Explanatory notes to the Regulation on electronic identification and trust services (M72B/2022)

Contents

1 Regulation background and legal basis

1.1 Regulation history and grounds for updates

This regulation repeals regulation Viestintävirasto 72 A/2018 (Regulation 72A/2018 on Electronic Identification and Trust Services) and issues a new, amended regulation.

Technological development, changes in information security threats, the progress in ETSI standards drafted for trust services, market development, application experiences from companies and the experiences of the Finnish Transport and Communications Agency on supervision require regular assessment of and changes to the requirements.

The current regulation on electronic identification and trust services was originally issued on 2 November 2016 in connection with the entry into force of the EU eIDAS Regulation (EU) 910/2014 to harmonise national and EU regulations and make them compatible. The intention was also to further the requirements for the nationally regulated strong electronic identification trust network in terms of competition and technical interoperability. The transition period of the regulation issued in 2016 was extended with an amendment on 14 May 2018. This means that the amended regulation is the third version of the current regulation.

Regulation 72/2016 M repealed FICORA Regulation 7 B/2009 M *on obligation of identification service providers and certification authorities providing qualified certificates*

to the public to submit notifications to FICORA and Regulation 8 C/2010 M *on reliability and information security requirements for identification service providers and certification service providers offering qualified certificates*. Regulation 7 laid down provisions on notifications of commencing or changing services and notifications of disturbances. Regulation 8 laid down provisions on information security requirements. Regulations concerning qualified certificates were issued for the first time in 2003, and in 2009 they were complemented with requirements concerning strong electronic identification services.

1.2 Legal basis of the regulatory authority

The authority is based on section 42 of the Act on Strong Electronic Identification and Electronic Trust Services (617/2009, the Identification and Trust Services Act)[1]

1.3 Other related regulations and provisions

1.3.1 Electronic identification

Government Decree 169/2016 on the trust network of strong electronic identification service providers, amended 1212/2018 (the 'trust network decree') [2]

The decree lays down provisions on certain administrative practices and interfaces. The decree is especially connected to chapter 3 of the Regulation, which concerns the interoperability of identification services.

*REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC ('**eIDAS** Regulation')*[3]

The provisions concerning trust services, accredited conformity assessment bodies and designated certification bodies for electronic signature or electronic seal creation devices is primarily provided in the eIDAS Regulation. The regulation provides minor, necessary additions to the provisions.

The Commission implementing acts specify the requirements of the eIDAS Regulation.

*Commission Implementing Regulation (EU) 2015/1502 ('**EU's Electronic Identification Assurance Level Regulation**') on setting out minimum technical specifications and procedures for assurance levels for electronic identification means pursuant to Article 8(3) 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*[4]

The EU Assurance Level Regulation lays down requirements for the assurance levels for electronic identification means. The Regulation applies to the identification means that are notified to the EU Commission. Several provisions on identification service requirements in the Identification and Trust Services Act refer to the Regulation, meaning that the Regulation, together with the Act, shall also be applied to identification means that are not notified.

The explanatory notes refer to the application guidelines concerning the Assurance Level Regulation, which have been drafted in cooperation by experts from Member States in a Cooperation Network.

*Commission Implementing Regulation (EU) 2015/1501 (‘**EU Interoperability 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.*[5]

The EU Interoperability Regulation mainly applies to the national node maintained by the Digital and Population data Services Agency. The specifications of minimum and optional attributes provided in the EU Regulation have also been implemented in national identification with this regulation. The EU Regulation also applies to the national node.

*Commission Implementing Decision (EU) 2015/1984 (‘**EU notification procedure decision’**) defining the circumstances, formats and procedures of notification pursuant to Article 9(5) 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*[6]

The EU notification procedure decision specifies the information to be included in the notification and the procedure to be followed. The Finnish Transport and Communications Agency, together with the identification means provider in practice, shall notify the identification scheme to the Commission and other Member States.

*Commission Implementing Decision (EU) 2015/296 (‘**EU cooperation network decision’**) establishing procedural arrangements for cooperation between Member States on electronic identification pursuant to Article 12(7) 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*[7]

The EU Cooperation Network decision contains provisions on the cooperation of Member States in the peer review related to the notification of identification schemes. The Finnish Transport and Communications Agency is a member of the Cooperation Network.

1.3.2 Electronic signature and seal creation device

*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 (Text with EEA relevance)*[8]

The Commission Implementing Decision sets out the requirements for the certification of electronic signature and seal creation devices. The provision is connected to provision 23 of the Regulation.

1.3.3 Personal data

*REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (‘**General Data Protection Regulation’**)* [9]

Definition of personal data according to Article 4

> *1) ‘personal data’ means any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier*

such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

Article 32 of the General Data Protection Regulation is applied to personal data information security.

Article 32 Security of processing

1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:

(a) the pseudonymisation and encryption of personal data;
[…]

2. In assessing the appropriate level of security, account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.

[…]

Section 29, subsection 4 of the Data Protection Act (1050/2018) [10] specifies the displaying of personal identity codes

A personal identity code shall not be unnecessarily entered into documents printed out from or drawn up based on a filing system.

2 Objective of the Regulation

2.1 Objectives

The specifications made to legal requirements with this Regulation make provisions foreseeable to operators and promote equal competition among operators. The Regulation aims to ensure the information security and interoperability of the services.

Preparatory work of the regulation together with the operators in the branch supports the specification of feasible requirements.

From the point of view of customers of identification and trust services, regulation ensures information security and the protection of privacy by design. Building trust in the branch requires that the operators build their services properly from the start.

2.2 Primary changes and assessment of the impact of the Regulation

The wording of the Regulation has been clarified in places. The layout of the Regulation has been changed to match the harmonised specifications of the Finnish Transport and Communications Agency, which is why some terminology changes have been made, for example. For the sake of clarity, sections and subsections are referred to as provisions to differentiate them from sections of the explanatory notes in these explanatory notes.

These explanatory notes have been formulated in accordance with the new practice adopted at the Finnish Transport and Communications Agency. The memorandum no longer contains explanatory sections adjacent to the theme.

The following sections describe the primary changes and their purposes. The impact will be addressed in further detail in the provision-specific explanations.

Provision 4 Information security management system

The wording of provision 4.1 will be changed to say that the selected **information security management standard(s) must be complied with, not only applied.** This makes the requirement slightly more restrictive. The purpose of this is to highlight the significance of the commitment of the identification service provider management and the significance of the maintenance of the information security management system and processes.

Certification is a good way to prove information security management conformity, but certification is not a requirement, even on the high assurance level.

The change to provision 4 does not require a transition period.

Provision 5 Information security requirements of an identification scheme

Provision 5.1 on the identification scheme's resistance is new to this version of the regulation.

A specification on the assurance level of the identification scheme's resistance will be added to the Regulation. Provision 5.1 specifies the level of the whole of the security measures and technical specifications of the identification scheme. This requirement could be derived from legislation by way of interpretation, but for added clarity, the matter is specified in the Regulation.

The required level of the security measures, i.e. technical controls, required in section 2.4.6 of the Electronic Identification Assurance Level Regulation, is specified based on the ability to provide protection against potential attacks specified in section 2.3.1 of the same regulation. No detailed criteria or standard to abide by will be regulated for the risk assessment. The assessment must be based on an excellent command of the branch and monitoring of the threats, vulnerabilities and technical developments.

Provisions from 5.2 to 5.4 on the safety of communications, information systems and operation will be specified to match established application. The requirement of good encryption practices and their relationship to encryption requirements in provision 7 will be clarified. The security requirement concerning the retention of data in section 7 of the act has been moved to provision 5.4.

The changes to provision 5 do not require a transition period.

Change to the recommendation related to provision 5: Recommendation on the reliability of the identification scheme time

The *Recommendation on the reliability of the identification scheme time* previously in section 1 of the explanatory notes 2016, part C, will be changed and moved to the explanatory notes of provision 5.3 e). The reliability of the time of the scheme is an important factor in logging and log time-stamps. It is also a core basic requirement. The provisions do not address time sources or synchronisation.

Provision 6 Information security requirements of an identification means

Provision 6.1 on identification means characteristics and resistance is new to this version of the regulation.

The purpose of this is to harmonise and improve the minimum security level of identification means and the related assessment. Identification means are constantly developing and information security threats are changing.

A requirement to perform a special risk assessment on the identification means will be added to the Regulation. The assessment must evaluate the threats related to various authentication factors and the authentication mechanism separately and the measures in place as protection against these threats. Of security measures, the regulation will address encryption solutions specifically as well as the separation of authentication factors, when they are used on the same terminal device (e.g. a mobile identification app and fingerprint or a PIN code).

The purpose of the special risk assessment requirement is to emphasise the importance of the design of the identification means security. The assessments will also provide the Finnish Transport and Communications Agency justified data based on which the agency may allocate identification service repair obligations pre-emptively and not only after an incident occurs.

A specification on the required level of the resistance of the identification means will be added to the Regulation. This requirement could be derived from legislation by way of interpretation, but for added clarity, the matter is specified in the Regulation. (Cf. corresponding change to provision 5). The requirement for the means to be able to protect itself will be specified by adding a reference to the Assurance Level Regulation and listing the components that must be observed in the threat and risk assessment in the Regulation.

According to an estimate by the Agency, this regulation model is flexible enough to allow identification services to develop their identification means. The model takes the security controls of the identification means into account as a whole.

Based on feedback from stakeholders, the Agency estimates that the identification means risk assessment requirement does not require a transition period.

As an alternative to provision 6.1, the Agency has assessed regulation models in which authentication factor specific requirements would be specified in the regulation or the requirements concerning the resistance of the identification means would be specified with a reference to a standard. Due to the diversity and development of authentication factors, an authentication factor specific regulation model would involve details that cannot be covered pre-emptively on a regulatory level, or doing so would not be practical, according to an evaluation by the Agency. Furthermore, threats to identification means security and security measures as protection against threats are not purely authentication factor specific. Resistance indicators or other specifications in the Regulation could be based on standards, but no such generally applicable standards that could be used to universally regulate compelling requirements exist to the Agency's knowledge.

Provision 6.2 on specific security measures is new to this version of the regulation.

The purpose of the provision is to harmoniously adopt some good security practices in identification means that allow for them in terms of technology.

A requirement (6.2.1), that identification request itemising data (***'session binding'***) that can be used to connect the service event and identification request and avoid authorising unjustified identification requests must be displayed to the user, will be added to the Regulation.

A requirement (6.2.2), that the **name of the relying party, or e-service**, must be displayed to the user, will be added to the Regulation. The displayed data will be authenticated by the identification broker service, but the allocation of the responsibility of displaying this data to the user is left to the discretion of the various operation models.

Provision 6.2.3 on single sign-on is new to this version of the regulation.

A provision (6.2.3) on **the security requirements of single sign-on** will be added to the regulation: a duty to manage session duration, transfer and termination related to single sign-on. In this respect, the purpose of the regulation is to lay down general provisions based on earlier cooperation with stakeholders. Single sign-on events must also display the names of the relying parties, or e-services, to the user.

A transition period will be given for the implementation of the requirements in provisions 6.2.1 and 6.2.2.

Provision 7 Encryption requirements of the identification scheme and interfaces

Provision 7.1 Communications encryption methods

The list of acceptable encryption methods and algorithms in communications encryption (7.1.1) in the regulation will be completed due to technical advancements. The section will be specified to also make it applicable with provisions concerning message encryption laid down in section 9. Encryption mode XTS, which is not technically suitable for encrypting communications or messages, but rather encrypting stored data on disks, will be left out of the section. Based on experience with supervision , the Agency is of the opinion that minimum requirements must be laid down unambiguously.

The option (7.1.2) to use algorithms and values listed by the Crypto Approval Authority (CAA) of the Finnish Transport and Communications Agency NCSA or SOGIS MRA, in addition to the algorithms and procedures listed, **will be added to the regulation**. The objective is to make the requirements more flexible in preparation for not having time to amend the regulation in keeping with rapid technical developments. The Agency is of the opinion that the regulation cannot be replaced by a mere reference to these sources, because they are maintained for a different purpose and they may in some regards be unnecessarily strict compared to identification requirements on the substantial assurance level.

Provision 7.2 Communications encryption protocol

The option to use version TLS 1.1 on exception will be removed from the regulation. This means that the required minimum level is TLS 1.2, without exception.

Based on experience from disallowing the use of version TLS 1.0 in the regulation issued in 2016, it is beneficial for fair competition that all identification services are

obliged to make the change at the same time. Based on feedback from stakeholders, the Agency has assessed that there is no need to provide a transition period for this requirement. TLS version 1.2 was widely adopted already during the previous transition period and it is also supported by terminal device hardware.

The changes to provision 7 do not require a transition period.

Recommendation on applying provision 7.1 on the high assurance level

The recommendation concerning encryption methods and algorithms on the high assurance level in the explanatory notes to the 2016 regulation will be retained as a recommendation and updated.

The recommendation corresponds to security category TL VI defined in the assessment guideline issued by the Crypto Approval Authority (CAA). The Agency assesses that making the values in the recommendation concerning the high assurance level mandatory would not cause interoperability issues, because identification brokering allows for case-specific selection of algorithms from the technical point of view. However, the Agency is of the opinion that the impact on relying parties using high assurance level identification is more difficult to assess.

Provision 8 Authenticating parties to the communications

The specification to the requirements in provision 8 and their extension to relying parties is the most significant and impactful change to the regulation.

The requirement to authenticate parties to communications in section 8.2 of the valid regulation will be specified by separating the establishment and management of a trust relationship. Provision 8 of the regulation specifies the requirements for communications connections between identification services and between identification services and relying parties, or e-services.

Provision 8.1 contains requirements for communications party authentication in establishing a trust relationship.

Provision 8.2 specifies the alternative procedures for updating digital certificates and keys in maintaining the trust relationship.

The purpose is to clarify the requirements and ensure the harmonised use of secure procedures, regardless of identification service. The requirements have proved ambiguous in practice and caused many issues with interpretation as well as varying procedures in terms of security, especially in authenticating relying parties, i.e. e-services.

The purpose of the requirements is to ensure that identification events are only relayed to organisations that have been reliably authenticated. Verifying the relying party is a crucial method of protecting the identification means user from verifying fraudulent identification requests. The purpose is also to ensure the integrity and confidentiality of communications and messages.

Requirements will provide better security than basic procedures of protocols, which trust any digital certificates generally trusted on the internet regardless of their actual reliability. Implementing the requirements requires process definitions concerning key and digital certificate provision and various setting determinations in server software in both identification services and e-services. That is why the impact and technical feasibility have been thoroughly assessed and considered and the technical

execution of the requirements using OpenID Connect and SAML protocols has been assessed in cooperation with stakeholders during the drafting phase. The Agency is of the opinion that the changes are technically feasible and necessary for the continued development of the security of strong electronic identification. However, these requirements need a transition period, especially in relation to e-services, and implementing the changes will require cooperation with guidance and communication services.

The Agency assesses that the changes to provision 8 require a transition period, because they have a significant effect on relying parties, i.e. e-services using identification services.

Provision 9 Integrity and confidentiality of identification messages

The categorical message-level encryption requirement will be changed so that an **alternative procedure** will be determined for securing the confidentiality and integrity of identification messages **alongside message encryption** by means of specific ensuring of the confidentiality and integrity of the communications connection. This alternative procedure is possible, if the messages are not relayed via the user's browser or terminal device.

The purpose of this change is to take into account the features of various standards and protocols and the purpose of the regulation better than in the valid regulation. This change will enable the current mobile digital certificate solution using the ETSI MSS standard and add flexibility when using the OpenID Connect protocol. The user's browser is usually used in connection with using the SAML protocol, meaning that message encryption must always be used.

The purpose of this requirement is to avoid unauthorised disclosure of personal data in the browser on the user's terminal device or on the servers. Together with the requirements in provision 8, identification message encryption and signatures also protect the identification event from forgery and duplication. The procedure also works to secure the provision of the verification of the user's authentication and personal data during authentication only to the correct relying party, i.e. the e-service. The protection requirement applies to connections between identification services and between identification services and relying parties alike.

The technical execution of encryption and signatures refers to provision 7, which has been changed to adapt it to message-level encryption in terms of technology.

Changes to provision 9 are tied to the requirements in section 8, meaning that the transition periods correspond to the transition periods in section 8.

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

Requirements concerning the notification procedure are added to the provision (11.3). The provision describes an established practice. The purpose is to clarify the obligation to provide notification to all identification services.

Otherwise, the provision clarifies the notification threshold for threats and disruptions and the content of the notification. The changes are in keeping with the supervision practice and do not change the requirement level.

In the opinion of the Agency, new notification thresholds do not need to be drafted for performance disruptions nor would it be functional. In this regard the assessment

from 2016 will not be amended. It should also be noted that the Identification Act does not contain specific requirements for the continuity, resilience or preparedness of identification services, meaning that the Agency has no authority to issue provisions on these.

The responses to the questionnaire on necessary changes to the regulation issued by the Agency contained concerns that not everyone would report disruptions to the Agency with a low enough threshold and that not all identification services would inform each other of disruptions. The Agency estimates that these observations should be primarily addressed with monitoring and by improving information exchange between the members of the trust network. The obligation to inform other operators is not covered by the regulatory authority. It is a matter for supervision.

The changes to provision 11 do not require a transition period.

Provision 12

Provision 12.1 on the mandatory set of data (attributes) brokered within the trust network.

Information on the relying party authenticated by the identification broker service, i.e. the name of the e-service, is added to the mandatory information in provision 12.1. 4). The purpose is to enable the practice of showing the user the name of the e-service that they are about to identify with specified in provision 6.2. to increase security.

Provision 12.3 on the pseudonymisation of identification is new to this version of the regulation.

Its purpose is to clarify attribute requirements in the interface between the identification means provider and identification broker service within the trust network if the e-service is only provided with a so-called impoverished confirmation of user authentication.

According to section 8, subsection 2 of the Identification and Trust Services Act, *the provisions of subsection 1 do not prohibit offering a specific service in a way that the identification service provider discloses to the service provider using the identification service the pseudonym of the identification means holder or only a limited amount of personal data.*

The act or this regulation do not lay down provisions on which personal data is provided to the relying party or authenticated through strong electronic identification. The regulation specifies the attributes that are processed in authentication within the trust network. Typically, the relying party will be provided with e.g. a name and personal identity code, but in keeping with the method described in the act the relying party may also be provided with a pseudonym or a limited amount of personal data. This also requires that the user is authenticated with strong identification means and the data concerning the identification event must be stored in accordance with section 24 of the act.

The term pseudonym is used instead of alias in the regulation because as far as regulation concerning personal data is concerned, these are pseudonymised personal data in the Agency's assessment. Even if the data were anonymous from the point of view of the relying party insofar as the relying party may not be able to

connect the data to a certain person, the data can be connected to a specific person based on the data saved by identification services when investigating disruptions, for example.

The changes to provision 12 do not primarily require a transition period. The processing of a name by a relying party in accordance with provision 12.1 is connected to the implementation of provision 6.2.2 in the regulation, meaning that the transition period is the same.

To the Agency's knowledge, pseudonymisation in accordance with provision 12.3 is not available, and any development of such a service must be based on the prerequisites of the regulation without a transition period.

Provision 14 Data transfer protocol and other requirements

The protocol used for data transfer in accordance with provision 14.1 has been specified by naming Open ID Connect and SAML as the standards, one of which must be used by the identification means provider as the minimum requirement for the interface used by the identification service for the chaining of initial identification between identification means providers in accordance with section 17 in the identification Act and for the identification brokering between the identification means provider and the identification broker service in accordance with section 12 a in the Act.

The purpose of the provision is to limit the number of the standards that the interfaces that the identification services must be prepared to maintain for their part to relay or receive identification data during initial identification or identification brokering.

In the provision, enabling means interpreting the requirement from the point of view of the rights of the recipient of the initial identification or identification event brokered to the relying party. The identification service may fulfil its obligations by offering the function through an identification service in another trust network, as long as the requirements laid down in the provisions and regulations are fulfilled.

The changes to provision 14 do not require a transition period.

Provision 15 Conformity assessment criteria

Interoperability within the trust network has been added as an assessed function to provision 15.1. According to section 29 of the Identification and Trust Services Act, interoperability is covered by conformity assessment, and the requirements are specified in chapter 3 of the regulation and they have been observed in the assessment guideline issued by the Finnish Transport and Communications Agency.

A reference to the assessment guideline issued by the Finnish Transport and Communications Agency as a possible set of assessment criteria has been added to the provision. The wording has been clarified.

The changes to provision 15 do not require a transition period.

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

The provision is connected to an identification service provider's obligation to notify commencement of operations and any changes to these operations according to section 10 of the Identification Act. The provision is also aimed at clarifying the infor-

mation that is not covered by the regular, independent and qualified conformity assessment specified in provision 15. The provision has been supplemented and amended in accordance with the supervision and guidance practice.

The changes to provision 16 do not require a transition period.

Provision 21 Assessment criteria for a qualified trust service

The provision specifies the conformity assessment criteria of qualified trust services by referring to existing ETSI standards. References to the standard concerning qualified validation services of electronic signatures or seals and the standards concerning a qualified electronic registered delivery service, which have been completed after the previous regulation was drafted, are added to the provision.

The purpose is to specify the assessment criteria insofar as the Commission has not exercised its authority to issue implementing acts. If the Commission were to issue implementing acts, the requirements in the Regulation would be repealed.

The changes to provision 21 do not require a transition period.

2.3 Other implementation options

The alternatives that were considered in the preparatory work of the provisions are described in the provision-specific explanations.

The feasibility of solving guidance requirements efficiently and equally using instructions and recommendations or co-regulation, instead of regulation, was reviewed during the Regulation drafting process. The assessments are included in the provision-specific explanations.

3 Preparatory work of the regulation

3.1 Key stakeholder consultation

On 4 August 2020, the Finnish Transport and Communications Agency conducted a comprehensive preliminary questionnaire on the field concerning any need for change oh the regulation (Doc. no. TRAFICOM/245890/03.04.05.00/2020). The questionnaire contained 74 questions. The questionnaire received eight replies. This input has been observed in the preparatory memoranda published during the preparatory phase.

A work plan concerning the amendment preparation of the regulation was published on 7 December 2020. The plan contains the issues under review, a grouping of the themes in stakeholder workshops and the entire timetable of the project. An updated version of the work plan was published on 26 March 2021, which described the policies drafted during the preparatory phase.

Seven workshops have been held for stakeholders and two additional workshops between 10 December 2020 and 16 June 2021, as specified in the work plan. The Agency has also met one on one with a few operators upon request. A preparatory memorandum has been published for each regulatory amendment theme before the workshop. This memorandum has contained the valid regulation and its explanations and earlier impact assessment, sources, input received from the preliminary questionnaire and proposed amendments to the regulations as well as views on the in-

formation security, feasibility and economic impact of the changes. Comments received in stakeholder workshops and the Agency's resulting conclusions have been compiled and published on the workshop presentation slides.

The restricted cooperation group within the identification service trust network, the identification and trust services eIDAS group open to all and the identification and trust services technical eIDAS group open to all have been notified of the drafting process of the Regulation by e-mail. This group includes a comprehensive number of identification and trust service providers, ICT operators, authorities and some e-services providers, who use identification and trust services. All preparatory material has been published on the Agency's website.

The consultation request has been provided to this same group on D Month 2021 and published in Lausuntopalvelu.fi, which is a service for responding electronically to official consultation.

The regulation concerns information society services and has been notified in accordance with the 'EU transparency directive' (EU) 2015/1535[1] on D Month 2021.

3.2 Comments received through consultation

A brief summary of the consultation (comments from stakeholders) may be included in the memorandum, a longer version may be provided as a separate annex.
A description of how the statements and comments have been observed and why must be provided. Statements in support of the regulation as well as statements opposing it must be presented. A summary of the comments may be provided as an annex.

Any notification comments must also be included.

4 Detailed rationale

Chapter 1 of the regulation General provisions

4.1 Provision 1 Scope of application

The Regulation applies, similarly to previous regulations, to the provision of *means of strong electronic identification*. Means of strong electronic identification mean those that have been notified to the Finnish Transport and Communications Agency and meet the set requirements.

The Regulation also applies to *identification broker services* notified to the Finnish Transport and Communications Agency. Identification broker service means brokering identification events to relying parties, or e-services.

The same legal person can act as both the identification means provider and the identification broker service, if they so wish.

The Regulation also applies to qualified trust services referred to in the eIDAS Regulation, meaning trust services that meet the requirements of the Regulation.

[1] DIRECTIVE (EU) 2015/1535 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services

The Regulation does not apply to trust services for which qualification has not been applied. According to section 42 b of the Identification and Trust Services Act and article 17 of the eIDAS Regulation, the task of the Finnish Transport and Communications Agency is to supervise non-qualified trust services under certain conditions, if the Agency is notified that non-qualified trust service providers or trust services provided by such providers do not allegedly meet the requirements specified in the regulation. In the Agency's assessment, actions during supervising situations could primarily be compared to the standards drafted to support the implementation of the eIDAS Regulation.

One reason why specific references to the EU legislation are necessary as clarifications in the regulation is that the precedence of EU law shall be clearly indicated.

No changes to the provision shall be made in the regulation in 2022, with the exception of the updating of the name of the Agency.

4.2 Provision 2 Objective

The provision describes briefly the principal objectives of the Regulation. The provisions are informative and do not e.g. define in more detail the scope of application of the requirements.

No changes to the provision shall be made in the regulation in 2022.

4.2.1 Identification services

Under the Identification and Trust Services Act, a requirement shall be adopted also at a national level that the minimum conditions to be met in the provision of identification services shall be those associated with the substantial level of assurance referred to in the Annex to the EU Assurance Level Regulation. The aim is to ensure that it is easy for various parties to apply for EU notification at whatever stage as long as they meet the requirements set at the national level. Therefore, it is not necessary for identification service providers to prepare a different identification solution for cross-border situations and national identification.

The drafting process of the Regulation is based on the same aim. In preparing the Regulation, the objective has been to draw on international standards, requirement specifications and notification methods to the greatest possible extent. The purpose of this solution is to facilitate cross-border provision of services and to avoid requirements that are tailored to national purposes.

4.2.2 Trust services

The general aim of regulation concerning trust services is to build the information society and increase confidence in e-services. The regulation concerning trust services helps the providers and users of electronic services identify the services that enable the implementation of the various e-service functions with the highest possible standard of information security.

The purpose of the Regulation is to clarify the requirements for qualified trust services laid down in the eIDAS Regulation by referring to international standards on which the EU preparatory work is based, inasmuch as these standards have not, at least by now, been referred to in the Commission implementing acts, even if the eIDAS Regulation would provide legislative competence to that effect.

References to standards in the Regulation also support what is to be taken as the minimum level of competence requirements in the accreditation of potential conformity assessment bodies.

4.2.3 Conformity assessment

The purpose of the Regulation is to clarify, for conformity assessment bodies and other parties, the requirements concerning trust services, inasmuch as the Commission has not exercised its legislative competence related to trust services and issued implementing acts that would refer to necessary standards.

With respect to identification service assessment, the purpose of the Regulation is to clarify the premises on which their assessment bodies are competent to perform identification scheme assessments. An assessment organisation of identification service providers does not have to apply for separate approval, unless it is an accredited conformity assessment body. The purpose of the Regulation is to provide various parties with a possibility to rely, as much as possible, on the audits that they are already performing.

4.3 Provision 3 Definitions

4.3.1 Provision 3.1 on Regulation definitions

The definition of an *interface* covers a more detailed specification of the elements dictated by the data transfer protocol and optional elements. It also covers the practical implementation, i.e. the range and format of the data content to be transferred.

The definition of a *digital certificate* will be added to the regulation. The definition in the Identification and Trust Services Act is tied to the digital certificates used in strong electronic identification or digital certificates offered as trust services.

The term digital certificate is used in its more general meaning in provision 8 of the Regulation. In general, digital certificates have different granting procedures, which is why their level of reliability varies quite significantly. The holder of the digital certificate is not always verified; instead, any information concerning the holder may be provided by the holder themselves. Authentication data means the holder's public key, which is part of the Public Key Infrastructure or PKI method. The private key connected to the public key should only be in the possession of the holder indicated in the digital certificate.

