliance with section 8; or

b) by encrypting and signing the messages with a key provided in compliance with the procedure in section 8.

9.1.2

Authentication messages between identification broker services and relying parties must be authenticated with signatures.

9.2 Protecting messages in the user interface

If the authentication messages are relayed via the user's browser or terminal device, the messages must be encrypted and signed in accordance with subsection 9.1.1.b).

9.3 Encryption algorithms and procedures

The encryption and signing of messages must employ the procedures specified in section 7.1, where applicable.

10 Information security requirements at the national node interface

The interface between the identification broker service provider and the national node must meet the requirements specified in sections 7–9.

11 Incident notifications by the identification service provider to the Finnish Transport and Communications Agency

11.1 Significant threats and disruptions

Significant disruptions to the identification service that need to reported to the Finnish Transport and Communications Agency according to section 16 of the Identification and Trust Services Act include events that are connected to incorrectness or abuse of electronic identity or to an information security threat or disruption that compromises the

integrity and reliability of identification. Unforeseeable disruptions with greater than minor effects on the trust network are also considered significant.

11.2 Reported information

Notifications of significant threats or disruptions provided to the Finnish Transport and Communications Agency shall contain at least the following information:

1) identification means or identification broker service affected by the disruption or threat;

2) description of the disruption or threat and any known reasons for it and its duration;

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

4) description of corrective measures; and

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

11.3 Reporting procedure

Significant disruptions or threats must be reported to the Finnish Transport and Communications Agency electronically by using an online form, e-mail or secure e-mail.

The report may be amended later on if all of the information is not available at the time of the initial report submitted without undue delay in accordance with section 16 of the Identification and Trust Services Act.

Chapter 3 Identification service interoperability

12 Minimum set of data to be relayed in the trust network

12.1 Mandatory set of data

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 authenticated by the identification means provider;

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 authenticated by the identification means provider;

3) an indication of whether the level of assurance is substantial or high; as well as

4) name of the relying party authenticated by the identification broker service.

12.2 Optional information

The interface between the identification means provider and the provider of an identification broker service must have the technically planned possibility to relay the following information:

1) 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; and

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[1] of the European Parliament and of the Council;

   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].

12.3 Pseudonymisation of identification

The duties specified in sections 12.1 and 12.2 above pertain to the interface between the identification means and the identification broker service in authenticating the user even when the identification broker service only discloses the pseudonym of the identification means user or a limited amount of personal data on the user to the relying party in accordance with section 8, subsection 2 of the Identification and Trust Services Act.

13 Information required in cross-border use

When using a Finnish identification means notified in accordance with the eIDAS Regulation 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 the trust network. It must be possible to relay the information between the identification brokering service and the national node. In addition, an indication of whether the identification

[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).

event relates to a public administration eService or to a private eService shall be relayed.

14 Data transfer protocol and other requirements

14.1 Data transfer protocol

The identification service provider must enable the chaining of initial identification in accordance with section 17 of the Identification and Trust Services Act and relaying identification events within the trust network in accordance with section 12 a of the Identification and Trust Services Act using an interface conforming to at least either the OpenID Connect or SAML protocol.

14.2 Other features of the interface

The identification means provider, the provider of the identification broker service, the relying party 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

15 Conformity assessment criteria

15.1 Identification scheme and identification means features to be assessed

The identification service assessment required in section 29 of the Identification and Trust Services Act must cover all of the requirements specified in the act and in this regulation, which pertain to:

1) certain properties of the functions affecting the provision of the identification service (the identification scheme), namely:
    a) information security management;
    b) record keeping and data processing;
    c) facilities and staff;
    d) technical measures (controls); and
    e) interoperability in the trust network; as well as
2) the identification means, 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; and

g) authentication mechanisms.

15.2 Assessment criteria

The conformity assessment may be based on the assessment guideline issued by the Finnish Transport and Communications Agency or 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. The assessment may be based on a combination of several sources mentioned above.