Cf. *certificate means an electronic verification that confirms the identity or confirms the identity and links the data in a trust service to the user of the trust service, and that can be used for strong electronic identification and trust services* in section 2.1(8) of the Identification and Trust Services Act

National node. The definition of the *eIDAS interface* is removed from the Regulation as unnecessary. The definition concerned interfaces between national nodes, and application experience has shown that the interface in question between the Digital and Population Data Services Agency and the nodes of public authorities in other member states does not affect national interfaces in the extent that would warrant the definition. Instead, the term *national node* is used. A *national node* is defined as a national interface related to the EU electronic identification interoperability framework in section 30 of the Identification and Trust Services Act. In Article 2 of the Commission Implementing Regulation (EU) 2015/1501 [5] *'node' means a connection point which is part of the electronic identification interoperability architecture*

and is involved in cross-border authentication of persons and which has the capability to recognise and process or forward transmissions to other nodes by enabling the national electronic identification infrastructure of one Member State to interface with national electronic identification infrastructures of other Member States.

The term national node is used in provisions 10, 13 and 17.

4.3.2 Provision 3.2 Definitions in the Identification Act and the eIDAS Regulations

The reference to provisions on higher levels of the hierarchy of the statutes is supplemented.

The following definitions laid down in section 2 of the Identification and Trust Services Act and Article 3 of the eIDAS Regulation are relevant to the Regulation:

Section 2 of the Identification and Trust Services Act [1]

> *1) **strong electronic identification** means the identification and verification of the authenticity and correctness of the identifying information of a person, legal person or a natural person representing a legal person by electronic means that fulfils the requirements of assurance level substantial referred to in Article 8 (2 b) of the EU Regulation on Electronic Identification and Trust Services or assurance level high in Article 8 (2 c);*
>
> *2) **identification means** means an **electronic identification means** referred to in Article 3(2) of the EU Regulation on Electronic Identification and Trust Services;*
>
> *3) **identification service provider** means the provider of an identification broker service or an identification means;*
>
> *4) **provider of an identification means** means a service provider that offers or issues electronic identification means for strong electronic identification to the general public and offers in the trust network their electronic identification means for a provider of an identification broker service to be distributed;*
>
> *5) **provider of an identification broker service** means a service provider that forwards strong electronic identification events to a party that relies on electronic identification;*
>
> *10) **trust network** means a network of identification service providers that have submitted a notification to the Finnish Transport and Communications Agency;*
>
> *11) **conformity assessment body** means a body approved by the Finnish Transport and Communications Agency and referred to in Article 2(13) regulation (EC) No 765/2008 of the European Parliament and of the Council setting out the requirements for accreditation and market surveillance relating to the marketing of products and repealing Regulation (EEC) No 339/93, which has been accredited in accordance with the Regulation.*

Article 3 of the eIDAS Regulation [3]

> *2) '**electronic identification means**' means a material and/or immaterial unit containing person identification data and which is used for authentication for an online service;*
>
> *4) '**electronic identification scheme**' means a system for electronic identification under which electronic identification means are issued to natural or legal persons, or natural persons representing legal persons;*

*6) '**relying party**' means a natural or legal person that relies upon an electronic identification or a trust service;*

*16) '**trust service**' means an electronic service normally provided for remuneration which consists of:*

a) the creation, verification and validation of electronic signatures, electronic seals or electronic time stamps, electronic registered delivery services and certificates related to those services, or

b) the creation, verification and validation of certificates for website authentication; or

c) the preservation of electronic signatures, seals or certificates related to those services;

*17) '**qualified trust service**' means a trust service that meets the applicable requirements laid down in this Regulation;*

*20) '**qualified trust service provider**' means a trust service provider who provides one or more qualified trust services and is granted the qualified status by the supervisory body;*

Section 1 in the Annex to the EU Assurance Level Regulation [4].

*2) '**authentication factor**' means a factor confirmed as being bound to a person, which falls into any of the following categories:*

a) ' possession-based authentication factor' means an authentication factor where the subject is required to demonstrate possession of it;

b) 'knowledge-based authentication factor' means an authentication factor where the subject is required to demonstrate knowledge of it;

c) 'inherent authentication factor' means an authentication factor that is based on a physical attribute of a natural person, and of which the subject is required to demonstrate that they have that physical attribute;

*3) '**dynamic authentication**' means an electronic process using cryptography or other techniques to provide a means of creating on demand an electronic proof that the subject is in control or in possession of the identification data and which changes with each authentication between the subject and the system verifying the subject's identity;*

*4) "**information security management system**' means a set of processes and procedures designed to manage to acceptable levels risks related to information security.*

Chapter 2 of the regulation Information security requirements of an identification service

4.4 Provision 4 Information security management system of the identification service provider

4.4.1 Provision 4.1 Information security management standard

The provision lays down general provisions on the aspects that need to be considered in the information security management of an identification scheme. The provision of an identification service means the overall identification scheme that covers the whole identification service.

Section 8(1)(5) of the Identification Act lays down provisions on information security management and refers, inter alia, to paragraph 2.4.3 of the EU Electronic Identification Assurance Level Regulation. Section 2.4.3 of Annex 1 of the EU's Electronic Identification Assurance Level Regulation provides that *the information security management system adheres to proven standards or principles for the management and control of information security risks.*

Provision 4.1 specifies the requirement in the Identification and Trust Services Act and the EU Electronic Identification Assurance Level Regulation. An example of a well-known and valid information security management standard is standard ISO/IEC 27001 [11]. Other standards or a combination of standards may also be used, provided that the standard indeed applies to information security management. The standard may be international, such as ISO, but also a national one, such as KATAKRI [12].

The wording of the provision will be changed to say that the selected information security management standard(s) must be complied with, not only applied. This makes the requirement slightly more restrictive. The purpose of this is to highlight the significance of the commitment of the identification service provider management and the significance of the maintenance of the information security management system and processes.

Certification is not made compelling even on the high assurance level, but the implementation and efficiency of information security management is assessed strictly throughout the high assurance level. Information security management must be comprehensive, consistent and active without exceptions.

4.4.2 Provision 4.2 Scope of information security management

Provision 4.2 lists the operational areas that the information security management shall cover. The specification of the requirements is partly based on the upper level grouping of requirements in standard ISO/IEC 27001.

The provision has not been amended. The requirements largely correspond to section 8(2) on information security management in the regulation valid prior to 2016.

Information security management must be comprehensive, consistent, organised, systematic and continually monitored. The provision specifies the minimum factors that must be observed in the management system.

The information security management of subcontractors must also meet these requirements. They can be proportioned to the criticality of the subcontracted operation within the identification scheme.

See section 15 of the Regulation and its explanation for conformity assessment of information security management.

The following is a description of the content of the subsections and assessment of their link to sections of the ISO/IEC 27001 standard [11]. This table has been supplemented compared to the explanations from 2016.

Regulation section 4.2 and its application	**ISO/IEC 27001**
1) *the overall context of the identification service provider* - The information security management system covers the key internal and external technical, legal and administrative requirements and needs affecting the identification scheme. - The identification service must e.g. comply with valid legislation and regulations, such as the Identification and Trust Services Act, Regulation 72 and the GDPR.	4 context of the organisation
2) *governance, organisation and maintenance of information security management* - The information security management system covers administration management, organisation and maintenance, which shall be documented in an information security policy or similar instructional documents. - An up-to-date information security policy or similar instructional documents approved by management are employed. The security principles and policies must be comprehensive and appropriate for the organisation and for the protected objects. - Responsibilities connected to staff and subcontractor information security have been described.	5 leadership 9.2 internal audit 9.3 management review 10 improvement A.5.1.1 Information security policies A.6.1.1 Information security roles and responsibilities A.15.1.1 Supplier relationship information security policy
3) *management of information security risks related to the provision of the identification service*; - The information security management system covers the management of information security risks connected to the provision of an identification service. - Risk management is a regular, continuous and documented process. - Identified risks are classified and prioritised.	6 planning

- The risk management process identifies risks related to data confidentiality, integrity and availability. - The risk management process and its results are utilised in designing the security measures of the identification service/scheme. - Cf. the application guideline for the eIDAS Assurance Level Regulation: *A general principle in risk management is that it is up to the organisation to choose which level of risk it finds acceptable. This general principle is modified by the requirement in 2.4, since the organisation should have controls that are commensurate to the risks at the given level.* - Provision 6.1 of the Regulation specifies more detailed requirements for assessing the risks of an identification means.	
4) *resources allocated to information security, competences, staff awareness of information security, communication, documentation and the management of documented information;* - The information security management system covers information security resourcing, qualification requirements, staff awareness of information security, communications and documentation as well as the management of documented data. - All those who participate in electronic identification tasks are aware of current information security instructions and practices and these have been made available. - Staff security training is regular and documented. The efficiency of the training is monitored. - Familiarisation with verifying the authenticity of passports and identity cards in the initial identification of identification means applicants or familiarisation with the information security practices of the remote control of the identification scheme systems are typical examples of identification means provider staff qualification requirement management.	7 support functions
5) *planning and control of the provision of the identification service for the purpose of meeting information security requirements* - The information security management system ensures that the identification service offering is de-	8 operation A.18.1.1 conformity/compliance with requirements in legislation and agreements: itemisation of

signed and provided in such a way that the information security requirements set for the identification service are met. - Identification service requirements (Identification Act, EU's Electronic Identification Assurance Level Regulation and Agency Regulation 72) have been taken into account in the management system	the applicable legal and contractual requirements
6) *evaluation of the efficiency and effectiveness of information security management* - The information security management system covers the regular assessment of the efficiency and functionality of information security management. - - i.e. how effective and efficient information security management is on the factors, processes and problems affecting the information security of the identification scheme.	9.1 monitoring, measurement, analysis and evaluation

4.4.3 Risk management model and process

Risk management required by provision 4.2 3) must cover the risks of the entire identification scheme. This also applies to risks related to identification means granted within the scheme. Provision 6.1 specifies the special requirements concerning the threat and risk assessment of the identification means and the minimum set of issues to be considered in the assessment.

The regulation does not address the risk management model used or the standard applied. The same standard or operating model selected by the identification service provider can be applied to the threat and risk assessment of the entire identification scheme and especially the identification means specified in provision 6.

Relevant standards may be utilised in risk assessment. The regulation does not stipulate any compulsory standards or any standards that must be used as comparisons. E.g. the following standards and instructions may be utilised in risk management:

- SFS-ISO 31000:2018 [13]
- ISO/TR 31004, Risk management – Guidance for the implementation of ISO 31000, and International Standard/ISO/TR 31004:fi [14]
- SFS-EN IEC 31010:2019, ISO/IEC 31010, Risk management – Risk assessment techniques, developed jointly with the International Electrotechnical Commission/ [15]
- ISO 27005 [16] https://en.wikipedia.org/wiki/ISO/IEC_27005
- VAHTI Ohje riskienhallintaan (VAHTI Risk management guideline), Ministry of Finance publications 22/2017 [17] https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/80013/VM_22_2017.pdf?sequence=1&isAllowed=y

- NIST Risk Management Framework (RMF) [18] https://csrc.nist.gov/projects/risk-management/about-rmf

- Standards, such as the following, may be used especially in the assessment of the implementation of identification means or encryption practices: FIPS 140-3 Security Requirements for Cryptographic Modules [19] https://csrc.nist.gov/publications/detail/fips/140/3/final

The following may also be considered a risk management checklist, source: KATAKRI 2020 [12], T-03:

1) *The management of information security risks is part of the organisation's operation and management of other risks.*

2) *The management of information security risks ensures that sufficient information security measures to protect Classified Information are in place.*

3) *The procedure for assessing and analysing information security risks produces appropriate and understandable information for the decision-making.*

4) *Information security risks are managed by a sufficient amount of specialised personnel.*

5) *The management of information security risks takes care of risks deriving from other organisations and supply chains. Cf. risks concerning supply chains for security critical devices and software (requirements I-01, I-12 and I-13).*

6) *The results of the assessment and analysis of information security risks are used in the planning and in the implementation of the protection of Classified Information, in the assessment of the impact of security incidents, in the change management and, when possible, in procurement.*

7) *Information security measures are scaled based on risks and taking into account e.g. the classification level, quantity, format, classification justification and storage of the information with relation to the assessed risks.*

8) *The organisation has documented the relevant parts of the monitoring and security measures, as well as the risk assessment, which these measures are based on.*

The risk management process should cover the processes described in the ISO31000 standard, which take the following into account (e.g. SFS-ISO 31000:2018, page 14) [13]

1) *Scope, operating environment and criteria*
2) *Risk assessment*
   - *Risk identification*
   - *Risk analysis*
   - *Risk significance assessment*
3) *Risk processing*
4) *Communication and information exchange*
5) *Records and reporting*
6) *Monitoring and reviews*

4.4.4 Provision 4.1, alternative regulation considered

The standards that could be referred to were discussed in 2016. ISO 27001 was deemed the only standard comprehensive enough at the time. Assessments have shown that, in practice, information security management relies in part on at least financial sector standards (such as PCI standards, PCI DSS [20]).

In the Agency's assessment, there continue to be no relevant, comprehensive alternatives to ISO 27001. It is not the only option, but it would seem to be the only widely applied standard across disciplines/branches targeting information security management specifically.

The feedback to the regulation amendment needs questionnaire suggested that the wording of the regulation be made more restrictive or specific so that the standard should be complied with or that operators should be certified. The Finnish Transport and Communications Agency assesses that a compelling requirement to certify would be financially taxing and would be a poor option in situations where information security management is based on several standards.

4.5 Provision 5 Information security requirements of an identification scheme

4.5.1 General

Provision 5 specifies the measures required for the implementation of information security throughout the identification scheme.

General provisions on the requirements are laid down in section 8(1)(4) of the Identification and Trust Services Act, which refers to paragraphs 2.2.1, 2.3.1 and 2.4.6 of the EU Electronic Identification Assurance Level Regulation [4].

Identification services of different sizes and newcomers. The requirements for identification schemes and means apply to identification service providers, or identification means providers, and where applicable also to identification broker services, of all sizes with different resources. The purpose of the requirements within the regulation is to improve security, but also to improve the predictability of regulation to ease the operation of identification services. According to an estimate by the Agency, clear-cut requirements also foster mutual trust in the information security of current and future identification services in the trust network.

Resistance to information security threats. According to section 2.3.1 of the Electronic Identification Assurance Level Regulation

> *The authentication mechanism implements security controls for the verification of the electronic identification means, so that it is highly unlikely that activities such as guessing, eavesdropping, replay or manipulation of communication by an attacker with moderate attack potential can subvert the authentication mechanisms.*

On the high assurance level, the security measures must be scaled according to a high attack potential.

According to section 2.4.6 of the Electronic Identification Assurance Level Regulation

> *1. The existence of proportionate technical controls to manage the risks posed to the security of the services, protecting the confidentiality, integrity and availability of the information processed.*

Section 2.4.6 of the Electronic Identification Assurance Level Regulation also provides for measures for the protection of electronic communication channels against eavesdropping, manipulation and replay; the protection of cryptographic material; the ability to respond to changes in risk levels, incidents and security breaches; and the security of media.

Information system, communications and operational security. Provisions 5.2–5.4 specify the communications, information system and operational security in order to ensure that the information security required by regulation is implemented. The specifications are based on the generally applied classification of information system security into information system, communications and operational security. These areas are not mutually exclusive; instead, they represent different viewpoints to the same identification scheme entity.

Separation as an information security measure. Separation of personnel duties, separation of physical workspaces and tools, or the potential separation of technical service environment and server environments from other production are part of normal good practices. Sufficient separation is assumed to be executed through normal information security management, design and auditing, and the matter is not regulated separately with the exception of the requirement in provision 5.5.

Impact. The requirements in provision 5 will not change, but they will be clarified. The provision has been specified and examples of applying the provision have been added to the explanation based on experience from conformity assessment and supervision of identification services.

The amendments are effective in improving the security of identification schemes. The requirements are not dependant on technology, meaning that they do not have any impact on developing the features of identification services.

Other instruments for steering

Guideline. Assessment guideline 211/2019 specifies the requirements concerning information security assessment.

Recommendation. Regulation amendment needs questionnaire respondents hoped that the Agency would offer a testing service. However, the Agency has not been tasked with operational tasks in electronic identification supervision, such as testing service acquisition or maintenance. Drafting a testing recommendation for testing services offered by the identification services themselves could be carried out in the trust network.

Co-regulation. The level of information security has been specified in regulation and supervision. Strong electronic identification service providers have the opportunity to exchange information on security threats and measures without breaching any confidentiality provisions.

Information steering. No notes.

4.5.2 Identification scheme entity (architecture and subcontractors)

The identification scheme (or eID scheme) refers to a system in which the electronic identification means are granted and maintained for users. An identification scheme covers the technical systems, information security control and other reliability requirements of the identification service provider. An identification scheme also co-

vers all subcontracted sections and functionalities of the system concerning the production of the identification service. The term used in the Identification Act is *electronic identification scheme*.

The following are examples of components of an electronic identification scheme:
- data centres and other premises
- servers and software related to the identification event
- system components related to identification
- connections, gateways and links between different parts of the identification scheme, incl. administration connections
- connection protection procedures, interfaces between system sections and other factors – incl. security controls of connections to external operators
- network information security components, such as firewalls
- information resources

Subcontractors. The regulation does not provide separate provisions for subcontractors. In accordance with section 13 of the Identification and Trust Services Act, the identification service provider must ensure that the services it subcontracts meet the requirements. In the implementation of identification schemes and identification means subcontracting is typical. In terms of assessing conformity, subcontracting is discussed in the identification service assessment guideline 211/2019 issued by the Finnish Transport and Communications Agency [21].

If the identification scheme utilises productised cloud service components or products (e.g. Amazon Web Services, Google, Microsoft Azure), the identification scheme requirements also apply to these components and they must be included in the scope of conformity assessment. Only components that meet the requirements and whose conformity can be ensured may be used in the identification scheme.

4.5.3 Provision 5.1.1 The resistance of the identification scheme

Provision 5.1.1 is new to this version of the regulation. It specifies the required level of the whole of the security measures and technical specifications of the identification scheme.

As a rule, the individual requirements pertaining to substantial and high assurance levels are not specified separately in the regulation. Instead, the assurance level of the security measures, i.e. technical controls, required in section 2.4.6 of the Electronic Identification Assurance Level Regulation are specified based on the ability to provide protection against potential attacks specified in section 2.3.1 of the same regulation. The requirement applies to the resistance of the entire identification scheme, and thus also the communications, information system and operational security factors specified in provisions 5.2–5.4.

No detailed criteria or standard to abide by will be stipulated for the threat and risk assessment. The material assessment must be based on an excellent command of the field and monitoring of the threats, vulnerabilities and technical developments.

See LOA Guidance [22], section 2.3.1

> *The Level of Assurance uses the terms "enhanced-basic", "moderate" and "high" to denote the different attack potentials. These terms were adopted from standards ISO/IEC 15408 "Information technology – Security techniques – Evaluation criteria for IT security" [23] and ISO/IEC 18045 "Information technology – Security techniques – Methodology for IT security evaluation" [24]. The standards are publicly available at www.commoncriteriaportal.org/cc*

(CCPART1-3 corresponds to standard ISO/IEC 15408 and CEM to standard ISO/IEC 18045).

In standard ISO/IEC 15408-1, attack potential is defined as a measure of the effort to be expended in attacking a target of evaluation, expressed in terms of an attacker's expertise, resources and motivation.

Annex B.4 to standard ISO/IEC 18045 / CEM provides instructions on how to calculate attack potential requiring the abuse of a certain vulnerability in the authentication mechanism.

In order to meet the requirements set out in the implementing regulation, some assessments of resistance against potential attacks should be carried out.

The appropriate threats should be considered in the evaluation. Standard ISO 29115 [25] mentions the following, for example: guessing online and offline, replication of identification data, phishing, eavesdropping, replay attacks, session hijacking, man in the middle attacks, stealing identification data, spoofing attacks and impersonation.

4.5.4 Provision 5.1.2 Relationship between the encryption requirements in provision 5 and 7

Sections of provision 5.1.2 are partly new to this version of the regulation. The previous regulation stipulated that *information system security* must use internationally or nationally recommended encryption solutions *with the exception of stipulations in section 7.* The requirement to use internationally or nationally recommended encryption solutions has been added to the section concerning communications and operation security and the relationship to the encryption solutions in provision 7 is defined in terms of all of the requirements in provision 5 in provision 5.1.2.

Section 7 of the Regulation stipulates special encryption or protection requirements for certain communications connections and messages. The requirement in section 5 of the Regulation applies to other connections and elements in general, meaning identification scheme internal elements, stored data and connections to subcontractor systems. The requirement also covers provision 5.2. on communications, provision 5.3 on information systems and provision 5.4 on operating. Here too it is recommended that technically applicable solutions defined in provision 7 be applied, but protection may also be implemented using other security measures.

4.5.5 Provision 5.2 Communications security

Provision 5.2 corresponds to the previous wording of the Regulation in section 5.1(1) to a great degree. The provision has been specified.

In addition to requirements stipulated in provision 5.2, provision 14 stipulates on the communications protocol and provisions 7–9 address the protection of communications and messages between identification services and between identification services and the e-services that rely on them. The security of the connection between the user and provider of the identification means is part of the authentication mechanism requirements in provision 6.

5.2.a) structural network security

The network's structural security is in place to ensure that *electronic communication channels used to exchange personal or sensitive information are protected against eavesdropping, manipulation and replay.*

The structure of the network must be documented. The hardware and systems of the identification scheme must be identified and documented. Structural security applies to the communications connection between the different parts of the identification scheme and their protection practices. It applies to network areas on different security levels, as well as the filtering and monitoring systems operating between them. The structural security requirement also covers all relevant communications connections with subcontractors (infrastructure, software, operational services, card factory, etc.).

5.2.b) zoning of the communications network

The requirement aims at reducing risks to network integrity, confidentiality and usability through communications connections.

An example of zoning is when the production network, maintenance and administration network and other office networks are separated from each other. A development environment separated from production must also be employed.

5.2.c) filtering rules according to the principle of least privilege

The principle of least privilege means that all connections that are not necessary for the operation must be denied or disabled. The connections between the production network and the public network must be based on risk and only allow for service functionalities.

5.2 d) administration of filtering and control systems

No application examples.

5.2.e) secure administration connections

The specification 'secure' has been added to the provision.

Administration connections can be both internal and external telecommunication of an organisation. The data processing environment used for administration must be separated from other environments.

See also section 5.5 of the Regulation.

5.2.f) *employing internationally or nationally recommended encryption solutions*

See section 4.7.5 of these explanatory notes for sources of recommended encryption solutions.

4.5.6 Provision 5.3 Information system security

Provision 5.3 corresponds to the previous wording of the Regulation in section 5.1(2) to a great degree. The provision has been specified.

5.3.a) access control according to the principle of least privilege

The specification 'according to the principle of least privilege' has been added to the provision.

The principle of least privilege means that access rights are only granted based on information system categorisation and the user's tasks. Access control must be used

to restrict access to data and data processing environments systematically, and this must be documented. Unnecessary access rights must be removed regularly.

Administrator rights must be determined especially carefully and the integrity of system and event logs must be ensured.

System separation, ensuring log stability and other appropriate measures must be used in determining administrator rights.

5.3.b) unique identification of the users of the systems

The specification 'unique' has been added to the provision. User IDs must be personal and they may not be in shared use.

Identification ensures that only the right users have access to systems and that all events can be traced.

It must be possible to identify users of identification scheme information systems using a known method that is considered secure. Primarily, identification based on several factors (*2FA i.e. 2-factor-authentication, MFA i.e. multi-factor-authentication*) should be used. If a user ID and password are assessed as a whole a sufficient combination in places based on other security measures, the passwords must be strong enough.

5.3.c) hardening of the systems

Hardening of the systems means only using the services, functions, processes, devices and components necessary for the operation of the identification scheme.

Their use must be determined in such a way that the installation is stripped of all unnecessary rights and functionalities. A hardened installation only includes components and services, as well as user and process rights, that are necessary to fulfil functional requirements and ensure security.

5.3.d) malware protection

The identification scheme must be able to detect, pre-empt, prevent and repair damage and threats posed by malware.

5.3.e) ability to trace security events and tracing procedure

The specifications 'ability to trace' and 'tracing procedure' have been added to the provision.

This means that the Regulation requires that a predetermined procedure to trace and repair any security events is in place.

The logging described in the following section is part of the ability to trace events.

The ability to trace requires that the identification scheme time is maintained reliably. The time is required for showing event times reliably. The reliability of the time means that the time must be retrieved from a reliable source and a sufficiently low tolerance for errors. The recommended error tolerance is 0.5 seconds.

5.3.f) *ability to detect security incidents and repair procedure*

The expression 'recovery' has been replaced with 'repair procedure' in the provision.

The regulation requires that the identification scheme has the ability and predetermined processes for detecting security incidents.

The configuration must take into account the criticality and classification of the components and processes of the communications connections and information systems of the scheme and the fact that events affecting security can also be traced retroactively.

The ability to detect requires that the identification scheme collects and records event logs on the operation of the scheme and any events and security incidents affecting information security. The detection of security incidents and information security violations requires that the operation of, changes to and event logs of the identification scheme are monitored.

The integrity of the logs must be ensured by e.g. exercising access and user right control, protecting environments and removing log data from the target system, if necessary. The separation of personnel duties is necessary at least to the extent that the same person must not be able to create the identification means and manage the log data related to the creation and introduction of the identification means.

The repair process means that all security incidents and disruptions in the identification scheme are processed and analysed, their severity is rated in accordance with systematically determined methods and any security incidents are repaired in the manner required by the severity rating.

5.3.g) *employing internationally or nationally recommended encryption solutions*

See section 4.7.5 of these explanatory notes for sources of recommended encryption solutions.

4.5.7 Provision 5.4 Safety of operation

5.4.a) careful change management

The word 'careful' has been added to the regulation.

The purpose of the requirement is to prevent any fault situations caused by changes to the identification scheme in terms of information security and usability. Changes often need to be made quickly and they can affect many parts of the scheme. That is why their careful planning, process standardisation and reserving sufficient time for changes is necessary. Reviews and testing are part of a reliable change process. Both processes and changes made should be documented to be able to trace the root causes of any errors. Appropriate documentation involves storing data on changes made to the identification scheme in the control logs of the identification scheme, separating the logs from other logs and ensuring their integrity.

5.4.b) *confidential data processing environment and storage based on data classification*

'Based on data classification' and 'storage' were added to the provision.

The protection of stored data has been moved from section 7(4) of the Regulation. It read: *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 concerning signatures, symmetrical encryption and hash functions shall apply.*

The basic requirement for processing data is the classification of data and material, based on which information systems and the functions they enable can be classified. The entire lifecycle of protected data should be considered in system classification.

The classification should take e.g. trade secrets, security arrangements and logs into account. Personal data and cryptographic secrets related to granting identification means should also be observed.

The security measures related to data processing and storing must be scaled to the data classification grounds, amount, form and storage location in relation to the threat posed to the data. Security measures, such as access control and encryption, must be used to secure the integrity and confidence status of stored data. Keys used for encryption or signatures and root certificate signature keys are examples of data that needs to be protected very carefully.

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

The words 'protecting' and 'from threats in the remote use environment' were added to the provision.

No application examples provided here. See section 5.5 of the Regulation.

5.4.d) *software development and software vulnerability management*

The specification 'software development' has been added to the provision.

The Regulation requires that the identification service has a method in place for monitoring typical vulnerabilities, which must cover the software affecting the security of the identification scheme.

The software used in the identification scheme must comply with secure programming principles. It must also take the security of the development environment into account.

The requirement concerning software security covers identification apps and software libraries, for example.

Vulnerability management means the monitoring of vulnerabilities in software and encryption algorithms and methods and monitoring bulletins as well as the automatic and regular inspection of the software used in the systems both in the external and internal network.

Cf. PiTuKri section KT-04 Vulnerability management, [26] Traficom publication 13/2020 Criteria to Assess the Information Security of Cloud Services (PiTuKri)https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/PiTuKri_v1_1_english.pdf

> *Reliable arrangements must be established for the entire lifecycle of the cloud service to manage software vulnerabilities.*
>
> *In particular:*
>
> *a) Security bulletins of the authorities, equipment manufacturers, software suppliers and other similar parties are followed and security updates deemed necessary based on a risk assessment are installed in a controlled manner (cf. MH-01).*

b) The systems are automatically checked for known vulnerabilities at least once a month. If the planned settings or the security update level are departed from, the reasons are analysed and any exceptions are corrected or documented in accordance with the security exception management process (see TJ-04).

Vulnerable algorithms and encryption methods. The key stakeholder consultation concerning section 7 of the Regulation highlighted the issue of how any future vulnerabilities in the algorithms and methods deemed qualified in the Regulation and the resulting need to stop using them affects the application of section 7.

According to section 5.4 d), the identification service has the opportunity and obligation to manage vulnerabilities. An appropriate way to observe vulnerabilities is to monitor the information channels concerning them and independently stop using vulnerable methods.

It is the Agency's understanding that encryption algorithms and methods do not become vulnerable suddenly; instead, these developments typically take years or decades. This allows for amending the Regulation when necessary, but if there was insufficient time to make any changes in surprising situations, the Agency could provide guidance on reacting to vulnerabilities.

5.4.e) *backup procedures*

The purpose of making backup copies is to ensure the retrieval of data and systems after disruptions and data tracing, when necessary.

Backup copies must be made systematically while observing data classification and lifecycles. Storage must take the separation of the physical storage space from the actual system into account.

5.4.f) *employing internationally or nationally recommended encryption solutions*

See section 4.7.5 of these explanatory notes for sources of recommended encryption solutions.

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

The requirements for remotely administered terminal devices and remote connections are specified on a substantial and high assurance level in provision 5.5. The provision corresponds to section 5(2) of the previous regulation.

The implementation and controls of the system must be proportioned to a moderate or high level of attack potential.

Staff terminals with which administration systems can be accessed may easily become information security risks, unless particular attention is paid to the issue.

On the substantial assurance level, the separation of terminal devices is not a requirement, but on the high assurance level, either a dedicated terminal device, virtualised termination or a solution based on the KVM principle (remote desktop) is a requirement.

The internet and the office network are considered non-trusted networks unless the office network falls within the scope of conformity assessment.

Requirements associated with the *substantial level of assurance* are usual and they are already covered by the requirements of ISO 27001, for instance, if the standard is applied. The data transfer channel shall be protected in remote use and the risks caused by the office network shall be taken into consideration.

At the *high level of assurance*, the requirements may be met at least by disabling access of a workstation in remote use to other services of the organisation, such as e-mail, and preventing the workstation from using other functions than those essential to the operation of the administration network. In practice, this means that there shall be a separate workstation for administration.

The *assessment as a whole* required at the high level of assurance means that if other workstations than such hardened workstations described above are used, the separation of the production system and other means for managing information security threats are taken into account in the implementation. In principle, such a case requires a virtual termination or a KVM solution.

The key point here is what is done on the terminal taking the virtualised connection, and therefore a two-factor VPN connection to a virtualised workstation alone is not a sufficient solution, for example. Using antivirus and web proxy is not sufficient, either.

When transferring necessary files from one terminal to another, the risk of malware shall also be taken into account, for instance, by ensuring the use of reliable sources only and safeguarding information security (integrity) using all appropriate methods.

4.5.9 Provision 5, alternative regulation considered

4.5.9.1 High assurance level requirements

In the Regulation amendment needs questionnaire, some respondents hoped that the technical requirements for substantial and high assurance levels were specified in more detail in the Regulation. However, no proposals of requirements that should specifically be specified were received.

In the Agency's opinion, specifying assurance level requirements in regulation is not possible, because the identification scheme contains numerous partial factors. Providing detailed specifications would not be practical, because technical implementations and threats keep changing.

Instead, the Regulation clarifies and specifies the scaling of all security measures to attack potential in accordance with the assurance level.

4.5.9.2 Separation requirements as information security measures

No grounds or need to stipulate new separation requirements were found in the 2021 drafting process.

Separation as an information security measure. While the regulation was being prepared in 2016, it was assessed whether one of the following was required due to information security requirements: separation of personnel duties, separation of physical workspaces and tools or the potential separation of technical service environment and server environments from other production.

At that time, the impact assessment concluded that the details of separation were to be implemented through general information security management, planning and audits. In the 2016 impact assessment, it was concluded that the separation of personnel duties is necessary at least to the extent that the same person must not be

able to create the identification means and manage the log data related to the creation and introduction of the identification means. It was expected that this was already covered by normal information security management, planning and auditing, and no separate regulations needed to be issued.

The specification of security requirements for terminals used in management networks and office networks raised so many questions during the drafting phase in 2016 that the requirements were clarified in subsection 2 of section 5 of the regulation as well as with the implementation guidelines in the explanatory notes. These are retained as they are in the Regulation and the explanatory notes.

4.5.10 Reliability of the identification scheme time

The explanatory notes for Regulation 72 contained a recommendation on the reliability of the identification scheme time (explanatory notes to regulation 2016/2018 section C, subsection 1).

The removal of the recommendation concerning the identification scheme time source and time error tolerance was discussed during the drafting process of the Regulation, because its application has not been addressed in identification service guidance work and supervision or stakeholder comments.

The identification scheme time is, however, part of general good maintenance of communications and information systems, and the matter will remain in the explanation, but it will be moved to the section concerning identification scheme information system security.

Recommendation MPS72 (identical on 2 November 20216 and 14 May 2018) section C, subsection 1

It is recommended that an identification service provider acquire a trusted time source with which the time applied in the identification scheme may be synchronised. The time is required for showing event times reliably. The recommended error tolerance is 0.5 seconds. Synchronisation between various parties does not seem necessary.

Recommendation ITU-R TF.1876 (03/2010) Trusted time source for time stamp authority [27] is related to this topic.

Possible time sources include NTP or PTP (with availability guarantee) by VTT Technical Research Centre of Finland/MIKES. There are also other options available.

4.6 Provision 6 Information security requirements of an identification means

4.6.1 Provision 6.1 Identification means characteristics and resistance

4.6.1.1 Provision 6.1.1 Itemised risk assessment

This provision is new to this version of the regulation.

Regulation 6.1.1 specifies the security requirements concerning the entity consisting of the identification means authentication factors and the authentication mechanism. Requirements concerning the specific risk assessment and the factors observed within it are added to the Regulation. The threats to the authentication factors and the authentication mechanism must be evaluated separately. The identification means, i.e. the authentication factors and security measures used within it, must be planned so that the entity provides protection against estimated threats.

In the Agency's assessment, this model is flexible enough in terms of various identification means and authentication factors and observes the identification means security controls as a whole. Any supervisory solutions defined by the Agency would be based on an accurate risk assessment of the identification service, which would also take the effect of security controls into account.

Based on stakeholder comments received during the preparatory phase, a risk-based approach is functional, but requires instructions on what to assess and how, to make the acceptability of the residual risk as foreseeable as possible. The selected regulation model specifies the requirement of conducting a risk assessment and the components that must be observed in it. Application will be addressed in the following sections.

Transition period. Based on stakeholder comments, the Agency is of the opinion that the requirement does not require a transition period, but the obligation to draft the assessment can enter into force simultaneously with the entry into force of the amended regulation.

Impact. In the Agency's assessment, the requirement concerning the conducting of the risk assessment is a natural part of producing an IT service such as an identification service and falls under the statutory requirement to manage information security. The specific requirement laid down in the regulation may specify the requirements concerning the assessment and add documentation obligations. In the Agency's assessment, the requirement will promote the secure development of identification means and offer a reasonable basis for any Agency supervisory measures.

Alternative methods of regulation. As an alternative to section 6.1.1, the Agency has assessed regulation models in which authentication factor specific requirements or the requirements concerning the resistance of the identification means would be specified in the regulation. Due to the diversity and development of authentication factors, the authentication factor specific regulation model would involve details that cannot be covered on a regulatory level, or doing so would not be practical, according to an evaluation by the Agency. Furthermore, threats to identification means security and security measures as protection against threats are not purely authentication factor specific. Resistance indicators or other specifications could possibly be included in the regulation.

Other steering instruments.

The identification service assessment guideline will take the amended requirements into account.

In terms of *co-regulation,* the Agency is of the opinion that shared information security threats can be discussed in information exchange within the cooperation group of the trust network based on section 16 of the Identification Act. Section 12 a of the Identification Act stipulates that members of the trust network may only use data on another identification service for the purpose for which they were disclosed to the identification service provider.

Recommendation or informative guidance. No notes.

Supervision. The risk assessment of the identification scheme and the identification means as part of it is an existing requirement, meaning that there is no need for a transition period. The risk assessment or the related documentation may, however, not have been drafted as precisely as required in the regulation. The Agency shall

assess separately whether the conducting of the assessment and its results are supervised at the time of the regulation entering into force by way of a monitoring survey during 2022, for example, or only as part of scheduled conformity assessments, i.e. in the 2023 biannual conformity assessment, which would mean that supervision would in practice be conducted in 2024. Regardless, the special assessment requirement pertains to changes to identification means notified to the agency after the regulation has entered into force. It can also be supervised case-specifically in the event of a disruption.

4.6.1.2 Threats to be observed in the risk assessment

The threats to be taken into account in the threat evaluation are based on expertise in the field, information accumulated during maintenance of an identification service, confidential information received in the trust network cooperation group and publicly available information on information security threats and vulnerabilities.

LOA Guidance [22], section 2.3.1:

> *The appropriate threats should be considered in the evaluation. Standard ISO 29115 mentions the following, for example: guessing online and offline, replication of identification data, phishing, eavesdropping, replay attacks, session hijacking, man in the middle attacks, stealing identification data, spoofing attacks and impersonation.*

Depending on the individual characteristics of the identification means, at least the following threats and their combinations mentioned in the ISO 29115 standard and NIST 800-63B Digital Identity Guidelines on Authentication and Lifecycle Management (https://pages.nist.gov/800-63-3/sp800-63b.html) should be taken into account in the threat evaluation, for example:

ISO 29115 Information technology — Security techniques — Entity authentication assurance framework [25]

- Online guessing
- Offline guessing
- Credential duplication
- Phishing
- Eavesdropping
- Replay attack
- Session hijacking
- Man-in-the-middle
- Credential theft
- Spoofing
- Masquerading

NIST 800-63B Digital Identity Guidelines, Authentication and Lifecycle Management [28]

- Assertion Manufacture or Modification/assertion
- Theft
- Duplication
- Eavesdropping
- Offline Cracking
- Side Channel Attack
- Phishing or Pharming
- Social Engineering
- Online Guessing
- Endpoint Compromise
- Unauthorised binding

4.6.1.3 Typical threats to authentication factors

Below are some examples of authentication type specific threats. The list is not exhaustive, but contains examples of threats.

Authentication factor based on possession. LOA Guidance [22], section 1. (2)(a):

> *Typical attacks on possession-based authentication factors are theft, duplication or tampering (manipulation), as well as attacks on the proof-of-possession during authentication.*

Printed online banking code list. Duplication, phishing, theft, target service masquerading

SMS OTP. Malware on the terminal device, SIM card replacement, insufficient protection of SMS gateways, phone lock bypass (SMS displayed on the locked phone screen), phishing/fraudulent websites, target service masquerading

OTP code device. Side channel attack, theft, phishing/fraudulent websites.

Identification app. Malware on the terminal device, theft and spying of knowledge-based factors (e.g. over the shoulder) or a poor biometric sensor, session hijacking, target service masquerading, identification app activation/unauthorised activation through phishing

Authentication factor based on knowledge. LOA Guidance, section 1. (2)(b):

> *Typical attacks on knowledge-based authentication factors are guessing, phishing, eavesdropping or duplication. A characteristic of knowledge-based factors is that attacks are not necessarily noticed by the subject of the electronic identification means. For example: brute force/dictionary attacks on a password with low entropy and without retry counter or a password that has been copied from a letter or e-mail without knowledge of the owner or the verifier.*

Password/pass phrase. Guessing, investigation, theft, phishing/fraudulent websites.

PIN code. Guessing, investigation, theft, phishing/fraudulent websites.

Factors likely to be known only by the owner of the factor (questions and answers). Guessing, investigation, theft, phishing/fraudulent websites.

Inherent authentication factor. LOA guidance, section 1.(2)(c):

> *Inherent authentication factors should have a variance even between people of similar characteristics so that a person may be uniquely identified: examples include fingerprints, palm prints, palm veins, face, hand geometry, iris, etc. A key consideration when a biometric factor is being used is to ensure that the person to whom it relates is physically present at the point of verification. This is to mitigate against spoofing or duplication.*

Fingerprint. A low FAR (False Acceptance Rate) due to its technical implementation, copying (from surfaces, photographs), malware, whether the user is unaware.

Face. A low FAR (False Acceptance Rate) due to its technical implementation, presentation attacks.

Factors based on continuous measurement. No notes.

4.6.1.4 Authentication mechanism

Authentication mechanism means the technical measures used to authenticate that the user is in possession of the authentication factors, has the relevant knowledge or has the inherent authentication factors of the identification means connected to them. Regulation requires dynamic authentication for strong electronic identification, i.e. that each identification event must be unique, and may not be replayed.

As shown in the examples below, the threats to authentication cannot be accurately separated from threats connected to authentication factors. In the Agency's estimate and in light of the Guideline for Assurance Level Regulation (LOA Guidance), the specific threats to authentication are at least connected to communications.

LOA Guidance [22], section 1.(3):

> *The primary purpose of dynamic authentication is to mitigate against attacks such as 'man-in-the-middle' or misusing verification data from a previously recorded authentication replay to the verifier. This includes:*
>
> - *replay attacks, i.e. intercepting verification data and reusing them in a different authentication context*
> - *certain types of session hijacking, e.g. exchanging (parts of) the authentication contexts of two or more simultaneously occurring authentications.*
>
> *It is important to understand that multi-factor and dynamic authentication are not the same; multi-factor authentication does not require that the authentication is dynamic (e.g. PIN and fingerprint) and can therefore be more exposed to replay attack than a dynamic authentication.*
>
> *Dynamic authentication might be implemented by the authentication factor (e.g. a one-time key from a device) or by the authentication mechanism (e.g. dynamic challenge in a challenge-response authentication).*
>
> *Examples of dynamic authentications are:*
>
> - *possession of a private key stored on a smart card and verified using a challenge-response-protocol*
> - *protocols based on an ephemeral Diffie-Hellman and providing authentication (e.g. PACE), cryptographic nonces, timestamps and/or non-repeating sequence numbers*
> - *protocols based on a static-ephemeral Diffie-Hellman, if the ephemeral key is provided by the relying party (e.g. EAC)*
> - *dynamically generated one-time access codes (e.g. OTP tokens) or challenge response protocols where the one-time code has been previously generated and distributed out of band but selected dynamically during authentication (e.g. OTP cards).*
>
> *If the subject's private key is stored remotely (centrally stored, e.g. in an HSM operated by the identity provider), the authentication used to access the private key should also be dynamic.*

LOA Guidance, section 2.3.1:

During assessing attack resistance, the whole authentication mechanism should be taken into account including the risks resulting from verification of the possession of the electronic identification means.

Examples:

- *For LoA high, it is not sufficient that a smart card protects a cryptographic key against manipulation with high attack potential; the cryptographic protocol should also protect the verification of the possession of the key against manipulation/replay against high attack potential.*

- *For a one-time-password token, where the generated one-time-password is transmitted via a secure channel (e.g. TLS), the strength of the possession-based factor is limited not only by the strength of the token, but also by the strength of the secure channel.*

- *The mechanism for proof-of-possession of a time-based one-time-password generator is the submission of a generated one-time-password to the verifier. The strength of this mechanism is limited, among others, by the length of the one-time-password, the time-window for validity of the password, and the confidentiality of the transmission.*

4.6.1.5 Security measures

Authentication factor based on possession. LOA guidance [22], section 1.(2)(a):

The relevant security characteristic of a possession-based authentication factor (e.g. token) is the sole control of it by the owner. This implies that it is important that reproduction of it by a third party is so difficult and unlikely that the risk of this is negligible. The Level of Assurance depends on the level of resistance against reproduction.

For example: asymmetric cryptographic (private) keys, the private keys may be stored on dedicated hardware devices (e.g. smart cards), or software tokens; uniquely identifiable tokens (e.g. the SIM card of a cell phone) or devices with one-time-passwords (e.g. "RSA Token" or printed cards).

Printed online banking code list. User instruction

SMS OTP. Out of reach of the identification service; securing the SMS gateway, SIM card/eSIM replacement process. User instruction, displaying the name of the relying party to the user in the browser interface

OTP code device/OTP token. Certification, employment of certified chips / technological solutions that are resistant to side channel attacks, user instruction, displaying the name of the relying party to the user in the browser interface

Identification app. Criteria in Annex C of the identification service assessment guideline 211/2019, displaying the session identifier to the user (*session binding*), transmitting the name of the relying party all the way to the app, user instruction. In order to ensure possession, the user must be notified using a second channel and verified contact details in connection with activating/connecting a new identification app (instance).

Authentication factor based on knowledge. LOA guidance, section 1.(2)(b):

If knowledge is used as a factor it is necessary to mitigate against guessing (either random or brute force) of the knowledge by an adversary.

For example: where the knowledge is a password, good practice prescribes a suitable password policy (e.g. see safeguard S 2.11 "Provisions governing the use of passwords" of the BSI IT-Grundschutz catalogues, Single token authentication & Password entropy of NIST 800-63-2 Appendix A).

Password/pass phrase. User instruction, requirements for diverse secrets, limiting the number of failed attempts

PIN code. User instruction, length requirement, the use of security measures provided by the app/platform in the entry phase, limiting the number of failed attempts

Factors likely to be known only by the owner of the factor (questions and answers). User instruction, several question and answer pairs, the questions may not be based on information available through other registries or sources.

Inherent authentication factor. LOA guidance, section 1.(2)(c):

Inherent authentication factors should have a variance even between people of similar characteristics so that a person may be uniquely identified: examples include fingerprints, palm prints, palm veins, face, hand geometry, iris, etc.

A key consideration when a biometric factor is being used is to ensure that the person to whom it relates is physically present at the point of verification. This is to mitigate against spoofing or duplication.

Annex C of the identification service assessment guideline 211/2019 contains criteria for the use of biometric authentication factors in connection with mobile apps. The security measures must observe both the characteristics of the application and the device.

For *inherent authentication factors,* there should be an effort to assess the capability of the terminal device sensors and the implementation of the comparison algorithms. Generally used terminology, such as FAR (False Acceptance Rate) and FRR (False Rejection Rate) are currently used indicators. Here, False Acceptance Rate depicting the rate of how likely it is to gain an accepted response for the wrong person is the more pertinent indicator. The number of retries increases the likelihood of gaining an approved response for the wrong person, meaning that inherent authentication factors should also consider this effect by restricting the number of attempts. Accepted FAR values must be based on the risk assessment.

Indicators related to implementations based on inherent authentication factors can be reviewed and tested on the NIST Face Recognition Vendor Test (FRVT) project [29] website, for example, https://www.nist.gov/programs-projects/face-recognition-vendor-test-frvt

It must be noted that identification service providers do not typically have the opportunity to affect these factors when using the terminal device's interfaces. The identification service provider may primarily try to determine and monitor the quality of functions that they employ in their own identification means.

A list of possible security measures
- Restricting the duration of the session
- Maximum number of failed attempts
- Password length and randomness

- Requirement to use multi-factor authentication
- Tolerances for false positives (fingerprint, face, other biometric factor)
- Encryption
- Secret processing and storage security
- Copying prevention
- Identification means holder notification

4.6.1.6 Risk assessment and attack potential

Risk management is part of the identification service risk management required in provision 4.2 3, meaning that the identification service is most likely already employing some form of risk management. Risk management requirements and possible standards are discussed above in the explanation for provision 4.

The identification means risk tolerance and residual risk acceptability must be scaled to the resistance requirement against attack potential on a certain level.

The Electronic Identification Assurance Level Regulation LOA Guidance mentions two standards as references for evaluating attack potential as follows:

LOA guidance [22], section 2.3.1:

> *The authentication mechanisms used in the authentication phase cannot completely prevent all attacks, they can only offer resistance to attacks on a certain level of security/assurance. A standard way to quantify the resistance of different mechanisms is to rank them according to their resistance against attacks with a certain attack potential (i.e. strength of an attacker).*
>
> *The Level of Assurance uses the terms "enhanced-basic", "moderate" and "high" to denote the different attack potentials. These terms were adopted from standards*
> *ISO/IEC 15408, "Information technology – Security techniques – Evaluation criteria for IT security" and ISO/IEC 18045 "Information technology – Security techniques – Methodology for IT security evaluation". The text of the standards is also freely available at www.commoncriteriaportal.org/cc (CCPART1- 3 being equivalent to ISO/IEC 15408 and CEM equivalent to ISO/IEC 18045).*
>
> *In standard ISO/IEC 15408-1, attack potential is defined as a measure of the effort to be expended in attacking a target of evaluation, expressed in terms of an attacker's expertise, resources and motivation.*
>
> *Annex B.4 to standard ISO/IEC 18045 / CEM contains Guidance on how to calculate the attack potential necessary to exploit a given weakness of an authentication mechanism.*
>
> *In order to meet the requirements set out in the implementing regulation, some assessments of resistance against potential attacks should be carried out.*

4.6.1.7 Provision 6.1.2 Authentication factor independence

A specified requirement concerning the characteristics and security measures of the identification means to ensure the independence of the authentication factors is added to provision 6.1.2.

The independence of the factors is essential, especially if the different factors are used on the same terminal device, such as a smartphone. The practical implementation of separation and any security measures depend on the means.

4.6.1.8 Provision 6.1.3 Encryption requirements of the identification means and authentication

Provision 6.1.3 specifies the encryption requirements concerning the identification means and authentication mechanism. The provision corresponds to provision 5.1.2, which stipulates the technical encryption quality of the entire identification scheme.

Other stipulations concerning the encryption of identification services and relying party communications are laid down in provision 7 and concerning messages in provision 9.

Provision 6.1.3 specifies the protection requirements in section 6.1.1 in terms of encryption solutions. The provision stipulates that internationally or nationally recommended methods must be employed. Similarly to other protection measures, the implementation and selection of an encryption solution must take into account the risk assessment. As far as communications are concerned, encryption solutions are based on the algorithms, methods and values in provision 7. The phrase 'where technically applicable' means methods that are technically possible in the first place. Taking the risk assessment into account means that other security measures can be grounds for applying solutions specified in provision 7 only partly when assessed on the whole.

Encryption methods deemed generally reliable must be used in
- creating and managing holder-specific secrets.
- protecting holder-specific secrets (usually a private key) on the terminal device or in the background system.
- all functions affecting the integrity and confidentiality of the identification means as a rule.

The communications encryption requirements in provision 6 in accordance with provision 7 pertain to
- communications between the identification means in the possession of the user and the identification scheme, i.e. the authentication of the identification means holder insofar as the messages are not covered by the requirements on message encryption in provision 9. In comparison to message encryption stipulated in provision 9, provision 6.1.3 refers to challenge-response messages that are used in authentication between the identification means holder and the system of the identification means provider.
- Example from assessment guideline 211/2019 [21], Annex C Special criteria for mobile identification solutions: hard fail certificate pinning between the mobile app and the background system.

The mobile app as part of the user's identification means is connected to the identification means provider's background system in current identification means. The information security concerning this section is stipulated in provision 6. Whereas in identification means that use a chip card, the user's means is connected to the identification means provider's card reader application, which is part of the identification scheme.

If identification means were to develop in accordance with Self Sovereign Identity models, for example, so that the application on the user's terminal device (so-called wallet app) relays identification messages or attribute verifications to relying parties, the implementation of the requirements would probably warrant a review. This would also probably mean that responsibilities and procedures in authenticating the parties should also be reviewed.

4.6.2 Provision 6.2 Specific security measures

4.6.2.1 Provision 6.2.1 Displaying service event itemising data to the user (session binding)

This requirement is new to this version of the regulation.

The identifying data for the identification event or service event means any character string, image or other information displayed to the identification means user both in the identification means and the e-service app or browser session (session binding). The user must be able to easily connect the identification request with the service event based on this information. The purpose is to make it possible for the identification means user to not authenticate any incorrect or fraudulent authentication requests.

Naturally, this requirement only applies to identification means using a dedicated screen. Displaying is not typically technically possible in one-time-password token/device . This procedure has been observed in the mobile application criteria ('binding message') in Annex C of the identification service assessment guideline 211/2019.

The displayed data may take different forms; character strings, phrases, images or QR codes. Legibility and comprehensibility must be observed, however, in order for the user to easily associate the service event with the identification request.

The accessibility requirements specified in the Act on the Provision of Digital Services (306/2019) [30] should be observed in displaying the event identifier.

The provision does not specify whether the responsibility to display the data lies with the identification broker service or the identification means provider.

See provision 24 on the transition period.

4.6.2.2 Provision 6.2.2 Displaying the name of the relying party to the user (SP-name)

This requirement is new to this version of the regulation.

Data on the relying party refers to the e-service that is the recipient of the verification of the identification. The purpose of the regulation is to ensure that when the name of the e-service that has requested the authentication and is the recipient of the verification is displayed to the user, the user has the possibility to realize and to not authenticate any incorrect or fraudulent identification requests. This works to reduce the risk of the user being mislead about which e-service they are identifying for.

Similarly to the identification request itemisation data specified in provision 6.2.1, data on the relying party can only be displayed on identification means with a screen.

The identification event implementation and the party informing the user in the identification chain will vary, making it impractical to determine binding rules for who shall display the information to the user, the identification broker service or the identification means provider. The specification concerning displaying data should take all phases in which the data can be displayed to the user into account as comprehensively as possible. The focus should, however, be on the phases and interfaces of the identification process in which the user is asked to perform actions, such as the identification means selection window, any interfaces presented by the identification broker service, the browser interface or the identification app of the identification means provider or other identification means or authentication sections that allow for displaying data.

The accessibility requirements specified in the Act on the Provision of Digital Services (306/2019) [30] should be observed in displaying the name of the e-service.

This data is stipulated as a mandatory attribute in the interface between the identification means and the identification broker service in provision 12.1. This data is produced by the identification broker service. The attribute has already been defined as voluntary in the SAML and OpenID Connect interface recommendations [31, 32] (*ftn_spname*) of the trust network, and mandatory since 2021, meaning that the preparedness for the attribute may already exist in the interfaces of some identification services.

See provision 24 on the transition period.

4.6.2.3 Provision 6.2.3 Single-sign-on (SSO)

This provision is new to this version of the regulation.

According to the interpretation of the Agency, the Identification and Trust Services Act allows for offering single sign-on, provided that a registered identification service provider is responsible for its security, reliability and conformity and the conformity of the implementation has been assessed.

General stipulations on factors specific to single sign-on affecting the security management of the identification means and authentication are laid down in the provision. These include at least session duration management, session transfer between relying parties and session termination, i.e. single logout.

Provision 6.2.3 stipulates that the requirement of displaying the name of the relying party specified in provision 6.2.2 also applies to special situations in which the identification service offers identification means holder identification to more than one relying party using single sign-on. Single-sign-on is sometimes also referred to as federation.

From the point of view of the user, SSO means that the user moves from the e-service of one relying party to the e-service of another relying party without identifying again, i.e. without authenticating again that they are the rightful holder of the strong electronic identification means. According to provision 6.2.3, the user must be informed of being transferred to another service in connection with the transfer and the name of the service must be displayed to the user, as required in provision 6.2.2. The user must have the option to accept or cancel the transfer. Please note, this means that provision 12.1 4) only applies to the first relying party. The log data for SSO sessions must be stored.

The provision does not specify whether the identification broker service or the identification means provider displays the information to the user.

Whereas in the Agency's assessment, the displaying of session binding specified in provision 6.2.1 for identification events / service events is not technically feasible in all of the sessions connected to SSO, meaning that it will not be required in other than the first phase of SSO, i.e. authentication.

Other instruments. Many legal interpretations and plenty of information exchange related to technical implementation and security have been connected to single-sign-on. The Agency has provided guidance on the interpretations in the matter and technical factors have been discussed together with identification services. This work will continue and the Agency will decide on practical instruments in the course of the work. Due to the differing views of the identification services thus far, *guidelines*, *recommendations* or *interpretation policies* issued by the Agency seem most feasible.

4.6.3 Provision 6.3 Connecting identification means to a person

Provision 6.3.1 is a basic requirement that has been added to the regulation in the interest of clarity. It states that authentication factors must be connected to the identification means holder in the identification scheme.

Naturally, this connection varies between authentication factors, e.g. the processing of PIN codes and biometric factors differs from connecting to an application or OTP code device.

Provision 6.3.2 corresponds to the requirement in section 6 of the regulation drafted in 2016, which specified certain details related to the creation and issuing of identification means that involve application issues. They concern single processes mainly related to the issuing of identification means used to ensure that the means may only be used by its rightful holder. The requirements are similar to the previous Regulation 8 predating 2016 apart from the requirement being made more flexible in 2016 by allowing different processes for issuing an identification means.