16 Report on the reliability of the identification service provider and the published data

In a notification made in accordance with section 10 of the Identification and Trust Services Act, the identification service provider shall provide proof, by means of either a written self-declaration or an independent and qualified notification or assessment 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) an established legal person in charge of the identification service and the competency and reliability of the persons in charge;

2) published notices and user information, such as identification principles, data protection principles, use restrictions, price lists and terms and conditions;

3) sufficient financial resources in order to organise operations and cover any liability for damages;

4) responsibility for subcontractors; as well as

5) for the event of termination of operations, a plan for a controlled termination or transfer of the service, data processing and notifications to authorities, to the trust network, to the relying parties and users.

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

18 Requirements concerning an external assessment body of the identification service

18.1 Proving procedures

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:

[5]Commission Implementing Regulation 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

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 recognised 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.

18.2 Competence

Proof of the competence to assess identification schemes also requires demonstrating how, and to what extent, the rules, guidelines or standards referred to in section 18.1 concern the requirements set for the identification scheme.

19 Requirements concerning an internal assessment body of the identification service

19.1 Independence

The independence of an internal assessment 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 organisational 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 government regulations or standards concerning overall independent internal audit management.

19.2 Competence

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 section 19.1 concern the requirements set for the identification scheme.

Chapter 6 Qualified trust services

20 Assessment criteria for a qualified trust service provider

20.1 Standards

20.1.1

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.

20.1.2

In addition to the requirements laid down in section 20.1.1, a qualified trust service provider issuing qualified website certificates or qualified certificates for electronic signatures or seals shall also meet the requirements of standards EN 319 411-1 and EN 319 411-2.

20.1.3

In addition to the requirements laid down in section 20.1.1, a qualified trust service provider issuing qualified time-stamps shall also meet the requirements of standard EN 319 421.

20.2 Voluntariness of the standards

Compliance may be proven through compliance with the standards referred to in section 20.1 or through other means to achieve a corresponding level of reliability.

21 Assessment criteria for a qualified trust service

21.1 Standards

21.1.1

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.

21.1.2

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

21.1.3

A qualified validation service for qualified electronic signatures or stamps must meet the requirements specified in standard EN 319 102-1, in addition to those specified in the eIDAS Regulation.

21.1.4

A qualified electronic registered delivery service must meet the requirements specified in standards EN 319 521 and EN 319 522, in addition to those specified in the eIDAS Regulation.

21.2 Voluntariness of the standards

Compliance may be proven through compliance with the standards referred to in section 21.1 or through other means to achieve a corresponding level of reliability.

Chapter 7 Conformity assessment body of trust services

22 Evaluation of the competence of assessment bodies

22.1 Assessment body operations

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

22.2 Competence

For the conformity assessment bodies of trust services, a prerequisite for complying with the requirement laid down in 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 seal creation devices

23 Electronic signature or seal creation device certification body

A prerequisite for complying with the requirements laid down in section 36 of the Identification and Trust Services Act is sufficient competence and resources for verifying that the requirements of the eIDAS Regulation and the Commission Implementing Decision (EU) 2016/650[6] or its replacement decision are fulfilled in the device to be certified.

Certification body compliance with the requirements 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 Transitional provisions and signatures

24 Transitional provisions and entry into force

24.1

The Regulation enters into force on 1 June 2022.

[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

24.2

The requirements laid down in section 6.2.1, section 6.2.2 and subsection 4 of section 12.1 of the Regulation must be implemented no later than on 1 June 2023.

24.3

The requirement on party identification specified in section 8.1 of the Regulation must be implemented

a) no later than on 1 June 2023 between identification services, and

b) no later than on 1 June 2023 between identification broker services and relying parties.

The requirement on updating keys and digital certificates in section 8.2 of the Regulation must be implemented no later than on 1 June 2023.

24.4

The procedure specified in subsection a of section 9.1.1. of the Regulation may be employed when a key or digital certificate in compliance with the requirements in section 8 is available.

The requirements in subsection b of section 9.1.1 and section 9.1.2 of the Regulation must be implemented within the transition period specified in section 24.3.

In Helsinki on 20 May 2022

Kirsi Karlamaa
Director-General

Sauli Pahlman
Deputy Director-General