The requirement of provision 6.3.2 means that in principle, identification means cannot be created and stored to wait for potential customers by linking personal information to the identification means. In principle, the initial identification shall be performed before linking personal information to the identification means.

Provision 6.3.2 also allows a process linking personal information to the applied-for means already before the initial identification referred to in section 17 of the Identification and Trust Services Act is performed. This may be necessary, for instance, if the initial identification is performed by a personal visit and the aim is to complete the issuance process during one visit. Such needs are justified, for instance, when the Digital and Population Data Services Agency produces identification certificates for people who are abroad.

Application. If personal information is linked to an identification means prior to initial identification, the application and issuance process shall otherwise contain security measures that account for the risk of wrongly created (using false personal information or without any intention to apply for an identification means) identification means and risk of using the identification means before passing initial identification. Such risks may be minimised, for example, by performing a Population Information System check before linking personal information to the means, by technically preventing the use of identification means prior to initial identification and by verifying

that the identification means applied for and ordered correspond to the delivered means.

As a primary safeguard, the Finnish Transport and Communications Agency recommends technically preventing the use of an identification means by a revocation list, for instance, until all conditions for issuing and delivering the means are fulfilled. Under regulation, a revoked certificate cannot be retrieved but this prohibition does not apply to technically preventing a certificate under preparation and activating the certificate after the applicant has passed the initial identification.

Section 21 of the Identification and Trust Services Act contains more detailed provisions on delivering the identification means to the applicant. Under paragraph 2.2.2 of the EU Assurance Level Regulation, identification means at the high assurance level also need a separate activation process.

Furthermore, it shall be ensured that the initial identification is associated with the issuance of the identification means and that the user is aware of this. However, it is possible to also provide other services, such as mobile subscriptions or banking services, in the same connection and identify the person for this purpose, too.

In connection with issuing an identification means and binding the means to a person, it is recommended to try to manage the risk of unauthorised binding by notifying the user via another channel and using verified contact details.

4.6.4 Provision 6.4 Processing identification means holder specific data

These requirements specify certain details related to the creation and issuing of identification means that involve application issues. They concern single processes mainly related to the issuing of identification means used to ensure that the means may only be used by its rightful holder. Sections 8 and 8 a of the Identification and Trust Services Act contain provisions on the security of the identification means and identification scheme.

Secret information referred to in the provision include at least the private key related to the identification means and the PIN code for its use, a password or a biometric authentication factor template.

According to provision 6.4.1, it shall be ensured that secret information related to the identification means is not revealed to the identification service provider staff under any circumstances. This requirement was included in the regulation issued prior to 2016.

In the Agency's opinion, the requirement must not be removed because situations where secret information, such as a PIN code, can be revealed to the service provider staff during the issuing process continue occasionally to be found during the supervision of issuing practices.

The requirement of provision 6.4.2 ensures that secret information is only known or accessible by the applicant (holder) of the identification means. This guarantees that no one else can use the identification means.

In practice, the requirement means that a PIN code or other code associated with an identification means must not be revealed at any stage to the staff of the registration desk, and it must not be transmitted through information systems, such as e-mail, in which a copy of it is left behind.

Cf. Electronic Identification Assurance Level Regulation [4]

> 2.2.1/2. *The electronic identification means is designed so that the issuer takes reasonable steps to check that it is used only under the control or possession of the person to whom it belongs.*
>
> 2.3.1/2. *Where person identification data is stored as part of the authentication mechanism, that information is secured in order to protect against loss and against compromise, including analysis offline.*
>
> 2.4.6/3. *Access to sensitive cryptographic material, if used for issuing electronic identification means and authentication, is restricted to the roles and applications strictly requiring access. It shall be ensured that such material is never persistently stored in plaintext. ...Sensitive cryptographic material, if used for issuing electronic identification means and authentication, is protected from tampering.*

4.6.5 Alternative regulation considered, provision 6.1 identification means security requirements

The definition of secure or vulnerable authentication factors and identification means entity was discussed during the preparation of provision 6.1. The alternatives have been discussed and assessed as follows:

a) Authentication factor specific requirements would be specified in the regulation

Any authentication factors connected to possession, knowledge or biometric characteristics are very different from each other and there are many of them. In comparison, PSD2 regulation provides detailed requirements for each primary type, e.g. protecting factors based on possession from copying.

Due to the diversity and development of authentication factors, this regulation model would involve details that cannot be covered on a regulatory level, or doing so would not be practical. Furthermore, threats to identification means security and security measures as protection against threats are not purely authentication factor specific.

An example of this type of regulation would be to stipulate that the copying of authentication factors based on possession must be prevented and that authentication factors based on possession must be based on a cryptographic secret. This would make it clear that a printed online banking code list would not meet these requirements and the regulation would need to specify a transition period for discontinuing the use of printed online banking code lists or for strengthening the lists with an additional feature based on a cryptographic secret to protect them from copying.

Based on stakeholder consultation, some identification services intend to continue using printed online banking code lists as part of their identification means, even though their use is largely being replaced with mobile identification apps and OTP code devices. The issue that adding SMS verification to the identification event, for example, will increase costs has been raised during preparatory work. This increase has been criticised because a maximum price for identification events between identification means and identification broker services has been regulated in the trust network. The Finnish Transport and Communications Agency has not reviewed the prices of SMS services to identification services.

b) Identification means resistance requirements would be specified in the regulation

The attack resistance of the authentication mechanisms of identification means on the substantial and high assurance level against moderate or high level attack potential is stipulated in the Identification Act and the Electronic Identification Assurance Level Regulation. The Assurance Level Regulation also mentions threat types on the provision level.

Resistance to moderate or high level attack potential is an entity based on the different security features of the authentication factors, the combination of identification means security measures and the continual monitoring of changing threats.

Resistance indicators or other specifications could possibly be defined in the regulation by means of a reference to a generally used risk assessment standard. The Assurance Level Regulation LOA Guidance mentions *ISO/IEC 15408 "Information technology – Security techniques – Evaluation criteria for IT security"*[23] and *ISO/IEC 18045 "Information technology – Security techniques – Methodology for IT security evaluation"*[24] as a reference for attack severity evaluation.

In the Agency's opinion, there is insufficient information on the applicability of the standards for all identification means to refer to them as compelling in the regulation.

Instead, the Agency is of the opinion that the resistance requirement can be specified in the regulation by listing factors that must be observed in the assessment.

c) The regulation specifies the requirements for identification means threat and risk assessments

The Guideline for EU Assurance Level Regulation (LOA Guidance) states that the different factors must be selected so that they work to prevent different threats / attack methods and that the procedure used to authenticate the factors must also be considered in addition to the factors themselves. The LOA Guidance also contains the references to the standards mentioned above.

This regulation model specifies the requirement of conducting a risk assessment and the components that must be observed in it. The risks to the authentication factors and authentication mechanism must be assessed separately and the resistance of the identification means must be based on a threat and risk assessment corresponding to the assurance level.

In the Agency's assessment, this model is flexible enough in terms of various identification means and authentication factors and observes the identification means security controls as a whole. Any supervision solutions defined by the Agency would be based on an accurate risk assessment of the identification service, which would also take the effect of security controls into account.

The operators considered this model good during the first hearing in the workshop on 10 March 2021. Specifications based on an established risk assessment standard were proposed to be added to the application instructions to enable conformity assessment. The fact that measures protecting users from phishing may reduce user comfort was also raised, and the participants proposed that these measures should be implemented across all identification means to keep competition fair. It was once again expressed that risks vary based on the number of identification means provider users and that attacking the users and method of a large service provider is much more attractive to criminals.

4.6.6 Provision 6 Compatibility of the Identification Act/Assurance Level Regulation and PSD2 regulation

Strong electronic identification used in bank and payment transaction services is regulated by the PSD2 directive [33] and the Commission implementation act based on it (EU) [34]. Nationally, stipulations on payment services are laid down in the act on payment services (290/2010)[35].

On the other hand, the stipulations in the eIDAS Regulation and the Identification Act are independent of the field, i.e. neutral in terms of which field and service uses the identification.

These regulations have not been harmonised on the EU level as of yet.

In Finland, many strong electronic identification means registered in accordance with the Identification Act are also used as strong electronic identification in accordance with payment service regulations. This raises the question whether the requirements in regulation are contradictory and whether the same identification means can be offered in both branch-independent identification and specifically regulated payment services.

In 2018, Traficom (known at the time as the Finnish Communications Regulatory Authority) and the Financial Supervisory Authority reviewed the technical compatibility of the regulations and consulted the branch, the Finnish Financial Supervisory Authority PSD2 co-operation group and the Finnish Communications Regulatory Authority eIDAS work group on the review [36]. **Based on the review and the statements, no impediments to using the same identification means within both of the regulatory frameworks were found in 2018, provided that the stricter or more detailed of individual requirements were always complied with.**

After the shared review in 2018, the Finnish Financial Supervisory Authority has drafted a policy stating that printed online banking code lists do not meet the requirements of the payment service regulations without an additional authentication factor. In payment services, identification means that use a printed online banking code list as one of the authentication factors must add a factor in addition to the online banking code list (and a factor based on the holder's knowledge and characteristic). Typically, banks use text messages as additional verification for online banking code lists, i.e. the user must prove the possession of both the online banking code list and mobile subscription.

In 2020, the Finnish Transport and Communications Agency compiled comparison data as part of its official duties for the preliminary amendment needs questionnaire on the application of the Electronic Identification Assurance Level Regulation and the payment service regulations and application instructions to identify differences and assess the effects of the differences. **No new observations or other essential differences with the exception of the printed online banking code list were found in the comparison or the comments from the branch from 2020-2021.**

4.7 Provision 7 Identification scheme interface encryption requirements

4.7.1 Provision 7.1 Communications encryption methods

4.7.1.1 General

Provision 7.1 contains stipulations on communications encryption. The purpose is to ensure the integrity and confidentiality of identification events on the communications level.

The requirements must be applied between identification service providers and between identification service providers and relying parties, i.e. e-services. These requirements apply to communications especially outside a protected physical space and in a non-trusted network. A non-trusted network refers to the internet or an office network or other network in which the security has not been fully evaluated and secured.

The application of the requirements to data transfers to identification scheme subcontractors is stipulated in provision 5.

The algorithms, values and methods listed in the provision are mandatory for the purpose of the provision *"in the encryption, key exchange and signing…".* This means that attacks that would prevent the use of the SHA-1 algorithm, which has as such been found weak, in certain cases have not been found in certain use cases of the SHA-1 algorithm. The use of the algorithm is not recommended because the applicator may have difficulties assessing the possible secure use cases, for example. It has been used in identification services for e.g. creating randomness, but the use of this algorithm should be discontinued unless it has been found to be secure and necessary in a careful assessment.

Alternative methods of regulation, 7.1 communications encryption. The Agency has assessed the alternative presented in branch comments during the preparation of section 7.1 to completely replace the list in the regulation with a reference to the NCSA [37] instruction. Firstly, based on experience with supervision , the Agency is of the opinion that minimum requirements must still be laid down unambiguously. Secondly, the Agency is of the opinion that the NCSA and SOGIS MRA [38] lists are maintained for a different purpose and they may in some regards be unnecessarily strict compared to identification requirements on the substantial assurance level. The requirements in the regulation should take the security requirement level of identification services into account, and the requirements should not be tied to the requirement level of nationally or internationally classified data.

4.7.1.2 Provision 7.1.1 Mandatory encryption methods

Provision 7.1.1, subsections 1–4 and their order are based on a typical cryptographic design order and requirements.

The word certificate has been added to the introductory sentence in the interest of clarity, because it is an essential part of communications encryption in practice.

The definition of secure procedures, algorithms and values used is based on the Finnish Transport and Communications Agency NCSA Crypto Approval Authority (CAA) instruction *Kryptografiset vahvuusvaatimukset luottamuksellisuuden suojaamiseen - kansalliset suojaustasot (ohje 28.11.2018, Doc no. 190/651/2015) (Cryptographic strength requirements for protecting confidentiality - national protection levels (Guideline 28 November 2018 reg. no. 190/651/2015))* for the purpose

of assessing the security of crypto solutions in situations where data is being transferred in a non-trusted network. [39]

The objective is to reach a strength of 112 bits on the substantial assurance level.

The NCSA (National Communications Security Authority) is in charge of security matters concerning the electronic transfer and processing of classified material. The NCSA function serves as the national *Crypto Approval Authority (CAA*). The tasks of the CAA authority include the assessment and approval of cryptos intended for the protection of classified material. The task is based on the EU Council security rules (2013/488/EU) and the act on international information security obligations (laki kansainvälisistä tietoturvallisuusvelvoitteista (588/2004)).

Abbreviations used in the regulation:

AES = Advanced Encryption Standard (symmetric encryption method)
DH = Diffie-Hellman (key exchange protocol)
DHE = DH ephemeral keys
ECDH = Elliptic Curve Diffie-Hellman (key exchange protocol)
ECDHE = ECDH ephemeral keys
ECDSA = Elliptic Curve Digital Signature Algorithm (signature method)
EdDSA = Edwards-curve Digital Signature Algorithm (signature method)
RSA = Rivest-Shamir-Adleman (asymmetric encryption and signature method)
SHA = Secure Hash Algorithm (hash function)
TLS = Transport Layer Security (encryption protocol)

7.1.1 1) Key exchange referred to in subsection 7.1.1 1) means methods included in the TLS protocol, for example. The Regulation specifies the encryption methods to be used in the key exchange.

The specified key exchange requirements may be met by using the DH groups 14 to 21, 23, 24 and 26 of IANA's (Internet Assigned Numbers Authority) IKEv2 specifications.

https://www.iana.org/assignments/ikev2-parameters/ikev2-parameters.xhtml
Transform Type 4 - Diffie-Hellman Group Transform IDs [40]

7.1.1 2) The basis for subsection 7.1.1 2) is that the RSA is the standard assessed and recommended by the NCSA, and ECDSA and EdDSA provide a corresponding level of confidence. In the Agency's view, there are no other alternatives available in practice. EdDSA is added to the section. Suitability for asymmetric encryption will be added to the section, because when using RSA for message encryption in accordance with section 9, the encryption is asymmetric.

7.1.1 3) Encryption algorithm ChaCha20 has been added to subsection 7.1.1 3). Encryption mode CCM has also been added to the subsection. Encryption mode CBC will remain in the regulation. Some assessment tools refer to it as outdated, but in the Agency's view it is sufficiently secure, provided that the correct definitions and updated libraries are used. It is worth noting that 3DES has been removed from the recommendations as early as 2016. Encryption mode XTS will be removed from the subsection, because it is not suited to communications encryption, but rather disk encryption.

7.1.1 4) Authentication code Poly1305 will be added to subsection 7.1.1 4). In the Agency's assessment, the combination of ChaCha20 and Poly1305 can be deemed

sufficiently secure in connection with identification operations, even though NCSA-FI or SOGIS MRA have yet to confirm POLY1305 for the purposes that the references in question are used. Allowing the combination will enable the use of a wider range of ICT services and the newest solutions provided within them to identification services.

SHA-2 functions refer to functions SHA-224, SHA-256, SHA-384 and SHA-512. SHA-3 functions refer to functions SHA3-224, SHA3-256, SHA3-384, SHA3-512. This specification will be moved from the regulation to the explanatory notes.

4.7.1.3 Recommendation on making section 7.1.1 stricter for high assurance level identification services

The recommendation on applying section 7(1) in the 2016 regulation, i.e. section 7.1 of the amended regulation, will be updated. Some of the lighter procedures and values listed in the regulation will be removed from the recommendation. The recommendation corresponds to security category TL VI [39] defined in the assessment guideline issued by the Crypto Approval Authority (CAA).

Alternative methods of regulation, 7.1 on the high assurance level. It was discussed during the preparatory phase whether the recommendation should be kept in the explanatory notes or whether it should be made mandatory and moved to the requirements for the high assurance level. The Agency assesses that making the values in the recommendation concerning the high assurance level mandatory would not cause interoperability issues, because identification brokering allows for case-specific selection of algorithms from the technical point of view. However, the Agency is of the opinion that the impact on relying parties using high assurance level identification is more difficult to assess.

Recommendation

Note! The requirements for the high assurance level have been written in **bold** in the text and the requirements for the substantial assurance level, which are insufficient on the high assurance level, have been ~~struck through~~.

At the high level of assurance, instead of using the requirements for substantial level of assurance provided in section 7.1 of the Regulation, it is recommended to apply the following values in parentheses, **which will meet the minimum assurance level of 128 bits**, *to the identification scheme:*

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~~ (**4,096** at high level of assurance) bits in DHE and at least ~~224~~ (**256** at high level of assurance) bits in ECDHE.*

   *The DH groups ~~14~~ to 21, ~~23, 24 and 26~~ (from **16~~15~~ to 21** at high level of assurance) of IANA's IKEv2 specifications meet the above requirements.*

2) ***Signature or asymmetric encryption:*** *When using the RSA for electronic signatures or encryption, the key length shall be at least ~~2,048~~ (**3,072** at high level of assurance) bits. When using the elliptic curve method ECDSA or EdDSA, the underlying field size shall be at least ~~224~~ (**256** at high level of assurance) bits.*

3) ***Symmetrical encryption:*** *The encryption algorithm must be AES, Serpent or ChaCha20 (**AES or Serpent** at high level of assurance). The key length shall be at least 128 (**128** at high level of assurance) 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.*

*SHA-2 refers to functions ~~SHA224~~, SHA256, SHA384 and ~~SHA512~~ (**SHA-3-256, SHA-3-384, SHA-3-512** on the high assurance level)*

5) In addition to methods and values mentioned above in sections 1–4, methods and values that have been assessed as secure in the uses referred to in the specified sections of the following documents or their updated versions:

a) The Kryptografiset vahvuusvaatimukset luottamuksellisuuden suojaamiseen - kansalliset turvallisuusluokat (Dnro 190/651/2015) [39] instruction (in Finnish) issued by the Crypto Approval Authority operating within the Finnish Transport and Communications Agency, or

b) the SOG-IS Crypto Evaluation Scheme Agreed Cryptographic Mechanisms of the SOGIS-MRA (*Senior Officers Group for Information Systems, Mutual Recognition Agreement*) [41], an agreement between certain certification bodies of EU or EEA Member States.

4.7.1.4 Provision 7.1.2 Encryption methods assessed and allowed by the NSCA and SOGIS MRA

Provision 7.1.2 is new to this version of the regulation.

According to it, algorithms and values assessed to be secure by the NCSA or SOGIS MRA, which can be found in the sources referenced in the Regulation, can be used in addition to the algorithms and methods listed in sections 1–4 of provision 7.1.1. The most up-to-date document must always be used when accessing the sources.

The Agency considers the list drafted by the NCSA an appropriate source, and it has also been used as a basis and baseline in issuing the regulation in more general terms. The Agency considers the list maintained by SOGIS MRA another current and relevant source.

The purpose of the addition is to enable the use of reliable procedures in situations where there is insufficient time to make changes to the regulation.

4.7.1.5 Provision 7.1.3 Enforcing settings

The requirement in provision 7.1.3 on the technical forcing of encryption settings means that when systems are configured, weaker default settings or a situation where the system could pass requirements must not be allowed. The requirement will not be changed.

The default features of software and devices are often based on supporting functionality in a flexible manner by using as many alternative specifications as possible, but when encrypting an identification scheme, the settings shall prevent a weaker encryption.

4.7.2 Provision 7.2. Communications encryption protocol (TLS)

Provision 7.2 contains stipulations on communications encryption protocols. The section specifies the requirement to only cover the TLS protocol, because it is the predominant protocol in practice.

The minimum TLS level is raised to version TLS 1.2.

The exception concerning TLS 1.1 allowed in the 2016 regulation will no longer be allowed. TLS 1.1 dates from 2006, and has known vulnerabilities.

The version of the TLS protocol for communications connections affects the age of the terminal devices and browsers used by the users. The Agency has assessed based on operator feedback, for example, that the users' terminal devices support at least TLS 1.2 quite comprehensively. Some already use version TLS 1.3.

Based on feedback from stakeholders, the Agency has assessed that there is no need to provide a transition period for this requirement. Updating the TLS version is part of ordinary technical development. In terms of identification service provision and fair competition, and based on experience from forbidding TLS 1.0, it is beneficial to mandate all operators to make the switch from the earlier version to the current version at the same time.

If an identification service safeguards the confidentiality and integrity of communications by other means than the TLS protocol (e.g. IPSec or SSH), it shall provide a corresponding level of cryptographic strength. In the Agency's assessment, there is still no need to specify any other communication protocols other than TLS in the Regulation.

4.7.3 TLS 1.2 and TLS 1.3 encryption profiles

This section provides instructions on how to identify cipher suites that meet the requirements in section 7.1.

Not all algorithms, methods and values mentioned in section 7.1 can be used in TLS, but combinations for TLS 1.2 and TLS 1.3 profiles can be selected from the list. In addition to specifying cipher suite, fulfilling the encryption requirements in the system in practice requires ensuring that the DH parameters and asymmetric keys and certificates in TLS configuration are sufficiently strong.

Cipher suites used by the NCSA in assessing cryptos (on level TL IV)

- DHE-RSA-AES-128-CBC-SHA256
- DHE-RSA-AES-256-CBC-SHA256
- DHE-RSA-AES-128-GCM-SHA256
- DHE-RSA-AES-256-GCM-SHA384
- ECDHE-RSA-AES-128-CBC-SHA256
- ECDHE-RSA-AES-256-CBC-SHA384
- ECDHE-RSA-AES-128-GCM-SHA256
- ECDHE-RSA-AES-256-GCM-SHA384
- ECDHE-ECDSA-AES-128-CBC-SHA256
- ECDHE-ECDSA-AES-256-CBC-SHA384
- ECDHE-ECDSA-AES-128-GCM-SHA256
- ECDHE-ECDSA-AES-256-GCM-SHA384

Those listed in RFC 7905[42]
https://tools.ietf.org/html/rfc7905

- ECDHE-RSA-WITH-CHACHA20-POLY1305-SHA256

- ECDHE-ECDSA-WITH-CHACHA20-POLY1305-SHA256
- DHE-RSA-WITH-CHACHA20-POLY1305-SHA256

TLS 1.3 ciphersuites listed in RFC 8446 [43]
https://datatracker.ietf.org/doc/html/rfc8446

- AES-256-GCM-SHA384
- CHACHA20-POLY1305-SHA256
- AES-128-GCM-SHA256
- AES_128_CCM_SHA256

4.7.4 Sources of nationally or internationally recommended encryption solutions

- The NCSA function of the Finnish Transport and Communications Agency (National Communications Security Authority, NCSA-FI) Kryptografiset vahvuusvaatimukset luottamuksellisuuden suojaamiseen - kansalliset suojaustasot (ohje 28.11.2018 dnro 190/651/2015) *(Cryptographic strength requirements for protecting confidentiality - national protection levels (Guideline 28 November 2018 Doc no. 190/651/2015))* [39]
    - https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/regulation/ohje-kryptografiset-vahvuusvaatimukset-kansalliset-suojaustasot.pdf
    - Encryption solutions approved by the NCSA (1 July 2020 Doc no. 1240/651/2017) [44] https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/NCSA_salausratkaisut.pdf
    - general NCSA-FI information https://www.kyberturvallisuuskeskus.fi/en/our-activities/ncsa
- SOGIS-MRA SOGIS Agreed Cryptographic Mechanisms (version 1.2 January 2020) [41]
    - https://www.sogis.eu/documents/cc/crypto/SOGIS-Agreed-Cryptographic-Mechanisms-1.2.pdf
    - Currently more up-to-date than the NCSA-FI list and contains more algorithms that have not yet been approved/listed in Finland. Updated every other year.
    - General information on SOGIS MRA

      https://www.sogis.eu/uk/supporting_doc_en.html#:~:text=The%20document%20%C2%AB%20SOG%2DIS%20Crypto,by%20all%20SOG%2DIS%20participants
- IANA (Internet Assigned Numbers Authority)
    - IKEv2 parameters [40]: http://www.iana.org/assignments/ikev2-parameters/ikev2-parameters.xhtml
    - IANA ciphersuites [40]: http://www.iana.org/assignments/tls-parameters/tls-parameters.xhtml#tls-parameters-4
- RFC 7905 ChaCha20-Poly1305 Cipher Suites for Transport Layer Security (TLS) [42]

- https://tools.ietf.org/html/rfc7905

- RFC 8446 The Transport Layer Security (TLS) Protocol Version 1.3 [43]
  - https://datatracker.ietf.org/doc/html/rfc8446

- The eIDAS Cooperation Network [45] technical specification eIDAS Cryptographic Requirements for the Interoperability Framework, TLS and SAML, Version 1.2, 31 August 2019 [46]
  - https://ec.europa.eu/cefdigital/wiki/download/attachments/82773108/eIDAS%20Cryptographic%20Requirement%20v.1.2%20Final.pdf?version=2&modificationDate=1571068651805&api=v2
  - General information on the eIDAS Cooperation Network: Cooperation Network Resources - eID User Community - CEF Digital (europa.eu)

- ETSI standards or specifications
  - Feb 2019 - ETSI TS 119 312 V1.3.1 (2019-02) "Electronic Signatures and Infrastructures (ESI); Cryptographic Suites" [47]
  - https://ec.europa.eu/cefdigital/wiki/display/EIDTECHSUB/Security+Profile+v+1.3

- NIST SP 800-52 Rev. 2, Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations [48]
  - https://csrc.nist.gov/publications/detail/sp/800-52/rev-2/final

4.8 Provision 8 Authenticating parties to the communications

4.8.1 General

Provision 8 specifies the requirement on identifying parties to communications in section 8.2 in the 2016 regulation and makes it stricter. Provision 8 also expands the requirement to cover connections between the identification service and the relying party and specifies the basic requirements for key exchange and updates.

Provision 8.1 stipulates how to ensure during the establishing of a communications connection that the other party is the correct party.

Provision 8.2 stipulates the maintenance of the communications connection trust.

These requirements are similar between trust network operators and between the identification service and the relying party, i.e. the e-service. Verifying the relying party is a crucial method of protecting the identification means user from verifying fraudulent identification requests.

Trust may be based on reliably provided TLS certificates or keys intended for protecting messages.

Transition periods, see provision 24.

Other steering instruments

Guideline. Until now, authorities have not issued guidelines on the practices of party authentication and key exchange.

Recommendation. The requirements may be added to interface recommendations. The questionnaire yielded comments on the recommendation not being applied consistently. That is why the Agency does not consider the guideline or recommendation a sufficiently effective measure to ensure reliable practices in authenticating e-services.

Co-regulation. The trust network co-operation group has tried to compile shared key exchange practices. In the Agency's assessment, consistent practices that everyone could commit to have not been found. Identification services hope that authorities would define approved procedures.

Information steering. Not considered.

4.8.2 Provision 8.1 Authenticating parties to the communications connection

Provision 8.1 stipulates how to ensure during the establishing of a communications connection that the other party is the correct party. Authenticating the parties to communications is a basic part of reliable electronic identification services. Electronic identification must ensure that communications and messages are genuine and remain confidential.

Direct bilateral procedure in the regulation means that the party's certificate and encryption keys must be supplied so that the holder can specifically be identified. The regulation does not unequivocally address the details of the procedure or what is a sufficient method of identifying the other party. Using strong electronic identification, for example, is a good practice. Parties always make an agreement between them, meaning that any practical matters can be covered in the agreement process.

The requirement concerning bilateral procedures means that the existing requirement is made more restrictive. Thus, authenticating a party may not rely solely on basic practices defined in protocols; instead, it requires special procedures to ensure that the communications certificate or keys belong to the communications party.

Bilateral means that identification cannot be solely based on the certificate of one party regardless of what type of certificate it is.

In the Agency's view, a single certificate alone will not prove that the pair to the certificate key is in the possession of the correct holder. The certificate holder's key management practices are not covered by the certificate issuing requirements.

The Agency also assesses that even though the CA issuing the certificate and the certificate itself were very reliable, it is quite easy to neglect to ensure that only the certificate in question is approved in the communications connection configuration, as this is not a typical basic function.

The key related to TLS certificate ot the key related to protecting messages can, however, be supplied after it has been signed using a qualified electronic signature or sealed using a qualified electronic seal in accordance with the eIDAS Regulation. The use of qualified electronic signatures or seals requires the use of a Qualified Signature/Seal Creation Device (QSCD), which works to secure that the keys used to create the signature or seal are in the possession of the correct person.

See the eIDAS Regulation [3]

> Art. 35.2: *2. A qualified electronic seal shall enjoy the presumption of integrity of the data and of correctness of the origin of that data to which the qualified electronic seal is linked.*
>
> Art. 25.2: *2. A qualified electronic signature shall have the equivalent legal effect of a handwritten signature.*

For the sake of comparison, the Agency states that during the TUPAS practice, trust was established by exchanging keys in reality. If the practice were to change here so that trust would be established based on certificates as in typical traffic exchange, security would no longer be on the same, sufficient level. In this regard, the requirements in the regulation differ from the PSD2 regulation requirement concerning authentication with payment initiation services and account information services (so-called *Third Party Providers, TPP*) based on trusting qualified website authentication or qualified electronic seal certificates in accordance with the eIDAS Regulation. However, PSD2 regulation has an added requirement that the TPPs in question are supervised by the finance branch supervisory authority and have been entered into their register.

Technical application. The Agency states that when using the OpenID Connect protocol[49], a *jwks_uri* address alone is not enough to authenticate a party reliably; instead, other procedures must also be used. Authenticating a *jwks_uri* address using a fixed IP address is not sufficient authentication for the other party, either. Similarly, the signatory to the metadata must also be authenticated when using the SAML protocol.

4.8.3 Provision 8.2 Certificate and key renewal

Provision 8.2 stipulates the maintenance of the communications connection trust. The keys implemented in the establishment procedure to ensure confidentiality and integrity cannot be permanently valid; instead, they must be renewed regularly.

The regulation specifies the requirements for key maintenance. The regulation defines boundary conditions for the prerequisites for utilising automated procedures in key renewal.

In the Agency's view, keys should be renewed at least every two years in accordance with good information security practices. Keys must naturally be renewed regularly regardless of this schedule, if their reliability has been compromised due to a security threat or incident.

Subsections 8.2 a–c specify the procedures that can be employed to renew certificates and keys sufficiently reliably. In other words, these procedures are in place to create trust anchors that meet the requirements in provision 8.1. Earlier keys and certificates must, of course, be supported as long as required by the use/implementation of new keys and certificates.

8.2. a) in accordance with the procedure in section 8.1

In the interest of clarity, subsection 8.2.a) states the obvious option to renew keys in accordance with the establishing procedure in section 8.1.

The procedures in sections b and c rely on the trust built during the establishing phase.

8.2 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

The procedure in subsection 8.2 b) is based on trusting the certificate supplied earlier using a bilateral procedure in the establishing procedure and using it to authenticate the communications connection used to supply the new keys. The technical term for this procedure is *secure channel* that can be executed by *certificate pinning or key pinning and mutual TLS (mTLS)*. In terms of the OSI model, the procedure is executed on the transport level.

The procedure is conventional and executable in communications as such, but it is not a default, established procedure in communications connections. The Agency stresses that technical configurations require diligence to prevent software from bypassing this hardening.

Technical application. The Agency states that the public key of the certificate identifies the holder and when the holder connection is bound to this public key, the binding executes the integrity and confidentiality of the communications connection. In other words, it is not sufficient to bind the traffic to CA; instead, it must be executed to a specific certificate or public key. The careful protection and renewal of the certificate used for this purpose is important.

Impact. As far as the Agency is aware, communications connections verified in accordance with subsection b are already being used within the trust network to some extent and the alternative can be assumed to be practically feasible between identification services. This option enables the automation of the renewal of keys used for message protection.

Certificate pinning may be impractical in authenticating communications with relying parties. Instead, *key pinning* or *mTLS* could be feasible and meet the requirements in this case.

In Certificate/key pinning implementation, e-services can typically use affordable DV certificates of the Let's Encrypt type, for example, which may be replaced as often as every three months. Even if trust was established carefully in accordance with provision 8.1, the ensuring of the new certificate being issued to the same pair of keys at the time of the certificate being replaced must be enabled and the earlier key must remain in use in the technical specifications.

In mutual TLS, mTLS, implementations the parties to the communications connection are authenticated by using *client authentication* in addition to using server certificate. mTLS is an alternative method of identifying parties to communications and ensuring information confidentiality and integrity.

The certificate/key pinning or mTLS procedure enabled by the Regulation allows for an automated process in message encryption in key maintenance (JWK set).

TLS connection pinning and mTLS differ from each other in terms of management. In pinned connections, the parties usually acquire their own certificates, but the typical procedure in mTLS use cases is that the other party supplies a client certificate to their client.

8.2. c) by signing for the new keys using a key provided in accordance with section 8.1

The procedure in subsection 8.2 c) is based on trusting the key and certificate supplied earlier using the establishment procedure. The new key is signed with the key supplied earlier. In terms of the OSI model this procedure is implemented on the application level.

This option is not very likely in practice, but the Agency wants to allow it in the Regulation in order to not rule out any implementation that could be based on this.

*Technical application. T*he Agency states that the requirement in the Regulation requires that jwks-uri keys are signed using a signature key supplied in accordance with provision 8.1 when using the OpenID Connect protocol.

This should be technically possible, but the standards do not contain existing specifications for this procedure. In preparing subsection 8.2 c), the Agency has paid special attention to assessing the possibility of implementing automated updates. This procedure could be the signing and encrypting of new jwks keys (when using the OpenID Connect protocol) with qualified keys in accordance with subsection 8.2. c), for example. This is not a hardening requirement for software as such, but would require the construction of an entirely new function in the systems of the relying party. The components related to the specification exist as such, but a compatible implementation would require coordination and co-development.

According to the Agency's understanding, automated renewal may not be possible so that the validation of signatures was bound specifically to an authentication/key entity supplied in accordance with provision 8.1. If, however, it is possible to ensure that the validation is specifically bound to a certificate and key supplied in accordance with provision 8.1, the procedure may meet the requirement in subsection 8.2 c. If this procedure is used, it is important that this is taken into account in specifying and agreeing on the procedures of the identification broker service and relying party.

It is unlikely that relying parties would engage in this type of development work just to specify a procedure that does not exist in the standard, i.e. the development work would need to be conducted in the trust network. If the procedure was not harmonised, interoperability between the identification broker services and relying parties would not be possible. Incoherence and errors would cause a need for repair and guidance processes.

In the Agency's estimate, it is not practical to draft separate specifications on the matter for the trust network, because the procedure contains an evident risk of interoperability issues.

The Agency has not verified whether the SAML standard [50] contains a specification for signing for meta data with manually supplied keys.

4.8.4 Summary of the technical application of provision 8.2.

In the Agency's assessment, at least the following options in compliance with the standard are available:

- Message-level encryption requirement and encryption key exchange in accordance with section 8.1, if a TLS encrypted connection is available with no certificate or key pinning.
- the use of an end-to-end encrypted TLS connection, with certificate pinning or key pinning or mTLS in accordance with 8.1, making message-level encryption optional and providing the option to automate encryption key exchange (JWKS and key rotation)

- Message-level encryption requirement is always valid when the identification messages travel through the user's browser or terminal device (e.g. SAML front-channel)

Message-level encryption is, of course, recommended in all connections that enable it.

4.8.5 Provision 8 objectives and impact assessment

4.8.5.1 Objectives

The purpose of the requirements is to ensure that identification events within the trust network and out of the trust network are only relayed to organisations that have been reliably authenticated. Verifying the relying party is a crucial method of protecting the identification means user from verifying fraudulent identification requests.

The purpose is also to ensure the integrity and confidentiality of communications and messages. Electronic identification must also ensure that communications and messages are genuine and remain confidential.

The purpose is to clarify the requirements and ensure the harmonised use of secure procedures, regardless of identification service. The requirements have proved ambiguous in practice and caused many issues with interpretation as well as varying procedures in terms of security, especially in authenticating relying parties, i.e. e-services.

Specifying the Regulation will clarify and harmonise the procedures, especially with relying parties. In the Agency's assessment, requirements can work to make the procedures employed by some operators more restrictive on the whole, but the objective is to ensure the continual development of identification security and ensure fair competition.

4.8.5.2 Hardening basic standard procedures

Authenticating the parties to communications is a basic part of reliable electronic identification services. Requirements will provide better security than basic procedures of protocols, which trust any digital certificates generally trusted on the internet.

From the point of view of technical development, it must be said that when the TUPAS protocol was used, the practice was to provide the other party with a shared key using a manual procedure in reality in connection with signing the agreement. This procedure allowed for the reliable identification of the other party to the communications and confirmation of the integrity of the transactions.

When starting the use of the OIDC or SAML protocol in standards, the standards would include technically standardised procedures for starting communications with a new party. That is why it is always necessary to assess whether these could be used in authenticating parties to communications connection in connection with strong electronic identification.

The basic procedures of OIDC and SAML protocols are built on established online practices. They enable the establishment of automatic trust, which promotes interoperability and usability, but does not secure the *sufficiently reliable authentication of the party to the trust* or integrity and confidentiality.

Implementing the requirements requires defining processes concerning key and digital certificate provision and various setting determinations in server software in both identification services and e-services.

Assessing the alternatives. During preparation, the alternative that certain certificates that could be trusted without the requirement of the bilateral supply procedure would be specified as an option has been considered. The certificates for website authentication (QWAC) qualified in accordance with the eIDAS Regulation or seal (eSeal) or EV certificates, for example, would however be a cost factor and it would be unlikely that companies would acquire these. The Agency also estimates that this would not secure key management either.

As stated above, in the Agency's view, a single certificate alone will not prove that the pair to the certificate key is in the possession of the correct holder. The certificate holder's key management practices are not covered by the certificate issuing requirements.

The Agency also assesses that even though the CA issuing the certificate and the certificate itself were very reliable, it is quite easy to neglect to ensure that only the certificate in question is approved in the communications connection configuration, as this is not a typical basic function.

4.8.5.3 The difference between the trust network and relying parties

The number of registered identification services is limited, whereas the number of e-services using identification services is large and keeps growing, hopefully. That is why it has been especially necessary to weigh the relationship between usability and security and assess whether there are grounds for e-services to employ different procedures than operators within the trust network.

However, brokering identification to the right e-services is an essential part of the reliability of strong electronic identification. The Finnish Transport and Communications Agency has not identified any grounds for not requiring the establishing of trust for the communications connection between identification broker services and e-services and brokering identification events to be as reliable as communications within the trust network. Neither has the Agency identified any compensating security measures that could achieve the corresponding effect.

As far as technical capability, identification services and the e-services that use them can differ quite significantly. Especially other than large e-service providers can have limited inhouse technical capabilities and they may rely on technical subcontractors in implementing e-services. The following sections contain assessments of the technical requirements of e-services.

4.8.5.4 Establishing trust and key supply

The requirement concerning bilateral procedures in provision 8.1 generates the need to make changes to the establishing of communications connections between identification broker services and their customers, i.e. e-service providers and relying parties.

The Agency's interface recommendations 212 and 213 have included the good practice of trying to avoid deriving trust from generally trusted internet/browser CAs, but during the drafting process of the regulation, it became evident that relying parties are in practice often authorised based on *jwks-uri* described above. The quality of

the certificates used by relying parties varies greatly depending on whether the certificate holder is authenticated based on their own notification or whether the certificate issuer verifies the holder in some way.

See Finnish Transport and Communications Agency recommendation 213/2021 S OpenID Connect Protocol Profile for the Finnish Trust Network [32], section 2.3

The use of extended validation (EV) certificates is RECOMMENDED.

Firstly, the requirement affects how the trust establishment process is implemented. Automated or remote processes would presumably be more cost-efficient. However, identification services are always subject to an agreement that contains provisions on matters related to supply, and this process can also include the reliable supply of keys or certificates.

If the agreement procedure contains a visit in person, the necessary keys can be exchanged at this time.

Typically, agreements on identification services with the relying party are made electronically, which requires the specification of **sufficiently reliable electronic method to supply the public key of the party**. A method specified as secure directly in the eIDAS Regulation has been used as an example in the Regulation. Other methods must be evaluated as an entity that takes the risk of receiving falsified data or receiving data from an incorrect source into account. That is why the electronic identification of the other party is necessary as part of the process, where strong electronic identification offers better reliability than other methods. The integrity of the data transfer channel is another factor to be assessed. It is clear that the security of e-mail alone is insufficient, but different secure e-mail solutions can ensure sufficient integrity and confidentiality, if they have been executed with high quality so that the sender and recipient have been identified and the communications have been encrypted. Other e-services solutions used by the parties, such as secure messaging services for banking or the use of several independent channels, can be used in key supply.

From an *identification broker service's* point of view, the requirements impact the fact that the broker must ensure that technical requirements are communicated to the relying parties it has made agreements with, because it is unlikely that they would be aware of them. In light of the Identification Act, the identification broker service is responsible for supplying identification services to relying parties in compliance with the requirements. Similarly to what has been agreed about data protection obligations (the relying party's right to process personal data disclosed or authenticated to it), the responsibility concerns taking the processing of requirements and any fault situations into account in the agreement and does not result in e.g. the obligation to audit the information systems of relying parties. Naturally, the identification broker service may also offer technical guidance, maintenance and installation services.

The agreement relationship also includes monitoring the validity of the keys in the possession of the relying parties, making sure that they are renewed regularly and the implementation of new keys in the identification service provider's system. In the Agency's assessment, technical checks at least every second year are useful and a good practice as such.

4.8.5.5 Hardening requirements concerning the systems of the relying party, i.e. the e-service

The knowhow of relying parties or their technical subcontractors may also vary, which is why the technical skill requirements resulting from the requirement must also be observed.

Technical feasibility using generally available technical solutions and software, any costs deviating from conventional ICT maintenance and the possibility of faults and human error connected to hardening must be taken into account.

The establishing of new trust and the renewal of certificates and keys during the agreement period must be separated.

Establishing phase. The relying party must be able to observe that the certificate / public key it provides is the exact same key or certificate that will be used in the use of the identification broker service either for the TLS encryption of the communications connection or signing and encrypting the identification requests to the identification broker service on a message level. The processing of a private key bound to a public key in the relying party's system must also be careful enough to prevent it from being disclosed.

The relying party information system hardening requirement to configure the encryption of the TLS connection in accordance with provision 7 so that it only uses certain trusted key pairs is connected to the establishing phase. This requires careful but relatively conventional technical configuration in the software.

If the security of the key update needs to be established in authenticating a TLS connection in accordance with 8.2 b), the TLS connection certificate pinning or key pinning or mTLS should be executed to the key or certificate itself, not the CA. This is a hardening requirement for the relying party in software configurations, which usually trust online CAs.

According to the Agency's understanding, as a procedure, certificate or key pinning or mTLS is completely harmonious with standards as such. Key pinning would probably be a practical procedure in binding TLS connections, because it would enable frequent certificate exchanges, which is characteristic of Let's Encrypt certificates, for example.

This is why these initial phase configurations are essential. Even if the establishing phase was executed carefully, the absence of hardening could result in the carefully selected certificate being automatically replaced with an unverified certificate in connection during updates or the required inspections not being conducted in the communications connection creation phase.

Technical difficulty level of hardening requirements and costs to relying parties. The hardening requirements in the procedures in the above sections 8.1 and 8.2 b are, in the Agency's understanding, relatively easy to achieve as such, but they require that the related processes and maintenance / execution responsibilities are taken into account in the technical maintenance of the party, which naturally requires a deeper understanding of software in addition to basic use. Technical implementations are often the responsibility of a technical subcontractor and the identification is part of a larger ICT entity. These changes will also result in costs for the relying parties. Party authentication and encryption key management incur some costs, but these can likely be considered basic costs of ICT implementation in identification services.

The Agency is of the opinion that the changes are technically feasible and necessary for the continued development of the security of strong electronic identification. However, these requirements need a transition period, especially in relation to e-services, and implementing the changes will require cooperation in guidance and communication.

4.8.6 Provision 8.2, assessment of the technical application alternatives

In preparing provision 8.2, the Agency has also assessed whether the use of DNSSEC could secure the confidentiality of the communications connection and, when using the OpenID Connect protocol, the JWKS-endpoint factor in accordance with the standard as reliably as binding the traffic to a qualified certificate. Generally, DNS-SEC is a good and recommended practice in traffic. Relying on it would have enabled the automated renewal of keys when using OpenID Connect.

However, the Agency assesses that specific technical configuration required by the security of the implementation cannot be ensured sufficiently reliably, especially in the systems of the relying parties. A secure implementation would require the use of DANE and the specification of the application (client) DNS resolver to use DNSSEC technology in the hard fail state. Software support for using DANE may not be readily available in some places. That is why the procedure has NOT been included in the procedure option specified in section 8.2 of the Regulation. (With hardened specification TLS with DNSSEC, JWT Encryption, Rotation of encryption keys (JWKS)).

Cf. Financial-grade API (FAPI) WG [51] https://openid.net/wg/fapi/

4.9 Provision 9 Integrity and confidentiality of authentication messages

4.9.1 Provision 9.1 Protecting messages between identification services and relying parties

The requirements on authentication message encryption from sections 7–9 in the 2016 regulation will be merged with provision 9. The requirements will be specified and amended.

Subsection 9.1. a) will specify an alternative protection procedure to be used instead of message encryption and signatures. It is based on the specific verification of the confidentiality and integrity of the communications connection and is possible, if the messages are not relayed via the user's browser or terminal device. This addition will make the categorical message-level encryption requirement in the 2016 regulation more flexible.

According to subsection 9.1 a), the integrity and confidentiality of authentication messages can be implemented by ensuring the integrity and confidentiality of the communications connection by binding the communications of the parties to certificates supplied in accordance with provision 8 at both ends. This will work to enable the verification of the reliability of the certificate of the end-to-end and both ends of the communications connection and the fact that the traffic will not be unpacked outside the systems intended for providing identification services for the parties.

The procedure and the requirement of reliability concerning the certificate correspond to the stipulations in section 8. Naturally, the underlying assumption is that the communications connection ("TLS pipe") is encrypted in accordance with the requirements in section 7 of the Regulation. If the communication connection is protected and encrypted using IPsec-VPN (virtual private network) instead of TLS encryption, similar procedures related to the confidentiality of messages must be performed on it.

Assessment of alternatives. In the Agency's view, MPLS connections, for example, do not offer sufficient security controls for this purpose, because they do not offer integrity and confidentiality by default. See Pitukri, [26] section SA-02: The Internet as well MPLS networks provided by operators and so-called dark fibre are considered public networks.

Personal data. According to general data protection regulations, all data that can be directly or indirectly connected to an individual person are considered personal data. This also applies to pseudonyms or transaction identifiers that can be connected to a person when compiled/combined from various sources. Of the personal data used for identification, the personal identity code enjoys special protection. The Finnish Transport and Communications Agency does not, however, have objective grounds to restrict any other personal data outside the protection. **This is why the Regulation does not stipulate the protection obligation based on what type of personal data is transmitted in the identification message** ("is minor" cf. " *is 121212+999Å, Alma Virtanen*"). It would be challenging to specify objective and comprehensive grounds for personal data classification and it is easiest to execute technical implementations similarly for all identification events.

4.9.2 Provision 9.1, impact and feasibility

The purpose of this requirement to protect authentication messages is to avoid unauthorised disclosure of personal data in the browser on the user's terminal device or on the servers. The protection methods must protect the authentication messages and personal data against unauthorised disclosure or misuse in connection with any unpacking of the communications 'along the way' on servers or recording without encryption onto the user's terminal device.

Together with the requirements in provision 8, authentication message encryption and signatures also work to protect the identification event from tampering and replay. The protection procedure also works to secure the provision of the verification of the authentication and personal data during authentication only to the correct e-service. This means that there are no grounds to separate the requirement within the trust network and between the trust network and e-services. The requirement applies to connections between identification services and between identification services and relying parties alike.

The requirement in the Regulation remains technically neutral, but the possibilities of executing other protection methods can vary between different protocols (OIDC, SAML, ETSI MSS) and implementations. The purpose of this change is to observe the features of various standards and protocols better than in the valid regulation. The change increases the flexibility of the technical implementation in OIDC executions and also enables the current mobile certificate solutions utilising the ETSI MSS standard [52], which was not evaluated to a sufficient degree in the preparation work for the regulation in 2016. The user's browser is used in connection with SAML implementations, meaning that message encryption must always be used. SAML would also enable other implementations, that are likely not typically used, however.

4.9.3 Provision 9.1.2 Authentication message signatures

Provision 9.1.2 is new to this version of the regulation.

Provision 9.1.2 adds the requirement to sign authentication messages, i.e. the identification requests made by the relying party to the identification broker service and the responses supplied to the relying party by the identification broker service.

The requirement only pertains to authentication messages between the identification broker service in the trust network and the relying party, i.e. identification requests and responses. The purpose is to authenticate the fact that the identification request of the relying party is coming from the correct system and authenticate the SPname attribute displaying the name of the relying party, which must be authenticated by the identification broker service provider in accordance with provision 12.1.

This means that, on the application level, the requirement also pertains to situations where an ensured communications connection in compliance with subsection 9.1 a) is employed on the transport/traffic level. The purpose is to specifically verify the applications that request identification in the relying party's systems.

This requirement will not be specified as mandatory between identification services in the trust network, because the information security of their systems has been assessed on the whole, but it is a good practice to follow there, too.

Impact/feasibility. Signing authentication requests made by relying parties have been discussed in the preparation work for interface recommendations. Based on feedback received during the preparatory phase, it is a generally requested procedure to increase security. This procedure is conventional in terms of technology.

Cf. eIDAS Cryptographic Requirements for the Interoperability Framework, version 1.2 [46]

The specification of the technical requirements of cross-border identification via the national nodes only uses the SAML protocol. In the specification, the signing of messages has been specified as mandatory and the signing and encryption of the content of the message is optional.

> *3.1 GENERAL REQUIREMENTS*
>
> *The following rules MUST apply to the SAML communication between eIDAS nodes:*
> *• SAML request and SAML response messages MUST be signed by the sending party.*
> *• The signature of an SAML assertion is OPTIONAL.*
> *• The (signed) SAML assertion within the SAML response message MUST be encrypted.*
>
> *Ephemeral keys or random numbers (for nonces or generation of ephemeral keys) SHALL be used only once. It is REQUIRED that random numbers to be used within SAML are generated with cryptographically secure random number generators that provide sufficient entropy (according to the security level of 120 bits).*
>
> *3.2 XML ENCRYPTION WITH SAML*
>
> *To protect the confidentiality of data, a hybrid crypto system is used. The content MUST be encrypted via symmetric cryptography (Content Encryption) and the corresponding symmetric key (Session Key) MUST be randomly generated for each transmission. A static public key of the receiver MUST be used to encrypt the session key (Key Encryption).*
>
> *3.2.1 Content Encryption*
>
> *For content encryption, algorithms of the following list MUST be supported:*
> *• http://www.w3.org/2009/xmlenc11#aes128-gcm*
> *• http://www.w3.org/2009/xmlenc11#aes256-gcm*
> *Additionally, the following algorithms MAY be supported:*
> *• http://www.w3.org/2009/xmlenc11#aes192-gcm*
> *Other algorithms than those listed above SHALL NOT be used or accepted for content encryption.*

4.9.4 Provision 9.2 Encrypting messages in the user interface

Provision 9.2 aims at clarifying that the requirements of the Regulation also impact the terminal device interface of a user.

If the user's browser, a service app or a terminal device of some kind is used in relaying the authentication message between the identification service and the relying party, i.e. e-service, the messages must still be encrypted in addition to the encryption of the TLS connection in accordance with section 7.

During the service and identification event, the user's browser or service app connects to the e-service, the identification broker service and the identification means provider. The aim of reliable encryption is to protect personal data throughout the entire process.

Please note that the Regulation does not otherwise apply to the interface between a relying party, i.e. e-Service and a user, but it obliges the providers of the identification means and the identification broker service to implement their identification services in a way which ensures the confidentiality of personal data in the user's terminal equipment interface.

4.9.5 Provision 9.3 Encryption algorithms and procedures

Provision 9.3 refers to provision 7.1, which lists secure algorithms and procedures. Message encryption must utilise certain procedures as far as they are technically applicable. Provision 7.1 has been amended to make it applicable for message-level encryption.

In terms of *technical application*, the Agency states that a good, current practice is to use RSAES-OAEP.

No message encryption application examples have been provided here, but the Agency states that RFC 7519 is a good source for specification, if necessary.

RFC 7519 JSON Web Token (JWT) [53] https://tools.ietf.org/html/rfc7519

> *Support for encrypted JWTs is OPTIONAL. If an implementation provides encryption capabilities, of the encryption algorithms specified in [JWA https://tools.ietf.org/html/rfc7519#ref-JWA], only RSAES-PKCS1-v1_5 with 2,048-bit keys ("RSA1_5"), AES Key Wrap with 128- and 256-bit keys ("A128KW" and "A256KW"), and the composite authenticated encryption algorithm using AES-CBC and HMAC SHA-2 ("A128CBC-HS256" and "A256CBC-HS512") MUST be implemented by conforming implementations. It is RECOMMENDED that implementations also support using Elliptic Curve Diffie-Hellman Ephemeral Static (ECDH-ES) to agree upon a key used to wrap the Content Encryption Key ("ECDH-ES+A128KW" and "ECDH-ES+A256KW") and AES in Galois/Counter Mode (GCM) with 128- and 256-bit keys ("A128GCM" and "A256GCM"). Support for other algorithms and key sizes is OPTIONAL.*

The Agency's OIDC interface recommendation 213 [32] already contains the following instructions on message-level encryption. Corresponding instructions concerning SAML can be found in recommendation 212.

Header	Usage	Value	Algorithm	Status in FTN

alg	**JWS**	**RS256**	**RSASSA-PKCS1-v1_5 using SHA-256**	**REQUIRED**
alg	JWS	PS256	RSASSA-PSS using SHA-256 and MGF1 with SHA-256	OPTIONAL
alg	JWS	ES256	ECDSA using P-256 and SHA-256	OPTIONAL
alg	**JWE**	**RSA-OAEP**	**RSAES OAEP using default parameters**	**REQUIRED**
alg	JWE	RSA-OAEP-256	RSAES OAEP using SHA-256 and MGF1 with SHA-256	OPTIONAL
alg	JWE	ECDH-ES	Elliptic Curve Diffie-Hellman Ephemeral Static key agreement using Concat KDF	OPTIONAL
enc	**JWE**	**A128GCM**	**AES GCM using 128-bit key**	**REQUIRED**

4.10 Provision 10 Information security requirements at the national node interface

A national node means a national interface related to the EU electronic identification interoperability framework. According to the Identification and Trust Services Act, the node is maintained by the Digital and Population Data Services Agency. Cross-border identification with notified identification means referred to in the eIDAS Regulation shall be implemented through national nodes.

According to provision 10, the same encryption requirements shall be followed between the trust network and the national node as in any other external or internal interfaces of the trust network.

Requirements concerning interfaces between national nodes are defined in the document *eIDAS - Cryptographic requirements for the Interoperability Framework, TLS and SAML, Version 1.2, 31 August 2019* [46]

https://ec.europa.eu/cefdigital/wiki/download/attachments/82773108/eIDAS%20Cryptographic%20Requirement%20v.1.2%20Final.pdf?version=2&modificationDate=1571068651805&api=v2

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

4.11.1 Provision 11.1 Significant threats and disruptions (notification threshold)

Provision 11 serves to specify the requirement in section 16 of the Identification and Trust Services Act to notify the Finnish Transport and Communications Agency without undue delay of any significant threat or incident directed at the functionality, data security or the use of electronic identity services.

The Agency has the authority to issue more detailed regulations on when a *disturbance referred to in section 16* is a significant one, and on the *content, form and delivery of the notification* based on section 42 of the Identification Act.

The purpose of the notification is to support the Agency's situational awareness of the reliability, threats and disturbances related to electronic identification services. On the basis of notified information, the Agency assesses whether requirements have been met and whether the situation shall be communicated more widely than the service provider has done. The Finnish Transport and Communications Agency may also provide information for recovery if such information is available.

Provision 11.1 primarily corresponds to subsection 11(2) of the previous regulation. Some clarifications in accordance with the supervision and application practice have been made to the provision. There is no intention to change the notification threshold or the information to be submitted, only clarify the rules.

Section 11.1 of this Regulation defines, at a general level, the factors deemed relevant in judging the significance of the disturbance or threat, i.e. the notification threshold. Such significant disturbances include:

- issuing an identification means to the wrong person
- disturbances related to the functioning of a revocation list in which an up-to-date revocation list is not available
- intrusions in the systems of the service provider
- disclosure of the identification means provider's certificate signature keys
- serious abuse of identification means, such as incidents related to the chaining of identification means
- serious internal misconduct.

The threshold for deeming faults or abuse related to electronic identities significant is very low, and the same applies to vulnerabilities or flaws that compromise the correctness of the identification data. With respect to usability or quality issues, on the other hand, the notification threshold is, in principle, somewhat higher, and they are deemed more significant mainly in the cases where the issue affects other trust network parties. Such issues include extended disruptions in the identification means or identification broker service that prevent the provision of identification services to e-services. Extended disruptions preventing the chaining of initial identification are significant.

On the whole, the Agency estimates that the number of disturbance notifications has increased since 2016. The Agency states that the procedures of operators continue to differ quite significantly in this regard. The Agency states that disturbance notifications may preferably also be submitted voluntarily.

The information provided in the notification submitted to the Finnish Transport and Communications Agency shall be processed in accordance with the Act on the Openness of Government Activities (621/1999), and the information may be disclosed to

third parties or trust network members only when the conditions laid down in the Act are met.

Section 16 of the Identification and Trust Services Act also stipulates that operators are obliged to and have the right to submit notifications on activities between each other. This information may only be pertinent to some members of the trust network. The Act also provides for the Finnish Transport and Communications Agency's possibility to technically transmit notifications between various parties. The Agency does not have a system that would enable, without special technical development, an automatic relay of encrypted information between various parties so that the information would be available to only some trust network members case-specifically. The Finnish Transport and Communications Agency maintains a mailing list that identification services can use to inform each other of disruptions that do not warrant a more information secure channel.

Section 12 a of the Identification and Trust Services Act contains limitations for using the information on disturbances and threats provided within a trust network which aim at lowering the threshold for informing between identification service providers.

4.11.2 Provision 11.2 Reported information

The provision corresponds to subsection 11(1) of the previous regulation.

Provision 11.2 specifies the information that the identification means or identification broker service provider shall include in its notification to the Finnish Transport and Communications Agency. In addition to a description of the disruption or threat, the notification must contain information on the impact on various parties.

The notification should explain when the disturbance or threat occurred and when it was detected as well as the estimated or actual duration of the incident, if known.

The technical incident report should include description of the part of the identification scheme affected by the disturbance or threat, observations on the progress of the events, description of the involvement of any other service providers and details of the cause of the incident.

The notification should also indicate the root cause of the disturbance, i.e. whether the disturbance was caused by a human error, system or software failure, hardware failure, distributed denial-of-service attack, other attack, other threat or natural phenomenon.

If the notification concerns an information security threat, it should specify whether the threat is malware, software vulnerability, data break-in or unauthorised access, certificate or key traffic rerouting or spoofing or other similar incident, for example.

The description of the disturbance or threat and its impact shall specify, for instance, whether it has affected the confidentiality, integrity or availability of data and whether personal data has been compromised.

The notification should also include information on the number of users and e-services affected by the disturbance or threat. It is recommended to also mention in the notification whether the disturbance or threat has affected services or activities that are essential or critical to society.

Furthermore, the notification should include a description of short-term and long-term corrective measures that have been or will be taken to eliminate and mitigate

the effects of the disturbance or threat and to prevent similar situations from occurring.

The notification shall explain how e-services, users and other providers of identification means and identification broker services in the trust network have been informed about the disturbance or threat. The threshold for such communication as well as its contents and time may naturally vary from one party to another. When informing different parties, it is important to consider such parties' ability and need to protect themselves against the effects of the disturbance or threat and minimise these effects.

4.11.3 Provision 11.3 Reporting procedure

This provision is new to this version of the regulation. It is intended to clarify established procedures.

According to section 16 of the Identification and Trust Services Act, the notification must be submitted *without undue delay.* The regulation does not specify any time limits, but the Finnish Transport and Communications Agency recommends that threats and disturbances exceeding the notification threshold in provision 11.1 be notified to the authorities within 1–2 days of their occurrence or detection. The more severe the disturbance, the sooner it should be notified to the Agency.

As a complete set of information on the disturbance is not always available when the disturbance is detected and first corrective measures are taken, it is possible to notify the available details first and supplement the notification later.

A form for reporting disturbances is available on the Finnish Transport and Communications Agency's website. The form can also be used for reporting confidential information, but specific data related to network security should be submitted in some other manner like secure e-mail. The notification may also be submitted via e-mail to eidas@traficom.fi.

In extremely serious and urgent situations the disturbance can also be reported to the Agency by calling: +358 (0)29 390 80. Threats and disturbances whose negative impact on society at large must be prevented quickly by utilising the coordination and communications measures of the National Cyber Security Centre are considered serious and urgent.

4.11.4 Provision 11 Discussed regulation alternatives and other instruments

The responses to the questionnaire on amendment needs to the regulation issued by the Agency contained concerns that not everyone would report disruptions to the Agency with a low enough threshold and that not all identification services would inform each other of disruptions.

The Agency estimates that these observations should be primarily addressed with supervision and by improving information exchange between the members of the trust network. The latter is not covered by the Agency's regulatory authority.

Nor does the Agency consider drafting new, specific notification thresholds for functionality (availability) disturbances that would define a notification threshold based on time or the number of affected users based on feedback. The assessment from 2016 will not be amended. It should also be noted that the Identification Act does not contain specific requirements for the availability, continuity or preparedness of

identification services, meaning that the Agency has no authority to issue provisions on these.

Guidelines, recommendation. No notes.

Co-regulation. The trust network co-operation group has drafted a practice for information exchange concerning disruptions and threats between operators.

Information steering. No notes.

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

4.12.1 Provision 12.1 Mandatory set of data (attributes)

4.12.2 General

This provision specifies the data, i.e. attributes, which shall be relayed in the identification event between the identification means provider and the identification broker service or the relay of which shall be prepared. The attributes correspond to the set of data defined in the EU Commission Interoperability Regulation 2015/1501 [5].

Sections 1–3 of provision 12.1 specify the identification data which the identification means provider shall relay to the identification broker service during an identification event. The Regulation has been clarified by specifying that sections 1 and 2 concern data authenticated by the identification means provider.

The purpose is to ensure interoperability, i.e. that the identification means providers and the providers of an identification broker service may agree on the relay of identification events smoothly without having to specify the attributes separately for each agreement. Another aim is to ensure that domestic identification means may be used in cross-border processes if identification means are notified to the EU.

In an identification event of a natural person, the relayed data includes the unique identifier of the person, which is either the personal identity code (Finnish: henkilötunnus, HETU) or the e-transaction ID (Finnish: sähköinen asiointitunnus, SATU), where this is permitted by the legislation. Parties agree between themselves on the unique identifier to be used. Additional information to be included in the identification data are the first name, family name and date of birth of the person. According to section 7 of the Identification and Trust Services Act, the identification means provider must acquire and update the information they need to identify natural persons from the Population Information System. According to section 6 of the Act, the identification service provider must check the applicant's personal identity code in connection with verifying their identity.

In the identification event of a legal person, at least the unique identifier, family name and first name of the natural person representing the legal person as well as the unique identifier of the organisation shall be relayed. Based on section 7 a of the Identification and Trust Services Act, the identification means provider must acquire and update the information it needs to identify a legal person from the Business Information System.

The assurance level of an identification means employed in the national trust network may be substantial or high, as defined in the eIDAS Regulation. An indication of the assurance level of the identification means shall be relayed at the interface between the identification means provider and the identification broker service.

4.12.3 New attribute: name of the relying party

Information on the relying party verified by the identification broker service, i.e. the name of the e-service, will be added to the mandatory information in subsection 12.1. 4) of the Regulation. In interface recommendations, the attribute is presented as the abbreviation SPname, i.e. service provider name.

The purpose is to add a new way of ensuring the security of electronic identification. The purpose of the attribute is to enable the informing of the user about the relying party, to whom the authentication and personal data will be supplied. Provision 6.2.2 stipulates the obligation to display the information to the identification means user.

The information on the name of the e-service is defined in the relationship between the identification broker service and the relying party. Due to reliability, the responsibility for the attribute must lie with the identification broker service because using information provided by the e-service would defeat the purpose.

On *technical application*, the Agency states that the attribute has already been defined in the interface recommendations, and based on information gathered during the preparatory phase, its execution is technically unproblematic. With regard to the demand, the names used for e-services should be such that the user is likely to identify the service. This means that it is not necessary to use the company name registered in the trade register, if the company uses a better-known name for its service.

The names should be statically specified in advance. Verifying the validity of the names specified dynamically by identification event on the go would require laborious processes and increase the risk of errors due to typing mistakes, for example.

Identification means provider. The initiative for making this attribute mandatory came from the identification means providers during the drafting process. The attribute was previously specified in the interface recommendations, meaning that some identification means providers may already have it specified in their interfaces. In terms of identification means providers, it requires the addition of a field to existing interface definitions and an increased amount of information provided to the users during identification requests.

Subsection 12 a(5) of the Identification and Trust Services Act lays down provisions on the restrictions to the use of information received from the trust network and liability for damages. Based on this, the Finnish Transport and Communications Agency assesses that the identification means provider may not use the information it has received on e-service customers of identification broker services in marketing for its own, competing identification broker service, for example.

Mandatory attributes are covered by the maximum price regulation concerning identification events specified in section 12 b of the Identification and Trust Services Act, but price regulation concerns information produced by the identification means provider, meaning that regulation bears no significance in this case.

Identification broker service. The identification broker service generates the SPname attribute (relying party, to whom the identification is being relayed). Agreements must regardless be made with the e-services, meaning that the specification of a service name within the agreement relationship should not incur significant extra costs. In addition to content specification, this change requires that a field is added to existing interface specifications. The attribute has been specified in the interface

recommendations, meaning that some identification broker service providers may already have it specified in their interfaces.

E-services/relying party. Together with the identification broker service, the e-service must specify a name for their service to be informed to the user. This has no significant economic impact.

Other steering instruments

Guideline. Based on observations from supervision and feedback from the questionnaire, the Agency assesses that the implementation of the attribute in all identification services might not necessarily happen based on an instruction alone, but requires binding regulation.

Recommendation. The attribute is already included in the Agency's interface recommendations [31, 32]. Its status has been changed to mandatory in the update in 2021.

Co-regulation. Information on observations concerning the specification of names of e-services and the displaying of the information to the users can be exchanged in the trust network, when necessary.

Information steering. No notes.

4.12.4 Provision 12.2 Optional set of data

Provision 12.2 lays down stipulations on optional set of data. The attributes correspond to the optional data defined in the EU Commission Interoperability Regulation 2015/1501 [5].

There is already a need for cross-border identification, and demand is increasing also in the private sector. The purpose of optional attributes is to support identification and transactions in situations where mandatory attributes are not sufficient in checking whether a person is already registered with the service (*identity matching, identity linking*).

In amendment to the regulation from 2018, subsection 25(4) of the Regulation provided for a transition period for the plan on implementing the changes required for relaying the optional attributes referred to in subsection 2 in the interface used in the trust network. *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.* At that time, the explanatory notes specified what plan was referring to in the regulation.

The specification that the plan must be *technically planned* from the transitional provision has been added to provision 12.2.

Being prepared to relay optional attributes means that the processing of optional attributes in the interface and identification schemes must be designed in a way where the identification service provider knows which technical measures are needed for the introduction of the attributes. Technical planning requires the documentation of the plan.

Technical implementation of optional attributes in systems is not required. However, in the technical configurations, it should be ensured that the optional attributes will not impede identification events, even in those cases where their use has not been agreed upon.

The Finnish Transport and Communications Agency is of the view that preparedness should be improved gradually, and by taking into account the development schedules of company systems. In the first phase, it suffices that the attributes are taken into account in designing the identification scheme. The Agency estimates that the planning process will accelerate implementation when need arises. The Agency's SAML and OIDC interface recommendations can be then referred to. The attributes do not need to be implemented in the systems until a need for them arises.

4.12.5 Provision 12.3. Pseudonymisation of identification ("impoverish")

This provision is new to this version of the regulation. Its purpose is to clarify attribute requirements in the interface between the identification means provider and identification broker service if the relying party, or e-service, is only provided with a so-called impoverished confirmation of user authentication.

According to section 8, subsection 2 of the Identification and Trust Services Act, *the provisions of subsection 1 do not prohibit offering a specific service in a way that the identification service provider discloses to the service provider using the identification service the pseudonym of the identification means holder or only a limited amount of personal data*.

The act or this regulation do not lay down provisions on which personal data is provided to the relying party or authenticated through strong electronic identification. The regulation specifies the attributes that are processed in authentication within the trust network. Typically, the relying party will be provided with e.g. a name and personal identity code, but as described in the act the relying party may also be provided with a pseudonym or a limited amount of personal data. This also requires strong authentication of the user and the data concerning the identification event must be stored in accordance with section 24 of the act.

The term pseudonym is used instead of alias in the regulation because as far as regulation concerning personal data is concerned, these are pseudonymised personal data in the Agency's assessment. Even if the data were anonymous from the point of view of the relying party insofar as the relying party may not be able to connect the data to a certain person, the data can be connected to a specific person based on the data saved by identification services.

The pseudonym may be single-use or more permanent depending on how the identification service has been productised. The relying party may also be supplied with e.g. proof of the user's age of majority. The relying party could also be supplied with the user's address or some other individual piece of personal data or set of personal data without the personal identity code or the authentication of the personal identity code that could identify the user as a person.

In the Finnish Transport and Communications Agency's assessment, offering identification services impoverished in the described manner could increase the events in which strong electronic identification and secure services are used also in situations where the relying party does not have the right or need to reliably authenticate the user's identity, only some other piece of information. Based on information received during the preparatory phase, pseudonymisation and impoverishing would be technically quite trivial, but there seems to have been no particular interest in these services thus far. In order to promote interoperability, it might be necessary to specify shared profiles in the trust network between identification means and broker services.

The provision of such services has not come to the attention of the Agency, but for the sake of comparison, seemingly the only thing authenticated using strong electronic authentication in payment card transactions between the payer and the recipient of the payment is that the payer is the holder of the card in question, and no personal data is transmitted between payment services.

The user should be informed of their personal data being processed in the trust network and the personal data provided to the relying party in accordance with the GDPR.

Other steering instruments

Guideline. No notes.

Recommendation. Harmonised practices could be specified in the interface recommendation issued by the Finnish Transport and Communications Agency, if necessary.

Co-regulation. The trust network could share information on the implementation of impoverishment and draft shared models, if necessary.

Information steering. No notes.

4.12.6 Provision 12 Alternative regulation considered

4.12.6.1 New optional attributes

It was reviewed during the drafting process of the Regulation whether there was a need to add citizenship, country of birth, city of birth, country of residence, telephone number and/or e-mail to the optional attributes of natural persons. It was further discussed whether there was a need to add telephone number and/or e-mail to the optional attributes of legal persons.

The attributes mentioned are being discussed in the technical cross-border identification eIDAS group. The attributes would promote the interoperability of cross-border identification and the possibility to connect a person to any previous personal data in the e-service in the country, where the identification is received.

The attribute sources and the possibilities of reliably verifying them vary. The attributes could be assigned different reliability levels.

The additional information can be acquired, authenticated and offered by the identification means provider or the identification broker service.

Section 12 b of the Identification and Trust Services Act refers to the Commission Implementing Regulation (EU) 2015/1501 [5] in terms of identification data processed in strong electronic identification. The processing grounds for any other personal data than the data mentioned above and obligations related to data protection should be assessed and managed based on the GDPR.

Attributes that are not included in the Commission Implementing Regulation are not covered by the price regulation specified in section 12 c of the Identification and Trust Services Act.

According to an estimate within the branch, the number of attributes is expected to increase as Self Sovereign Identity (SSI) models develop, and it is important that

this development is not hindered. The current operating model, however, does not pose any acute needs. A market survey conducted in 2020 did not indicate that e-services had any identified needs for new attributes either.[2]

Decision. The Agency shall not make any additions, because there is no conceivable need for new optional attributes that would necessitate the promotion of their definition in regulation at this time.

Other steering instruments

Guideline. No notes.

Recommendation. In order to enable interoperability, optional attributes and their presentation methods can be listed in interface recommendations.

Co-regulation. The trust network may exchange information concerning the e-services' attribute needs, if necessary.

Information steering. Interoperability requires harmonised interface specifications. Information on the attributes available in different identification services alone is not a practical method of specifying an interoperable list of attributes and method of presentation in a multi-operator environment.

4.12.6.2 Initial identification attributes

In the drafting process of the Regulation in 2016, hopes concerning long-term evolution and the possibility to relay details of the initial identification via the interface (such as the document on which the initial identification in person was based: a passport, an identity card, electronic identification) were expressed.

It has now been re-evaluated during the drafting process whether there is a need to add information transmitted during the chaining of initial identification from a qualified identification means to the Regulation.

An amendment of section 17 of the Identification and Trust Services Act enabled identification means providers to chain identification operations indefinitely, i.e. issue new electronic identification means by relying on electronic identifications provided by others.

The interface recommendation issued by the Finnish Transport and Communications Agency contains the attribute *FTN chain level* specified for the initial identification event. This is displayed in the identification request submitted by an identification means provider to another. The provisions don't preclude relaying the request and identification for the issuing of a new identification means also through an identification broker service. During the drafting process, the Agency suggested that some information related to trusted identification means would be specified as mandatory

[2] See Traficom Research Reports 2/2021 Sähköisen tunnistamisen markkinat (the electronic identification market), Sähköinen tunnistaminen turvallisen asioinnin mahdollistajana (electronic identification enabling secure services), section 5.2 Yritysten tarpeet (company needs), Sähköisten asiointipalvelujen näkemyksiä tulevaisuuden tarpeista (electronic identification service views on future needs), p. 53 Lähes kaikki eli 98 prosenttia näkemyksensä antaneista vastaajista pitää vahvan sähköisen tunnistamisen yhteydessä saatavia tietoja riittävinä (Nearly all of the respondents who provided their opinion, i.e. 98 per cent, consider the information received during strong electronic identification sufficient).

in the Regulation. According to an initial assessment by the Agency, from the perspective of information security and the overall reliability of electronic identification, the transfer of such information would be beneficial. Due to price regulation, the chaining of initial identification is expected to increase.

When information security breaches are investigated, it is important that possible chaining can be found out quickly and efficiently in one manner or another. If, for example, an identification means provider issues identifiers on the basis of stolen or fake IDs, it must be possible to find out whether such electronic identification means in the possession of the wrong person have been used to electronically apply for new identification means.

Necessary information could include e.g. information on the time when the identification means was issued and whether the qualified identification means was issued based on a document proving the person's identity (passport, identity card or driving licence prior to 2019) or based on strong electronic identification. In terms of the chaining of initial identification, the Agency questioned whether any earlier identification chains were necessary and suitable for transmission.

According to an initial assessment by the Agency, the identification scheme would technically contain the necessary information, because storing the information concerning initial identification is mandatory according to section 24 of the Identification and Trust Services Act. This means that implementing the requirements would require the drafting of interface definitions to the interface recommendation in addition to the Regulation and the related changes to the interfaces and use of data bases of the identification means providers.

Details of the performance of the initial identification and the parties belonging to the chain would support risk assessment and management in the view of the Agency. Pursuant to section 17(4) of the Identification and Trust Services Act, the identification means issuer that relies on the identification means of another provider shall bear the liability for damages. For this reason, chaining requires that the means issuer who uses chaining shall evaluate the risk potentially associated with the trusted identification. This risk is affected by the following factors (quote from the 2016 assessment): how long ago and on the basis of which ID the original personal identification was carried out, whether there are several identification means issuers in the chain, whether any of the identification means issuers in the chain have discontinued its operations, and whether any of the identification means issuers in the chain have experienced information security breaches that may have affected the integrity of data.

During the drafting process, identification service providers presented the unanimous opinion that covering the cost of specifying new attributes with the regulated initial identification maximum price of 3 cents would take long. They also stated that there are only a few instances of error investigation and the implementation costs would exceed the benefits of investigating errors and that acquiring, recording and transmitting data would require development. The harmonised specification of understandable data would be laborious. Similarly to 2016, identification services suggested that a database on initial identification chaining (i.e. identification means issued to users), maintained by an authority, such as the Digital and Population Data Services Agency, would implement the security objectives and enable the closing of all chained identification means.

Decision. Not regulated. The Finnish Transport and Communications Agency has taken the operators' grounds and the fact that, based on disruption notifications submitted to the Agency, disruptions related to the chaining of initial identification occur seldom, into account. The Agency also considers the monitoring of the possible impact of the ongoing Government Digital identity development project on electronic initial identification to be practical.

Other steering instruments

Guideline. No notes.

Recommendation The Finnish Transport and Communications Agency monitors any disruptions and, when necessary, assesses whether it would be useful to specify the information transmitted during the chaining of initial identification as optional in the interface recommendations. Based on feedback received during the drafting process, however, it is unlikely that identification services would broker the attributes voluntarily.

Co-regulation. The trust network disruption group can exchange information and specify the procedures of investigating disruptions, if necessary.

Information steering. No notes.

4.13 Provision 13 Information required in cross-border use

4.13.1 Identification in the public sector

The objective of the eIDAS Regulation is that, in the future, it will be possible to use identification means notified by Member States, such as Finland, for identification in foreign public administration e-services, while notified foreign identification means may be used for identification in Finnish public administration e-services.

Provision 13 pertains to situations where a Finnish identification service has been notified to the Commission in accordance with the eIDAS Regulation and the identification means user identifies in a public sector e-service in another Member State using their identification means. Identification using a Finnish identification means would take place via an identification means provider, an identification broker service and the national node maintained by the Digital and Population Data Services Agency.

Provision 13 stipulates that the trust network should at this time transmit the data specified in provision 12 to the node. In cross-border identification, identification in public administration e-services should not be subject to a fee between Member States according to the eIDAS Regulation, but in private e-services, the eIDAS Regulation and its implementing acts allow to collect compensation for the use of the identification means. For this reason, it must be possible to relay data of whether the identification event relates to a public administration e-service or a private e-service also across this interface.

According to provision 10 concerning the interface between the broker service provider and the node, the same general requirements as those pertaining to the interface between the identification means provider and identification broker service are applied to the interface. The other properties of the interface are subject to a mutual agreement between the broker service provider and the node operator in accordance with provision 14. However, it would be appropriate that the chosen protocol is one of the protocols used in the trust network.

Identification using a foreign notified identification means to a Finnish public sector e-service takes place via the national node and suomi.fi. This is not discussed in the Regulation.

4.13.2 Identification in the private sector

Subsection 13(2) of the earlier regulation on attribute processing in situations where foreign identification means notified in accordance with the eIDAS Regulation would be used to identify to a private sector e-service in Finland through the node and the trust network will be removed from the Regulation.

However, there are no harmonised EU or national specifications concerning the use of the national node for identifying to *private e-services*. Cross-border identification to public sector e-services is implemented through the national node, but the Digital and Population Data Services Agency has not executed or planned the transmission of foreign identification to private e-services. This means that the provision in the Regulation is unnecessary. The matter will be reviewed, if required by future changes to the eIDAS Regulation.

Customers using foreign identification means can be identified by Finnish private sector e-services on the basis of an agreement, similarly to identifying to a foreign private e-service using a Finnish identification means. The reliability of a foreign identification service could be found indirectly based on notification, on the basis of regulation and supervision of the home state of the identification service, if any, or on the basis of an agreement.

When an identification broker service belonging to the trust network wishes to relay strong identification to foreign services, the same requirements for the interface and the contractual relationship between the identification broker service and the foreign e-service apply as in the case of domestic e-services. In this event, regulation and monitoring carried out by the Finnish Transport and Communications Agency meet the requirements for identification brokering specified in the Identification Act and the regulation. The interoperability and security requirements for cross-border identification laid down in the eIDAS Regulation (EU) 2015/1501 [5] only apply to the national node.

4.14 Provision 14 Data transfer protocol and other requirements

4.14.1 Provision 14.1 Data transfer protocol

The provision has been specified by naming OpenID Connect and SAML as the standards, one of which the interface offered by the identification service must at least comply with between identification means providers, i.e. for chaining initial identifications and between the identification means and the identification broker service.

The purpose of the provision is to specify the requirements concerning interoperability and interface characteristics specified in sections 12 a and 17 of the Identification and Trust Services Act and the Government Decree on trust networks and limit the number of the standards for the interfaces that the identification services are prepared to maintain must comply with in order to avoid or receive identification data during initial identification or identification brokering for relying parties.

In the provision, *enabling* means interpreting the requirement from the point of view of the rights of the identification means provider or identification broker service, which the Act and the Decree aim to secure. The identification service may fulfil its obligations in the trust network also by offering the function through an identification

service in another trust network, as long as the requirements laid down in the provisions and regulations are fulfilled.

According to responses to the Finnish Transport and Communications Agency questionnaire 2020 on the amendment needs of the Regulation, the technical steering of interface protocols does not need to be changed significantly. The responses to the survey supported the Agency's preliminary assessment that the informative provision should remain in section 14. It remains practical to execute a more specific steering of interfaces using a recommendation. There were, however, some critical comments concerning the efficiency, or rather inefficiency, of recommendations in promoting interoperability.

The Finnish Transport and Communications Agency recommends the use of the nationally drafted profiles for the SAML 2.0 or Open ID Connect protocols, which the Agency has published as separate recommendations in 2018 and updated in 2021 [31, 32]. Special nationally stipulated or regulated requirements for interface executions are specified in recommendations. Otherwise, good general practices must be applied to compliance with the standards.

This freedom of contract is affected by the regulations within the Identification and Trust Services Act and the Government Decree on the trust network. According to section 12 a.3 of the Identification and Trust Services Act *[i]dentification service providers must collaborate to ensure that the technical interfaces of the members of a trust network are interoperable and that they enable the provision of interfaces that implement commonly known standards to the relying parties.*

According to section 1.1 of the Government Decree on trust networks (169/2016, amended as 1212/2018) [2], *the technical interfaces referred to in section 12 a(2) of the Identification Act (this reference is not updated, but the matter is stipulated in 12 a(3) in the Act after the change to section 12 a in the Act) are*

1) the interface between providers of identification means,
2) the interface between an identification means provider and identification broker service provider and
3) the interface between an identification broker service provider and the party relying on the identification service.

Pursuant to section 1.3 of the Decree, *an identification service provider belonging to a trust network shall, in both the interfaces referred to in subsections 1(1) and 1(2), provide at least one technical interface that meets a universally applied standard.*

The following issues were evaluated in the preparatory phase for the regulation in 2016: *What is the degree of precision for interface requirements to be included in the Regulation with respect to individual protocols, such as SAML and Open ID Connect? In other words, shall there be room for the use of other protocols? How should the purely national TUPAS protocol be taken into account, since it does not, in all respects, meet the requirements, and its development plans or potential remained unclear during the preparation of the Regulation?*

It was decided during the drafting process of the regulation in 2016 that the *protocols to be applied shall not be determined, but shall be negotiated between the various parties*. *However, the end result to be achieved through the application of the protocol shall be determined; that is, the minimum data that the protocol must allow to be transferred and the information security requirements of the interface.*

The Tupas protocol was discontinued after 2016, at least in strong electronic identification, and mobile operators have replaced the old ETSI mobile verification interface with the OpenID Connect interface in some interfaces. As it is, OpenID Connect is the prevalent protocol, but SAML is also used to some extent.

4.14.2 Provision 14.2 Other features of the interface

The provision corresponds to section 14 of the previous regulation.

The purpose of the provision is to clarify the fact that the parties to the trust network and relying parties agree on the protocol and the characteristics of the interface that have not been regulated together. Freedom of contract has been restricted by regulating attributes and protocols within the trust network. Freedom of contract has been restricted with relying parties in terms of the interface security requirements.

4.14.3 Adopting new protocol standards in the trust network

Based on information received during the drafting process and the monitoring of the branch, the Agency estimates that there is no current need to discuss certain new protocols in any more detail in technical steering. It seems that OpenID Connect and SAML enable the development of identification services within the trust network to a sufficient degree. ETSI is used to some extent in interfaces between mobile certificates.

If the need to adopt new protocols as a *technical interface in accordance with a generally used standard* specified in the Government Decree on trust networks should arise, preparatory information should be exchanged in the co-operation group of the trust network specified in the decree and the Agency should evaluate the maturity of the technical development based on objective information available both nationally and internationally.

The interface and architecture needs for enabling Self Sovereign Identity highlighted by the Findy group during the drafting process are not yet sufficiently clear or established internationally ('according to a generally used standard' in the Government Decree on the trust network) that they could be observed in the regulation or technical steering or that this would be practical. The matter will be re-evaluated if changes to EU or national regulation or technical development require it.

4.14.4 Provision 14 Alternative regulation considered

4.14.4.1 The interoperability requirements impacting relying parties

The Finnish Transport and Communications Agency has investigated whether the technical specifications of the trust network are connected to factors that have an impact on identification brokering to relying parties during the drafting process.

According to section 12 a of the Identification and Trust Services Act, *identification service providers must collaborate to ensure that the technical interfaces of the members of a trust network are interoperable and that they enable the provision of interfaces that implement commonly known standards to the relying parties.*

Here, the Finnish Transport and Communications Agency has paid attention to the identification means use restrictions in accordance with section 18 of the Identification and Trust Services Act and the inspection opportunity that the identification means provider must arrange for relying parties.

No needs connected to relying parties were highlighted in the questionnaire on the amendment needs of the Regulation in 2020 or during the drafting process, with the exception of single sign-on.

The Finnish Transport and Communications Agency is not aware of any functions whose enabling should or could be promoted with the regulation to promote interoperability with relying parties. The boundary conditions and information secure execution of single sign-on affecting the services received by relying parties are discussed in provision 6.2.3. and identification pseudonymisation in provision 12.3.

4.15 Provision 15 Conformity assessment criteria

4.15.1 Provision 15.1 Identification scheme and identification means features to be assessed

The provision corresponds to section 15.1 of the previous regulation. The provision specifies the conformity assessment criteria stipulated in section 29 of the Identification and Trust Services Act.

All requirements set in the act and in this regulation. The provisions clarify the fact that the assessment must cover all of the requirements set for the functions to be assessed in the Identification and Trust Services Act and the Regulation. The Identification and Trust Services Act also refers to the sections of the EU Electronic Identification Assurance Level Regulation referenced in the Act. Information security and interoperability requirements are specified especially in chapters 2 and 3 of this Regulation.

The provision lists the functions of identification service implementation and provision for which the compliance with the requirements of the regulatory framework shall be demonstrated by either an internal or external assessment. The grouping of functions or areas is based on grouping in the EU Commission Assurance Level Regulation. The assessment of interoperability related to the national regulation of trust networks will be added to the Regulation.

A detailed assessment and guideline on which stipulated and regulated requirements the assessment requirement pertains to is presented in the Identification service assessment guideline 211/2019. Section 3 of the guideline lists the relevant provisions by area and Annex B General assessment criteria for identification services itemises the requirements by area.

The sections of subsection 15.1 1) of the provision cover the following matters.

Information security management means the requirements in provision 4 of the Regulation, which specify the requirements in subsection 5 of section 8.1 of the Identification and Trust Services Act and introduction 2.4 and sections 2.4.3 and 2.4.7 in the Annex to the Assurance Level Regulation.

Record keeping and other *data processing* has been combined into one entity in the Regulation and the guideline.

Facilities and staff mean premise security and staff competence and sufficiency in accordance with subsection 8.1(5) and section 13 of the Identification and Trust Services Act and section 2.4.5 in the Annex to the Assurance Level Regulation.

Technical measures, or controls, contain comprehensive information security measures that are used to ensure the integrity and confidentiality of the identifica-

tion scheme and identification means. In addition to information system, communications and operation security, this entity contains cryptographic solutions and incident detection, management and information. Stipulations on the information security of the identification scheme are laid down in paragraph 4 of section 8.1 of the Identification and Trust Services Act and sections 2.2.1, 2.3.1 and 2.4.6 of the Annex to the Assurance Level Regulation. Disturbance notifications are stipulated in section 16 of the Act. Chapter 2 of the Regulation concerns technical measures.

Interoperability within the trust network includes attribute transmission and interfaces. Chapter 3 of the Regulation concerns interoperability.

Relationship to the information security management system. It must be noted in conformity assessment that information security and risk management in accordance with provision 4 is not sufficient to meet the material requirements of the identification scheme. Instead, the identification scheme must meet all aspects of the stipulated and regulated technical requirements. In terms of conformity assessment, this means that the evaluation of information security management alone is not sufficient to demonstrate the fulfilment of the specified requirements, but it must be specifically assessed whether the scheme meets the encryption requirements for communications, for example.

The point of view in the ISO 27001 standard, for example, differs significantly from the assessment criteria in the Identification and Trust Services Act and this Regulation. Information security management systems certified using ISO standards or specified otherwise create an administrative layer and a framework for data processing and service management. Certification as such does not demonstrate the sufficiency of the information security and data protection level or existence of technical information security measures in the individual services or the entire service offering of an organisation.

Cf. LOA guidance, section 2.4 [22]

> *A general principle in risk management is that it is up to the organisation to choose which level of risk it finds acceptable. This general principle is modified by the requirement in 2.4, since the organisation should have controls that are commensurate to the risks at the given level.*

The sections of subsection 15.1 2) of the provision cover the following matters. It should be noted that this is a description of the requirements on a general level and various special circumstances must be assessed in light of the act and its rationale. Differentiating between different measures is not unambiguous when only one of the authentication factors is renewed, for example.

Application and registration mean the application procedure of an identification means and the collection and verification of personal data required for identification in accordance with sections 6 and 7 of the Identification and Trust Services Act.

Identity proofing and verification of the applicant mean the initial identification of an identification means applicant in accordance with section 17 of the Identification and Trust Services Act, including the verification of the authenticity of qualified IDs and their validity in accordance with section 7 b in the Act.

Identification means characteristics and design mean the selection of the authentication factors used in the means, and the features of the factors and authentication mechanism that ensure the reliability of the means as a whole in accordance with

sections 8 a and 8.1(4) of the Identification Act and section 2.2.1 and 2.3.1 in the Annex to the Assurance Level Regulation.

Issuance, delivery and activation of the identification means mean procedures and measures in accordance with sections 20 and 21 of the Identification and Trust Services Act and section 2.2.2 of the Annex to the Assurance Level Regulation, which are used to bind the identification means to the holder, providing it to the holder and taking it into use.

Suspension, revocation and reactivation of the validity means blocking services and measures in accordance with sections 25 and 26 of the Identification and Trust Services Act on the initiative of the holder or the identification service.

Renewal and replacement means providing a new identification means to replace a previous means in accordance with section 22 of the Identification and Trust Services Act and section 2.2.4 of the Annex to the Assurance Level Regulation. This provision may also be connected to the application of section 26 of the Act.

Authentication mechanism means the authentication procedure of the holder of the identification means using dynamic authentication in accordance with section 8 a of the Identification and Trust Services Act and section 2.3.1 of the Annex to the Assurance Level Regulation. The requirements of the authentication mechanism pertain in part to the identification broker service, too, when it participates in relaying messages in the authentication.

4.15.2 Provision 15.2 Assessment criteria

This provision will be clarified to have it better describe the purpose and established supervision practices.

According to section 29 of the Identification and Trust Services Act, *in addition to the provisions in subsections 1 and 2 above and provisions or guidelines issued by the EU or another international body, the Finnish Transport and Communications Agency may order the assessment to be based on published and generally or regionally applied information security guidelines or widely applied information security standards or procedures*.

The Agency will not regulate certain sources as grounds. Instead, the regulation will specify the boundary conditions for the criteria used in conformity assessment. A reference to the assessment guideline issued by the Finnish Transport and Communications Agency, whose current version at the time of the preparation of the regulation is 211/2019 [21], will be added to the Regulation. The guideline was updated thoroughly in 2019 to accommodate all the regulated requirements and include special criteria concerning mobile applications. The up-to-date version of the guideline should be used to observe all of the requirements.

Other sources that may be used in the assessment include information security standards which specify good information security practices and concretise details to be taken into account in the assessment. Examples of these are listed below.

Identification service providers may meet the assessment requirements set out in the provision by means of one or several assessments of their choice. There may also be several assessment bodies. Requirements concerning the independence and competence of assessment bodies are laid down in section 33 of the Identification and Trust Services Act, and the requirements are further specified in sections 18 and 19 of this Regulation.

An identification service provider who acquires the assessment must ensure that also the requirements concerning expressly the identification scheme and the identification means are taken into account in the assessment, regardless of the fact that the service production and management environment is often only a part of the overall production and management environment and the assessment might target this environment at large.

The objective is to enable operators to utilise those sets of assessment criteria that they would otherwise use flexibly. On the other hand, parties need to estimate and ensure that their set of criteria that are based on different standards indeed cover all the required areas of identification scheme assessment and their requirements.

4.15.3 Examples of assessment sources

Standards or sources that can be applicable to identification scheme assessment as part of the assessment.

- ISO/IEC 27001 [11]
- KATAKRI [12]
- PiTuKri [26]
- PCI DSS, PCI/QSA [20]
- Webtrust Trust Services Principles and Criteria for Certification Authorities and Webtrust for Certification Authorities – SSL Baseline Requirements Audit Criteria [54]
- Information Security Forum (ISF) Standard of Good Practice [55]
- ISF IRAM criteria (Information Risk Analysis Methodology) [55]
- ISRS 4400 [56] and ISAE 3000 [57]
- Vahti instructions [58]
- Information Management Board recommendations [59]
- European Central Bank instructions
- Regulations or instructions issued by the Finnish Financial Supervisory Authority[60]
- FIN-FSA regulation and guideline 2.4 'Customer due diligence; Prevention of money laundering and terrorist financing'[61]
- European Central Bank SREP cyber risk questionnaire [62]
- BIS, Bank for International Settlements, ohjeet External audits of banks and supplemental note to External audits of banks - audit of expected credit loss [63]
- Swedish Finansinspektion (FFFS) and Finnish Financial Supervisory Authority regulations and instructions concerning the organisation and operations of internal auditing
- IIA, The Institute of Internal Auditors [64] instructions, rules and auditing principles
- ETSI standards [66, compiled trust service links]

4.15.4 Alternative instruments to the Regulation and Agency assessment guideline

Recommendation/guideline. The Finnish Transport and Communications Agency electronic identification service assessment guideline 211/2019 [21] was updated thoroughly in 2019 to accommodate all the regulated requirements and include special criteria concerning mobile applications. The intention is to maintain the guideline so that the use of the current version covers all stipulated requirements.

Co-regulation. From the perspective of market entry threshold and possible competition law issues, it is better that the authority is responsible for setting minimum

requirements. Exchange of information on the application of different sets of criteria and interpretation issues is compatible with co-regulation.

Informative guidance. No notes.

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

4.16.1 Reports related to the identification service's notification obligation

For the sake of clarity, the sections related to the reliability of the identification service provider and the statutory information published by it that are not covered by the independent and qualified conformity assessment specified in provision 15 have been compiled in the provision.

The provision is related to the notification obligation of the identification service provider to the Finnish Transport and Communications Agency stipulated in section 10 of the Identification and Trust Services Act. Based on section 42 of the Identification and Trust Services Act, the Agency has the authority to stipulate *the content of the notification referred to in section 10 and the delivery of the notification to the Finnish Transport and Communications Agency.*

This means that the identification service provider must provide information and reports to the Finnish Transport and Communications Agency in connection with commencement or changes of operations or if the Agency otherwise requests information in connection with its task of supervising identification services.

The Regulation does not provide exhaustive stipulations on the information to be submitted or the form of the reports. The Regulation provides general provisions stating that the fulfilment of these requirements may be demonstrated in the form of a report provided by the company or another applicable report or assessment.

Guidelines and instructions on notifications and reports are provided on notification forms and notification guideline as well as in the form of operator-specific guidance, if necessary.

4.16.2 Content of the information

The phrases of the regulation are partially based on sections 2.4 Management and organisation and especially 2.4.1 General provisions and 2.4.2. Published notices and user information of the Electronic Identification Assurance Level Regulation. Corresponding requirements are also included in the Identification and Trust Services Act. The title and phrasing of the Regulation has been clarified, the order of the sections has been changed and some specifications have been made to the content with regard to the notification obligations of the identification service provider.

1) *an established legal person in charge of the identification service and the competency and reliability of the persons in charge* The requirements in this section are connected to the requirements in section 9 of the Identification and Trust Services Act. The identity of a legal person may, for example, be demonstrated by presenting an extract from a register and the trustworthiness of the persons in charge can be established by written declarations provided by the persons or from applicable sources.

2) *published notices and user information, such as identification principles, data protection principles, use restrictions, price lists and terms and conditions.* The requirements in this section are connected to the requirements in sections 12 b, 14, 15 and

18 in the Identification and Trust Services Act. The reliability of published data is established by presenting the publication locations and published information.

3) *sufficient financial resources in order to organise operations and cover any liability for damages*. The requirements in this section are connected to the requirements in section 13 of the Identification and Trust Services Act. Financial resources and the ability to assume the risk of liability for damages is established by providing financial statements, the balance sheet and an auditor's report as well as any proof of liability insurance.

4) The requirement in section 4 is connected to the requirements in section 13 of the Identification and Trust Services Act. The *responsibility for subcontractors* is also specified in the conformity assessment specified in section 15, but it is also included in the conformity of the identification service management. Key subcontractors should also be mentioned in the identification principles in accordance with section 14 of the Act.

5) The requirement in section 5 is connected to the requirements in section 13 of the Identification and Trust Services Act. The purpose and content of the plan is described in section 2.4.1 5 of the Electronic Identification Assurance Level Regulation: *Electronic identification schemes not constituted by national law shall have in place an effective termination plan. Such a plan shall include orderly discontinuations of service or continuation by another provider, the way in which relevant authorities and end users are informed, as well as details on how records are to be protected, retained and destroyed in compliance with the scheme policy.*

4.16.3 Agency notification guideline

FICORA's Guideline 214/2016 O on electronic identification and trust service notifications [65] specifies some of the information or annexes which shall be submitted to the Finnish Transport and Communications Agency. However, there are no detailed application instructions concerning such information. The required content shall be assessed on the basis of the preparatory materials for the Identification and Trust Services Act, for instance.

4.17 Section 17 National node assessment criteria

This provision is mainly informative. The Commission Implementing Regulation (EU) 2015/1501 [5] refers to information security management based on standard ISO/IEC 27001 [11] as the default. The Regulation confirms this presumption, because it is an appropriate practical solution also for the Digital and Population Data Services Agency. The Commission Implementing Decision lays down certain requirements for the operation of a node.

4.18 Provision 18 Requirements concerning an external assessment body of the identification service

In the commencement or change notification to be submitted to the Finnish Transport and Communications Agency in accordance with section 10 of the Identification and Trust Services Act and its annexes, the supervisory authority shall be provided the details of the independent assessment. Furthermore, the notification shall include other information, on the basis of which it is possible to confirm that the party performing the assessment meets the requirements of section 33 of the Identification and Trust Services Act concerning the independence and competence of an assessment body.

The assessment body performing the audit may, under section 29 of the Identification and Trust Services Act, be an internal assessment body, other external assessment body or an accredited conformity assessment body.

The purpose of the provision is to clarify the criteria for determining the independence and competence of an assessment body in a predictable manner. The provision also seeks to clarify that the independence and competence of an assessment body cannot be based on the party's own set of rules or own consideration. Instead, they must be objectively justified.

Provision 18.1 lists examples of the international standards or regulatory or self-regulatory frameworks on which the independence and competence of an assessment body may be based. The list is not exhaustive, and paragraph 1(5) states general conditions for demonstrating independence and competence. The purpose is to enable parties to apply, as flexibly as possible, the audit criteria that they are already using.

Examples of possible assessment bodies are bodies accredited according to ISO 27001, other external ISO 27001 audit bodies or corresponding auditors based on other relevant standards.

Provision 18.2 implies that a condition for applying various standards or sets of rules to independent and competent identification scheme assessments is that the assessment actually concerns the requirements of the identification scheme. It is the responsibility of the identification service provider to ensure that this is actually the case and that the assessment covers all areas defined in this Regulation.

The assessment report must clearly show that the audit actually concerned the requirements of the identification scheme.

4.19 Provision 19 Requirements concerning an internal assessment body of the identification service

The explanation for the provision is identical to that of provision 18. Similarly, the independence and competence of an internal assessment body cannot be based on the party's own set of rules or own consideration. Instead, they must be objectively justified and legitimately applicable to the assessment of identification scheme requirements.

Chapter 6 Qualified trust services

4.20 Provision 20 Assessment criteria for a qualified trust service provider

4.20.1 General information on trust service regulation and standards

The general aim of regulation concerning trust services is to build the information society and increase confidence in e-services. The regulation concerning trust services helps the providers and users of electronic services identify the services that enable the implementation of the various e-service functions with the highest possible standard of information security.

The eIDAS Regulation [3] specifies the requirements that a provider of a qualified trust service and trust services shall meet. To define these requirements, the European Telecommunications Standards Institute ETSI has drafted standards concerning trust service providers under the Commission's mandate [66]. If trust service

providers meet the exact concrete requirements of the standards, they are compliant with the eIDAS Regulation.

The purpose of the Regulation is to clarify the requirements for qualified trust services laid down in the eIDAS Regulation by referring to international standards on which the EU preparatory work is based, inasmuch as these standards have not, at least by now, been referred to in the Commission implementing acts, even if the eIDAS Regulation would provide legislative competence to that effect.

References to standards in the Regulation also support what is to be taken as the minimum level of competence requirements in the accreditation of potential conformity assessment bodies.

The standards are not mandatory, and operations may be organised in other ways. However, the standards indicate the level of confidence required by the eIDAS Regulation. If other standards with similar requirements are applied, the service provider shall specifically demonstrate that the operations meet the requirements of the eIDAS Regulation. The Regulation refers to the standards that had already been completed when the Regulation was issued.

The Regulation will be supplemented with references to standards that have been completed after the previous regulation was issued.

ETSI standards are directly applicable in Finland and they have also been approved as SFS standards. Therefore, these standards are named as SFS-EN 319 401, for example.

Enisa has drafted an assessment of eIDAS standards: Enisa Assessment of Standards related to eIDAS (14 December 2018)[67] https://www.enisa.europa.eu/publications/assessment-of-standards-related-to-eidas

4.20.2 General and service-specific requirements for qualified trust service providers

4.20.2.1 Provision 20.1.1 General requirements for qualified trust service providers

ETSI EN 319 401 V2.2.1 (2018-04) Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers [66]

The standard includes general requirements for all providers of qualified trust services that apply regardless of the service. It contains requirements concerning risk assessment, information security policies and practices as well as management and operation, for example.

4.20.2.2 Provision 20.1.2 Additional requirements for qualified certificate issuers

References to standards concerning qualified trust service providers issuing certificates have been compiled in one provision, which pertains to the issuing of qualified certificates.

ETSI EN 319 411-1 V1.2.2 (2018-04) Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements [66]

The next version of ETSI EN 319 411-1 V1.3.0 (2021-02) is in the process of being approved.

The standard includes general requirements for trust service providers issuing certificates. It supplements and specifies the requirements of standard EN 319 401. The standard contains detailed requirements for certificate policies and practices. Informative Annex C (Conformity Assessment Checklist) to the standard contains a checklist of the requirements of the standard. The checklist may be used, for example, when auditing trust service providers.

ETSI EN 319 411-2 V2.2.2 (2018-04) Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates [66]

The next version of ETSI EN 319 411-2 V2.3.0 (2021-02) is in the process of being approved.

The standard contains requirements for trust service providers issuing qualified certificates referred to in the eIDAS Regulation. It supplements the requirements provided in standard EN 319 411-1 so as to correspond with the special requirements of the eIDAS Regulation. The supplementary requirements concern certificate policies and practices, among others.

Informative Annex B (Conformity Assessment Checklist) to the standard contains a checklist of the requirements of the standard. The checklist may be used, for example, when auditing trust service providers.

4.20.2.3 Provision 20.1.3 Additional requirements for qualified time-stamp issuers

ETSI EN 319 421 V1.1.1 (2016-03) Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Electronic Time-Stamps [66]

The standard contains information security policy and information security requirements for trust service providers issuing electronic time-stamps. The standard mainly refers to the requirements of standard EN 319 401 but it also specifies them to some extent. The standard contains detailed requirements for TSU (Time-Stamping Unit) management. Informative Annex H (Conformity Assessment Checklist) to the standard contains a checklist of the standard's requirements. The checklist may be used, for example, when auditing trust service providers.

4.21 Provision 21 Assessment criteria for a qualified trust service

4.21.1 Qualified trust service types

The following types of services can be qualified trust services in accordance with the eIDAS Regulation (EU) 910/2014 [3]:

1) Qualified certificate for electronic signature (Article 28)
2) Qualified validation Service for qualified electronic signature (Article 33)
3) Qualified preservation Service for qualified electronic signature (Article 34)
4) Qualified certificate for electronic seal (Article 38)
5) Qualified preservation Service for qualified electronic signature (Article 40)

6) Qualified preservation Service for qualified electronic seal (Article 40)

7) Qualified time stamp (Article 42)

8) Qualified electronic registered delivery Service ("eDelivery"/QERDS) (Article 44)

9) Qualified certificate for website authentication (QWAC) (Article 45)

The qualification is acquired in accordance with Articles 20 and 21 of the eIDAS Regulation.

4.21.2 Standards

The Regulation specifies the assessment criteria for qualified trust services.

Annexes I, III and IV to the eIDAS Regulation define the requirements for qualified certificates for electronic signatures, electronic seals and website authentication.

To define these requirements, the European Telecommunications Standards Institute ETSI has drafted the standards referred to in this Regulation under the Commission's mandate. If a trust service meets the exact concrete requirements of the standards, they are compliant with the eIDAS Regulation.

The standards are not mandatory, and services may be organised in other ways. However, the standards indicate the level of confidence that the eIDAS Regulation requires for services. If a service is organised according to one of these standards, the requirements of the eIDAS Regulation will be followed. If other standards with similar requirements are applied, the service provider shall specifically demonstrate that the service meets the requirements of the eIDAS Regulation.

The certificate profiles listed in this Regulation include a standard for general requirements (EN 319 412-1), standards in accordance with the intended application of the certificate (EN 319 412, sections 2–4) and a standard specifying the contents of qualified certificates (statements) (EN 319 412-5).

Insofar as the standards separate the parts concerning the compliance with the requirements of EU regulation and other requirements, the requirements of EU regulation are considered applicable to this Regulation.

Standards concerning qualified trust service providers and various trust services have been compiled in the following table. Technical specifications (ETSI TS) have not been confirmed as of yet, and will not be referenced in the Regulation.

Table: Standards for qualified trust service providers and trust services

References to standards are compiled in the list of references, completed standards [66] and technical specifications [68]

Service, eIDAS Article	complete standard	technical specification

qualified trust service provider (all trust service types)	ETSI EN 319 401	see ETSI TS 119 312 V1.3.1 (2019-02)[47]
trust service provider offering certificates (all qualified certificates)	ETSI EN 319 411-1 ETSI EN 319 411-2	
Certificates for electronic signatures Article 28	ETSI EN 319 412-1 ETSI EN 319 412-2 ETSI EN 319 412-5	
Certificates for electronic seals Article 38	ETSI EN 319 412-1 ETSI EN 319 412-3 ETSI EN 319 412-5	
Certificates for website authentication (QWAC) Article 45	ETSI EN 319 412-1 ETSI EN 319 412-4 ETSI EN 319 412-5	
Time stamp Article 42	ETSI EN 319 421 ETSI EN 319 422	
validation of electronic signature Article 33	ETSI EN 319 102-1	ETSI TS 119 441 ETSI TS 119 442 ETSI TS 119 102-2 ETSI TS 119 172-4
validation of electronic seal Article 40, reference to Article 33	ETSI EN 319 102-1	ETSI TS 119 441 ETSI TS 119 442 ETSI TS 119 102-2 ETSI TS 119 172-4
Preservation of electronic signatures Article 34		ETSI TS 119 511 ETSI TS 119 512
Preservation of electronic seals Article 40, reference to Article 34		ETSI TS 119 511 ETSI TS 119 512
Electronic registered delivery services (eDelivery) Article 44	ETSI EN 319 521 ETSI EN 319 522 1-4	ETSI TS 119 524

Chapter 7 Conformity assessment bodies of trust services

4.22 Provision 22 Evaluation of the competence of assessment bodies

4.22.1 Accreditation and approval

The status of a conformity assessment body requires that the meeting of independence and competence requirements specified in section 33 of the Identification and

Trust Services Act is demonstrated through an accreditation to be applied from FINAS [69].

The provision specifies the competence requirements for conformity assessment bodies specified in section 33 of the Identification and Trust Services Act.

When FINAS makes a decision on the assessment body accreditation criteria referred to in the Act on Verifying the Competence of Conformity Assessment Services (920/2005), it may take into account other requirements concerning the assessment of independence and competence in addition to the standards referred to in this Regulation.

In addition, the body shall apply for approval by the Finnish Transport and Communications Agency. A prerequisite for approval is the FINAS accreditation and a declaration on how the guidelines in section 33(1)(4) of the Identification and Trust Services Act will be followed.

The following figure describes the relationships between general accreditation regulation and the sectoral supervision of the eIDAS Regulation in the conformity assessment of an electronic trust service. The image does not include the approval and supervision role of the conformity assessment body (CAB), which is nationally regulated in the Identification and Trust Services Act as the task of the Finnish Transport and Communications Agency. In the image, the specifications to the regulation are connected to the Accreditation Scheme which is decided by the National Accreditation Body, which is FINAS in Finland.

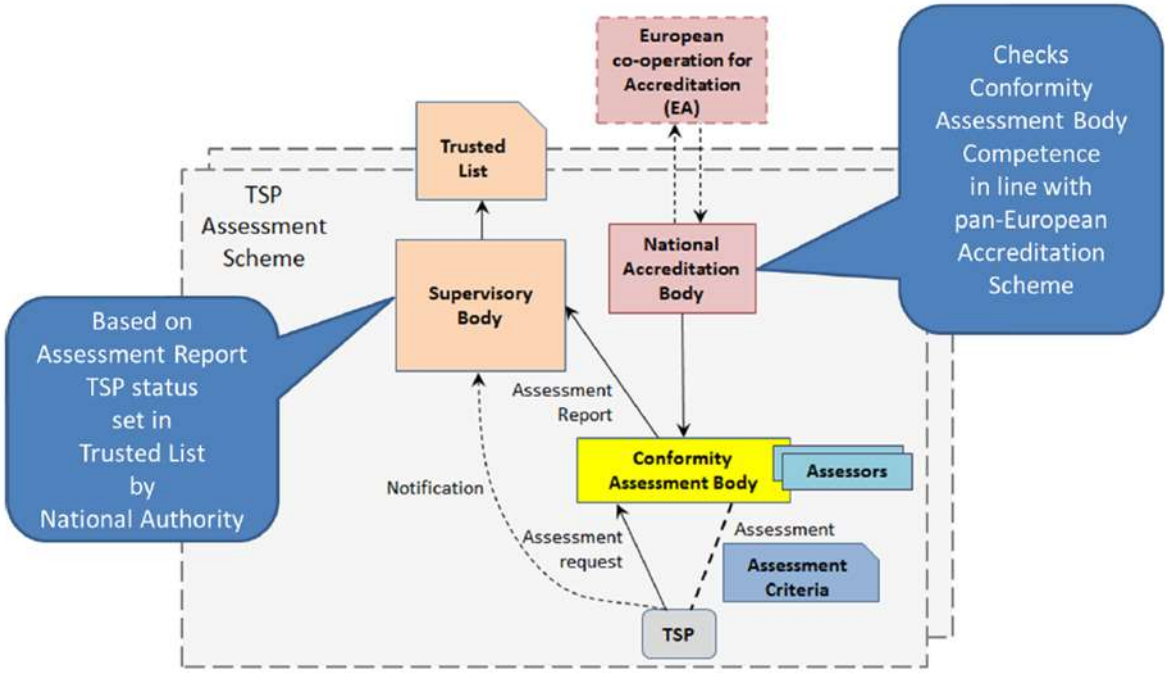

Image: Trust service provider assessment scheme

(Source: European Union Agency for Network and Information Security (ENISA): *Auditing Framework for TSPs, Guidelines for Trust Service Providers, Version 1.0 - December 2014* [70])

4.22.2 Standard

The Commission has not drafted an implementing act to specify the conformity assessment body standards under Article 20.4 of the eIDAS Regulation.

Since the Commission has not issued an implementing act on this issue, the standards listed in the EA document and described in the following paragraph form the basis for the accreditation and approval of conformity assessment bodies. Some Member States have confirmed their own requirements.

The European accreditation co-operation body EA (European Co-operation for Accreditation) prepared the document *EA Certification Committee Reference Paper; ETSI / EA Recommendations regarding; Preparation for Audit under EU Regulation (EU) No 910/2014 Article 20.1* .[71] in 2015. It defines how, in the accreditation of Conformity Assessment Bodies (CAB), the move from the earlier practice to the practice defined in the eIDAS Regulation shall take place, which requirements the assessment bodies are expected to meet in the accreditation, and in which matters they are expected to be competent. The document is based on ETSI standards.

Requirements concerning Conformity Assessment Bodies have been defined in the standard *ETSI EN 319 403-**1** V2.3.1 (2020-06) Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment - Requirements for conformity assessment bodies assessing Trust Service Providers* [72].

The standard is based on standard ISO/IEC 17065 that defines general requirements for assessment bodies. Standard EN 319 403 complements the requirements of the ISO/IEC standard, particularly with regard to requirements concerning trust service providers and the services provided by them.

Part 2 on the assessment of certificate issuers has been added to the standard. Part 2 has not been confirmed as of yet, it is only a technical specification (TS). This is why the standard is not stipulated as a reference, but it can be applied.

*ETSI TS 119 403-**2** V1.2.1 (2019-04) Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment; Part 2: Additional requirements for Conformity Assessment Bodies auditing Trust Service Providers that issue Publicly-Trusted Certificates* [73]

Under the Identification and Trust Services Act, conformity assessment bodies shall be competent to assess service providers and their services. Provisions 20 and 21 of the Regulation specify the assessment requirements for trust service providers and trust services which means that conformity assessment bodies shall be competent for assessment in accordance with the standards referred to in the sections.

4.22.3 Assessment report

Part 3 has been added to ETSI standard 119 403, in which the assessment report is standardised. Part 3 has not been confirmed as of yet, it is only a technical specification (TS).

*ETSI TS 119 403-**3** V1.1.1 (2019-03) Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment; Part 3: Additional requirements for conformity assessment bodies assessing EU qualified trust service providers* [74]

The Finnish Transport and Communications Agency's authority to issue regulations specified in section 42 of the Identification and Trust Services Act does not apply to

trust service conformity assessment reports, only the assessment criteria. This is why the standard is not stipulated as a reference, but the assessment body may apply it.

The Finnish Transport and Communications Agency has issued guideline 215/2019 *Assessment reports on qualified eIDAS trust services* [75]. The content of the guideline on trust service assessment corresponds to the content of guideline 215/2016.

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

4.23 Provision 23 Electronic signature or seal creation device certification body

4.23.1 Competence requirements

Provisions 23 and 24 from the previous Regulation have been merged.

If a Finnish certification body wants to become a designated certification body, it may apply for approval by the Finnish Transport and Communications Agency in accordance with section 36 of the Identification and Trust Services Act under the conditions laid down in this section.

Provision 23 stipulates how statutory competence can be demonstrated. Possible ways include at least accreditation, which means a competence assessment by FINAS, or participation in a peer review based competence assessment procedure of the SOGIS-MRA agreement.

SOGIS-MRA (Senior Officers Group for Information Systems, Mutual Recognition Agreement) [38] is a European scheme for the mutual recognition of certifications. The members include eight countries (*qualified/authorising participants*) with their own certification bodies and two countries (*consuming participants*) with no certification bodies (including Finland).

Competence as a certification body requires that the operator has the ability to authenticate the requirements of the creation device which have been laid down in the Commission Implementing Decision (EU) 2016/650 [8].

Certificates issued by certification bodies that have been designated and notified to the Commission by EU or EEA Member States are also valid in Finland as such. Currently the majority of certification bodies notified to the Commission are also included in the SOGIS-MRA agreement.

4.23.2 Standards

The requirements are based on the Commission Implementing Decision (EU) 2016/650 [8].

The decision (EU) 2016/650 contains references to standards concerning creation devices based on possession. CEN standards for remote creation devices have been approved in the standardising procedure, but their addition to the Commission Implementing Decision is only pending at the time of the drafting of these explanatory notes.

Of the standards confirmed in the Commission Implementing Decision Annex, the general IT information security assessment standard series ISO/IEC 15408 Information technology -- Security techniques -- Evaluation criteria for IT security [23] is also known as the Common Criteria.

Chapter 9 Transitional provisions and signatures

4.24 Provision 24 Regulation entry into force and transitional provisions

The intention is for the Regulation to enter into force in April 2022.

The Regulation enters into force on DD Month 2022.

4.24.1 Transition period for provisions 6.2 and 12.1

The transitional provision for section 6.2.1 of the provision, i.e. the transition period for the displaying of the event identifier, means that the information must be displayed to the identification means user in identification events on X October 2022, at the latest.

Identification service providers are able to meet this requirement and relying parties are not expected to take any measures. Many identification services already use this feature. The implementation requires that identification means providers perform technical specifications to create in the background system a character string, QR code or some other message that is displayed in the service during the browser session or in the application as well as in the confirmation request displayed in the identification means. In the Agency's estimate, the required technical specifications are relatively minor, but the transition period is required in order to provide sufficient time to plan and execute the necessary specifications.

The transition period for sections 6.2.2 and 12.1. 4) of the provision, i.e. displaying the name of the relying party, means that the name of the relying party must be displayed to the user on x October 2022, at the latest.

The fulfilment of this requirement requires measures from both identification services and relying parties, to some degree.

The identification broker service and the relying party must agree on the names to be displayed. This is discussed in section 4.12.3 of the explanatory notes.

Provision 9.1.2 is also connected to displaying the name of the relying party, as it requires that the relying party signs an identification request. The key used for the signature and the transition period for provision 9.1.2 are stipulated in provision 24.4.

Implementing the requirement requires technical specifications in the interface of the identification broker service and the identification means provider to transmit data. The attribute has already been specified in the interface recommendations and it has been made mandatory in the update in 2021. The recommendation has been prepared in close cooperation with operators. This means that the preparedness for interoperability is good.

Implementing the requirement requires technical specifications in the confirmation request displayed in the identification means. This primarily pertains to identification means providers, but if the identification broker service presents the identification

means user with information in the intermediate phases of the event, the presentation of this information requires that the identification broker service also takes some measures.

In the Agency's assessment, the required technical specifications are relatively minor. Some identification services have already executed this feature. In the Agency's assessment, the transition period is necessary in order to execute technical specifications and in order for the identification broker services to have the opportunity to agree on the displayed names with relying parties, if they have not yet been agreed on.

4.24.2 Transition periods for provision 8

The transition period for subsection 24.3 a) means that it must be ensured that the communications connections between identification services in the trust network use a certificate supplied in accordance with provision 8.1 by X October 2022.

The transition period for subsection 24.3 b) means that the identification broker service must use a procedure in compliance with provision 8.1 when it adds new e-service customers to its identification scheme on X October 2022, at the latest.

The transition period for subsection 24.3. c) means that the identification broker service must identify those e-service customers that the identification broker service has added to its identification scheme without identification in accordance with section 8.1 on x April 2023, at the latest. The certificate or key must be replaced in accordance with provision 8.1. The transition period means that the entire previous set of agreements must be made compliant with the new requirement on X April 2023, at the latest, regardless of when the agreement was originally made.

The requirement in the provision concerning the implementation of requirement 8.2 on X April 2023, at the latest, means that starting from this date, the certificates and keys must always be updated in compliance with the requirements in the provision.

Implementing the requirements requires the specification of procedures and processes in identification and key and certificate exchange as well as the specification of the process in the exchange cycle. Implementing the requirements in terms of technology requires various setting configurations in server software in both identification services and e-services.

The number of trust network identification services is limited and the services have the technical capability to meet the requirements. However, planning will require some time and some time should also be reserved for information exchange concerning procedures, so that they may be harmonised within the trust network, if necessary.

In terms of the identification broker service, the requirements impact the fact that the service must ensure that technical requirements are communicated to the relying parties makes or it has made agreements with, because it is unlikely that they would be aware of them.

The technical requirements in provisions 8.1 and 8.2 for e-services are evaluated in section 4.8.5.5. The hardening requirements for e-service systems required by the procedures also require that any processes and maintenance and implementation responsibilities are observed in the technical maintenance of the e-services and any subcontracting. In the Agency's assessment, the procedures can be implemented for

new customers as soon as the identification broker service adopts them and an e-service acquires an identification service. However, existing contract customers have already integrated the manner of using the identification service in their production and they must make changes to the maintenance of it. Considering that the identification broker service must first plan its own processes and inform e-services about upcoming changes, this requires a longer transition period. In the Agency's understanding, ICT projects are typically planned and acquired in cycles and the projects are combined.

In the Agency's assessment, as the critical factor is communication and awareness of changes and their content and not a technically demanding matter, the planning and production of the changes can be executed in one year in e-services. Naturally, this requires that identification services and authorities communicate the upcoming changes and their content actively.

4.24.3 Transition periods for provision 9

The transitional provision concerning the new procedure in subsection 9.1.1 a) means that the alternative procedure for message-level encryption can only be adopted when it is able to employ a certificate or key in compliance with the requirements in section 8.1.

The transition period for message signatures specified in the provision means that encryption and signing must be executed using keys in accordance with provision 8 by the time they must be employed in accordance with the transition periods in provision 8. During the transition period, message-level encryption can continue to use the keys that were in use prior to the provision entering into force. Messages may also be signed using these keys until the old keys have been replaced. Signing messages is not mandatory before the transition period has ended, however.

5 Appendices and references

5.1 References

Provisions connected to the Regulation are available in the Finlex Data Bank or EurLex and have been marked with an asterisk* in the list.

The Finnish Transport and Communications Agency's guidelines and recommendations are available on the Finnish Transport and Communications Agency website and they have been marked with two asterisks ** in the list. References to legislation have also been compiled on the website.

General links
Electronic identification | National Cyber Security Centre
Electronic signatures and other eIDAS services | National Cyber Security Centre

ETSI standards are available on ETSI's website and they are marked with three asterisks *** in the list of references.

- General search link with query 'Electronic Signatures': https://portal.etsi.org/TBSiteMap/ESI/ESIActivities.aspx

[1] * Act on Strong Electronic Identification and Electronic Trust Services (617/2009 as amended, **the Identification and Trust Services Act**) 617/2009 - FINLEX ®

[2] * Government Decree on the trust network of strong electronic identification service providers 169/2016, amended 1212/2018 (‘**Government Decree on trust networks’**) https://www.finlex.fi/fi/laki/smur/2016/20160169

[3] * REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (‘**eIDAS Regulation’**) EUR-Lex - 32014R0910 - EUR-Lex (europa.eu)

[4] * COMMISSION IMPLEMENTING REGULATION (EU) 2015/1502 (**EU ASSURANCE LEVEL REGULATION**) ON SETTING OUT MINIMUM TECHNICAL SPECIFICATIONS AND PROCEDURES FOR ASSURANCE LEVELS FOR ELECTRONIC IDENTIFICATION MEANS PURSUANT TO ARTICLE 8(3) 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 EUR-Lex - 32015R1502 - EN - EUR-Lex (europa.eu)

[5] * COMMISSION IMPLEMENTING REGULATION (EU) 2015/1501 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 EUR-Lex - 32015R1501 - EN - EUR-Lex (europa.eu)

[6] COMMISSION IMPLEMENTING DECISION (EU) 2015/1984 (‘EU notification procedure decision’) defining the circumstances, formats and procedures of notification pursuant to Article 9(5) 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

[7] * COMMISSION IMPLEMENTING DECISION (EU) 2015/296 (‘**EU cooperation network decision**’) establishing procedural arrangements for cooperation between Member States on electronic identification pursuant to Article 12(7) 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

[8] * 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 (note: applies to so-called QSCD certification) EUR-Lex - 32016D0650 - EN - EUR-Lex (europa.eu)

[9] * REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (**General Data Protection Regulation**)

[10] * Data Protection Act (1050/2018)

[11] ISO/IEC 27001 Information security management

[12] KATAKRI, Information Security Audit Tool for Authorities, Traficom's publication series 232/2020 https://um.fi/information-security-auditing-tool-for-authorities-katakri and Katakri 2020 (um.fi)

[13] SFS-ISO 31000:2018 Riskien hallinta. Ohjeet. ISO 31000 Riskienhallinta | SFS (in Finnish)

- In English ISO 31000:2018(en), Risk management — Guidelines

[14] ISO/TR 31004, Risk management – Guidance for the implementation of ISO 31000, and International Standard/ISO/TR 31004:fi [14]

- In English ISO - ISO/TR 31004:2013 - Risk management — Guidance for the implementation of ISO 31000

[15] ISO/IEC 31010, Risk management – Risk assessment techniques ISO - IEC 31010:2019 - Risk management — Risk assessment techniques

- SFS-ISO/IEC 31010 Product (sfs.fi)

[16] SFS-ISO/IEC 27005:2018, Information technology — Security techniques — Information security risk management Product (sfs.fi)

- In English ISO - ISO/IEC 27005:2018 - Information technology — Security techniques — Information security risk management

[17] VAHTI Ohje riskienhallintaan (VAHTI Risk management guideline, in Finnish), Ministry of Finance publications 22/2017, https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/80013/VM_22_2017.pdf?sequence=1&isAllowed=y

[18] NIST Risk Management Framework (RMF) https://csrc.nist.gov/projects/risk-management/about-rmf

- NIST, (National Institute of Standards and Technology) www.nist.gov

[19] FIPS 140-3 Security Requirements for Cryptographic Modules, https://csrc.nist.gov/publications/detail/fips/140/3/final

- FIPS, FIPS standards (Federal Information Processing Standards) www.nist.gov

[20] PCI Security Standards, incl. PA-DSS (Payment Application Data Security Standards) Official PCI Security Standards Council Site - Verify PCI Compliance, Download Data Security and Credit Card Security Standards

[21] ** Finnish Transport and Communications Agency guideline 211/2019 O Assessment guideline for electronic identification services https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/regulation/O211_Assessment_guideline_for_electronic_identification_services_211_2019_O_EN.pdf

[22] Assurance Level Regulation (EU) 2015/1502 application guideline (LOA Guidance 2021) https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/LoA%20guidance%20%282021%29.pdf

- Finnish translation of the 2016 version https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/LOA_Guidance_Final_suomeksi.pdf [2021 translation added when complete]
- LOA Guidance 2021 https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/LOA_Guidance.pdf
- Cooperation network https://ec.europa.eu/cefdigital/wiki/display/EIDCOMMUNITY/Cooperation+Network+Resources

[23] ISO/IEC 15408 Information technology – Security techniques – Evaluation criteria for IT security ('Common Criteria')

- *www.commoncriteriaportal.org/cc CCPART1-3 equivalent to standard ISO/IEC 15408*

[24] ISO/IEC 18045 Information technology – Security techniques – Methodology for IT security evaluation

- *www.commoncriteriaportal.org/cc CEM equivalent to standard ISO/IEC 18045*

[25] ISO/IEC 29115 Information technology — Security techniques — Entity authentication assurance framework ISO - ISO/IEC 29115:2013 - Information technology — Security techniques — Entity authentication assurance framework

[26] ** Criteria for Assessing the Information Security of Cloud Services (PiTuKri), Traficom publication 13/2020 https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/PiTuKri_v1_1_english.pdf

[27] ITU-R TF.1876 (03/2010) Trusted time source for time stamp authority https://www.itu.int/dms_pubrec/itu-r/rec/tf/R-REC-TF.1876-0-201004-I!!PDF-E.pdf

[28] NIST 800-63B, Digital Identity Guidelines, Authentication and Lifecycle Management https://pages.nist.gov/800-63-3/sp800-63b.html

[29] NIST, Face Recognition Vendor Test (FRVT) https://www.nist.gov/programs-projects/face-recognition-vendor-test-frvt21]

[30] * Act on the Provision of Digital Services (306/2019) 306/2019 - FINLEX ®

[31] ** Finnish Transport and Communications Agency recommendation 212/2021 S, Finnish Trust Network SAML 2.0 Protocol Profile, Doc no. Traficom/6194/09.02.00/2020 7 July 2021 [link to be added]

[32] ** Finnish Transport and Communications Agency recommendation 213/2021 S, OpenID Connect Protocol Profile for the Finnish Trust Network, Traficom/6194/09.02.00/2020, 7 July 2021 [Link to be added]

[33] * DIRECTIVE (EU) 2015/2366 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/1001/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC (**PSD2**, Payment Services Directive) EUR-Lex - 32015L2366 - EN - EUR-Lex (europa.eu)

[34] * COMMISSION DELEGATED REGULATION (EU) 2018/389 supplementing Directive (EU) 2015/2366 of the European Parliament and of the Council with regard to regulatory technical standards for strong customer authentication and common and secure open standards of communication (‘**RTS SCA & CSC’**) EUR-Lex - 32018R0389 - EN - EUR-Lex (europa.eu)

[35] * Maksupalvelulaki 290/2010 (Act on payment services, in Finnish) 290/2010 - Säädösmuutosten hakemisto - FINLEX ®

[36] Assessment material

- Slides 2018 eIDAS ja PSD2/RTS -tarkastelu (eIDAS and PSD2/RTS review, in Finnish)https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Kalvot%2010102018%20PSD2-seurantaryhm%C3%A4%20eIDAS-%20ja%20PSD2-RTS-vaatimusten%20vertailu.pdf
- Statement version 10102018 Vivin ja Fivan eIDAS-PSD2-RTS -vaatimusten vertailu (säännösecxel) (Comparison of requirements in eIDAS, PSD2 and RTS by Traficom and FIN-FSA, in Finnish) https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Lausuntoversio%2010102018%20Vivin%20ja%20Fivan%20eIDAS-PSD2-RTS-vertailu.XLSX

[37] NCSA-FI, National Communications Security Authority of the Finnish Transport and Communications Agency

- General NCSA-FI information https://www.kyberturvallisuuskeskus.fi/en/our-activities/ncsa

[38] SOGIS-MRA (Senior Officers Group for Information Systems, Mutual Re-cognition Agreement), http://www.sogisportal.eu/

- General information on SOGIS MRA https://www.sogis.eu/uk/supporting_doc_en.html#:~:text=The%20document%20%C2%AB%20SOG%2DIS%20Crypto,by%20all%20SOG%2DIS%20participants

[39] ** Kryptografiset vahvuusvaatimukset luottamuksellisuuden suojaamiseen - kansalliset suojaustasot (ohje 28.11.2018, dnro 190/651/2015) (Cryptographic strength requirements for protecting confidentiality - national protection levels (Guideline 28 November 2018 Doc no. 190/651/2015)) https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/regulation/ohje-kryptografiset-vahvuusvaatimukset-kansalliset-suojaustasot.pdf

[40] IANA (Internet Assigned Numbers Authority)

- IKEv2 parameters http://www.iana.org/assignments/ikev2-parameters/ikev2-parameters.xhtml
- cipher suites: http://www.iana.org/assignments/tls-parameters/tls-parameters.xhtml#tls-parameters-4

[41] SOG-IS Crypto Evaluation Shceme Agreed Cryptographic Mechanisms, (version 1.2 January 2020) https://www.sogis.eu/documents/cc/crypto/SOGIS-Agreed-Cryptographic-Mechanisms-1.2.pdf

[42] RFC 7905 ChaCha20-Poly1305 Cipher Suites for Transport Layer Security (TLS) https://tools.ietf.org/html/rfc7905

[43] RFC 8446 The Transport Layer Security (TLS) Protocol Version 1.3 https://datatracker.ietf.org/doc/html/rfc8446

[44] NSCA-FI -toiminnon hyväksymät salausratkaisut (1.7.2020 dnro 1240/651/2017) (Encryption solutions approved by NSCA-FI (1 July 2020 Doc no. 1240/651/2017), in Finnish) https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/NCSA_salausratkaisut.pdf

[45] eIDAS Cooperation Network

- General information on the eIDAS Cooperation Network: Cooperation Network Resources - eID User Community - CEF Digital (europa.eu)

[46] eIDAS - Cryptographic requirements for the Interoperability Framework, TLS and SAML, Version 1.2, 31 August 2019 https://ec.europa.eu/cefdigital/wiki/download/attachments/82773108/eIDAS%20Cryptographic%20Requirement%20v.1.2%20Final.pdf?version=2&modificationDate=1571068651805&api=v2

[47] *** ETSI TS 119 312 V1.3.1 (2019-02) Electronic Signatures and Infrastructures (ESI); Cryptographic Suites https://ec.europa.eu/cefdigital/wiki/display/EIDTECHSUB/Security+Profile+v+1.3

[48] NIST SP 800-52 Rev. 2, Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations https://csrc.nist.gov/publications/detail/sp/800-52/rev-2/final

[49] OpenID Connect [to be supplemented]

[50] SAML [to be supplemented]

[51] Financial-grade API (FAPI) WG Financial-grade API (FAPI) WG | OpenID

[52] ETSI MSS, ETSI TS 102 204 V1.1.4 (2003-08) Mobile Commerce (M-COMM); Mobile Signature Service; Web Service Interface

[53] RFC 7519 JSON Web Token (JWT) https://tools.ietf.org/html/rfc7519

[54] Webtrust, CA/Browser Forum https://cabforum.org/webtrust-for-cas/

- Webtrust Trust Services Principles and Criteria for Certification Authorities ja Webtrust for Certification Authorities - SSL Baseline Requirements Audit Criteria

[55] Information Security Forum (ISF)

- Standard of Good Practice https://www.securityforum.org/solutions-and-insights/standard-of-good-practice-for-information-security-2020/
- INFORMATION RISK ASSESSMENT METHODOLOGY 2 (IRAM2) https://www.securityforum.org/solutions-and-insights/information-risk-assessment-methodology-iram2/

[56] ISRS 4400, International Standard on Related Services (ISRS) 4400 https://www.iaasb.org/publications/isrs-4400-uudistettu-toimeksiannot-erikseen-sovittujen-toimenpiteiden-suorittamisesta

[57] ISAE 3000, International Standard on Assurance Engagements (ISAE) 3000 Revised, Assurance Engagements Other than Audits or Reviews of Historical Financial Information https://www.iaasb.org/publications/basis-conclusions-international-standard-assurance-engagements-isae-3000-revised-assurance

[58] Vahti instructions https://www.suomidigi.fi/en/ohjeet-ja-tuki/vahti-instructions

[59] Recommendations by the Information Management Board (in Finnish)https://vm.fi/suositukset

[60] FIN-FSA regulations and guidelines Regulation – FIN-FSA regulations and guidelines – www.finanssivalvonta.fi

[61] FIN-FSA, Standard 2.4, Customer due diligence; Prevention of money laundering and terrorist financinghttps://www.finanssivalvonta.fi/en/regulation/FIN-FSA-regulations/organisation-of-supervised-entities-operations/2.4/

[62] European banking Authority SREP cyber risk questionnaire https://www.eba.europa.eu/regulation-and-policy/supervisory-review-and-evaluation-srep-and-pillar-2/guidelines-on-ict-risk-assessment-under-the-srep

[63] BIS, Bank for International Settlements:

- External audits of banks External audits of banks (bis.org)
- Supplemental note to External audits of banks - audit of expected credit loss Supplemental note to External audits of banks - audit of expected credit loss (bis.org)
- The internal audit function in banks http://www.bis.org/publ/bcbs223.htm

[64] IIA, The Institute of Internal Auditors www.theiia.fi

[65] ** Finnish [Transport and] Communications Agency guideline 214/2016 O on Electronic identification and trust service notifications https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/regulation/Ohje_214_2016_sahkoisten_tunnistus-_ja_luottamuspalveluiden_ilmoituksista_EN.pdf

[66] ETSI standards on trust services

- Current versions see (search for Digital Signatures and/or ESI - Electronic Signatures and Infrastructures) Download ETSI ICT Standards for free

*** Trust service provider

- ETSI EN 319 401 ETSI EN 319 401 Electronic Signatures and Infrastructures (ESI); **General Policy Requirements** for Trust Service Providers
- ETSI EN 319 411-1 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers **issuing certificates**; Part 1: General requirements
- ETSI EN 319 411-2 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates;

Part 2: Requirements for trust service providers **issuing EU qualified certificates**
- ETSI EN 319 421 Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers **issuing Electronic Time-Stamps**
- ETSI EN 319 521 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for **Electronic Registered Delivery Service Providers**

*** Trust services

- EN 319 412-1 Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: **Overview and common data structures**
- EN 319 412-2 Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to **natural persons**
- EN 319 412-3 Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 3: Certificate profile for certificates issued to **legal persons**
- EN 319 412-4 Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 4: Certificate profile for **website certificates**
- EN 319 412-5 Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements

- ETSI EN 319 422 Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and **time-stamp token profiles**

- ETSI EN 319 102-1 Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and **Validation**

- ETSI EN 319 522 Electronic Signatures and Infrastructures (ESI); **Electronic Registered Delivery Services**
  - ETSI EN 319 522-1 Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail (REM) Services; Part 1: **Framework and architecture**
  - ETSI EN 319 522-2 Electronic Signatures and Infrastructures (ESI); Electronic Registered Delivery Services; Part 2: **Semantic contents**
  - ETSI EN 319 522-3 Electronic Signatures and Infrastructures (ESI); Electronic Registered Delivery Services; Part 3: **Formats**
  - ETSI EN 319 522-4-1 Electronic Signatures and Infrastructures (ESI); Electronic Registered Delivery Services; Part 4: Bindings; Sub-part 1: **Message delivery bindings**
  - ETSI EN 319 522-4-2 Electronic Signatures and Infrastructures (ESI); Electronic Registered Delivery Services; Part 4: Bindings; Sub-part 2: **Evidence and identification bindings**
  - ETSI EN 319 522-4-3 Electronic Signatures and Infrastructures (ESI); Electronic Registered Delivery Services; Part 4: Bindings; Sub-part 3: **Capability/requirements bindings**

[67] Enisa Assessment of Standards related to eIDAS (14 December 2018) https://www.enisa.europa.eu/publications/assessment-of-standards-related-to-eidas

- General information on ENISA, The European Union Agency for Network and Information Security, www.enisa.europa.eu

[68] *** ETSI technical specifications

- ETSI TS 119 441 Electronic Signatures and Infrastructures (ESI); Policy requirements for TSP providing **signature validation** services
- ETSI TS 119 442 Electronic Signatures and Infrastructures (ESI); Protocol profiles for trust service providers providing AdES digital **signature validation** services
- ETSI TS 119 102-1 Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and **Validation**
- ETSI TS 119 102-2 Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 2: Signature **Validation Report**

- ETSI TS 119 172-4 Electronic Signatures and Infrastructures (ESI); Signature Policies; Part 4: Signature applicability rules (validation policy) for European qualified electronic signatures/seals **using trusted lists**

- ETSI TS 119 511 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers providing **long-term preservation of digital signatures** or general data using digital signature techniques
- ETSI TS 119 512 Electronic Signatures and Infrastructures (ESI); Protocols for trust service providers providing **long-term data preservation services**

- ETSI TS 119 524 Electronic Signatures and Infrastructures (ESI); Testing Conformance and **Interoperability of Electronic Registered Delivery Services**

[69] FINAS (Finnish Accreditation Service) Accreditation department of the Finnish Safety and Chemicals Agency (Tukes) https://www.finas.fi/Sivut/default.aspx

[70] Auditing Framework for TSPs, Guidelines for Trust Service Providers, Versio 1.0 - December 2014 Auditing Framework for TSPs — ENISA (europa.eu)

[71] European Co-operation for Accreditation (EA): EA Certification Committee Reference Paper; ETSI / EA Recommendations regarding; Preparation for Audit under EU Regulation (EU) No 910/2014 Article 20.1. (not published online)

- General information about European co-operation for Accreditation - European Accreditation (european-accreditation.org)

[72] ***ETSI EN 319 403-1 Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment - Requirements for **conformity assessment bodies** assessing Trust Service Providers

[73] ***ETSI TS 119 403-2 V1.2.1 (2019-04) Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment; Part 2: Additional requirements for **Conformity Assessment Bodies** auditing Trust Service Providers that issue Publicly-Trusted Certificates https://www.etsi.org/deliver/etsi_ts/119400_119499/11940302/01.02.01_60/ts_11940302v010201p.pdf

[74] ***ETSI TS 119 403-3 V1.1.1 (2019-03) Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment; Part 3: Additional requirements for **conformity assessment bodies** assessing EU qualified trust service providers

[75] ** Finnish Transport and Communications Agency guideline 215/2019 O Assessment reports on qualified eIDAS trust services https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/regulation/EN_O215__Assessment%20reports%20on%20qualified%20eIDAS%20trust%20services%20%289_10_2019%29.pdf

5.2 Summary of comments

[TBA after hearing]