Dnro
TRAFICOM/245890/03.04.05.00/2020
v 2.9.2020

Finnish Transport and Communications Agency survey of 4 August 2020 on the update needs of Regulation 72A/2018 on Electronic Identification and Trust Services and of other technical guidance

Content

1 Grounds, organisation and schedule concerning updating the regulation

The regulation was issued in 2016. Technological development, the progress of ETSI standardisation, market development, feedback from identification and trust service providers concerning the application of the provisions and the Agency's experiences with supervision warrant an assessment of the currency of the requirements and potential changes. This process must observe the limits of the right to issue regulations and compatibility with EU regulations.

Paragraphs 2–5 of the Regulation concern strong electronic identification service providers, the assessment of the conformity of the identification service and the competence of the assessment bodies.

Meeting the requirements of the Regulation is required for the strong electronic identification service provider to be entered into the Finnish Transport and Communications Agency register, which is governed by the Act on Strong Electronic Identification and Electronic Trust Services (617/2009).

Paragraphs 6–8 of the Regulation concern the assessment of the conformity of qualified trust services in compliance with the eIDAS Regulation EU (910/2014) and the certification body for the approved electronic signature or seal creation device.

The Regulation was passed in 2016 in connection with the coming into force of the EU eIDAS Regulation. The requirements concerning the regulation of identification services were harmonised with EU regulations and regulations on interoperability with national trust networks were put in place.

The regulation to be changed

Regulation on electronic identification and trust services (Finnish Communications Regulatory Authority 72A/2018 M)

The transitional period in section 25 was extended by amending Regulation 72A/2018 M. No other requirements were changed at that time, meaning that the provisions remain the same as in Regulation 72/2016 M issued by the Finnish Communications Regulatory Authority.

1.1 Legislative competence

The right to issue regulations of the Finnish Traffic and Communications Agency is laid down in the Act on Strong Electronic Identification and Electronic Trust Services. This competence is restricted to the matters specified in section 42 of the Act.

In requirements set for identification services, the Agency shall observe that the Act strives to harmonise the requirements with those laid down in the EU eIDAS regulation, i.e. the Commission's regulation on setting out minimum technical specifications and procedures for assurance levels (EU) 2015/1502, in particular. The Assurance Level Regulation is interpreted in peer reviews in connection with notifying the identification schemes to the Commission. The Agency participates in reviews and takes shared views into account in national regulations.

The right to issue regulations concerning trust services is limited. The Regulation will only make necessary additions in order to ensure that the assessment framework of qualified trust services is sufficiently precise and predictable where the requirements have not been specified in EU regulations. The Regulation is used to specify EU regulation and the regulation concerning identification and trust services so that there are legal prerequisites for the accreditation of assessment bodies in charge of assessing the conformity of trust services or the appointment of a certification body for an electronic signature or seal creation device, if any interest is sparked.

1.2 Schedule and organisation

The following schedule is preliminary and it may have to be changed, if the legislative environment (eIDAS, the Act on Strong Electronic Identification and Trust Services) changes. The schedule for the EU notification of the regulation may affect the schedule of the final stage towards the end of 2021.

August 2020 Industry survey on need for change and implications
September–November 2020 Official drafting (change drafts and impact assessments)
December 2020–June 2021 Working group activities (the Agency invites members of the trust network and technical eIDAS work group to themed workshops, initial estimate 5–8 workshops)
June–August 2021 Official drafting and translations (Swedish, English)
September 2021 Consultation on the new proposal for regulation and explanatory notes
October 2021– Summary of statements, any changes and their translations, EU notification (three months)
January–February 2022 New regulation enters into force

1.3 Alternative methods of regulation

1.3.1 Regulation, guideline or recommendation?

Mandatory rules imposed through regulations are an appropriate regulatory tool when information security, quality or interoperability need to be ensured. Equally specified requirements promote fair competition between the operators. Regulations are efficient, because they are always directed at all stakeholders and define the requirements in advance. The content of regulations could be derived by interpreting the law in supervision, but the specifications implemented with the regulation make regulatory work more predictable. Cooperation with the industry is necessary to ensure that the requirements are feasible. Issuing regulations requires that the requirements being decreed are technically sufficiently mature to serve as mandatory rules.

From the point of view of customers of identification and trust services, regulation ensures data security and the protection of privacy by design. Building trust for the industry requires that the stakeholders build their services properly from the start.

The regulations issued are justified in the explanatory notes for the Regulation, which also provide instructions and recommendations on good practices, especially in matters that might be unclear to the stakeholders during the preparatory work of the Regulation.

If the matter cannot be regulated in light of the above targets, or issuing regulations is not appropriate, the Agency may provide technical guidance through instructions or recommendations intended to enhance the security and compatibility of the services as well as cooperation within the industry and the flow of information to the authorities.

The Agency has issued several guidelines (O for *ohje*) and recommendations (S for *suositus*) on identification and trust services.

- Guideline 211/2019 O Model criteria for identification service provider audits
- Recommendation 212/2018 S Finnish Trust Network SAML 2.0 Protocol Profile (update under way 2020)
- Recommendation 213/2018 S OpenID Connect Protocol Profile for the Finnish Trust Network (update under way 2020)
- Guideline 214/2016 O On electronic identification and trust service notifications

- Guideline 215/2019 O Assessment reports on qualified eIDAS trust services
- Recommendation 216/2016 S Code of conduct for trust network

1.3.2 Co-regulation and self-regulation

Whether the objectives could be achieved through co-regulation and self-regulation within the industry is also assessed during the preparatory work of the Regulation. Efficient co-regulation requires a readiness by the industry to invest in organising and maintaining co-regulation, and it can only be utilised in matters that do not pose a risk of activities in violation of competition regulation.

The impact assessments in the explanatory notes on the valid regulation cover the possibilities of co-regulation and self-regulation, and a corresponding assessment will also be conducted during the upcoming updating process for the regulation.

In 2012, the Agency commissioned a judicial report on the prerequisites for co-regulation in terms of competition law from Krogerus Attorneys Ltd. Further information is available on the website under the heading *Conditions for co-regulation* https://www.kyberturvallisuuskeskus.fi/en/our-activities/regulation-and-supervision/how-we-regulate

Based on the report, the impact of regulatory cooperation is the key from the point of view of competition law. The potential pitfalls of the co-operation in terms of competition law include a) coordination effects resulting from competitor cooperation and b) exclusion resulting from competitor co-operation, the shared dominant market position of those participating in the regulatory work or the dominant market position of the regulatory organ.

1.4 Legislation

The regulation to be changed

Regulation on electronic identification and trust services (Finnish Communications Regulatory Authority 72A/2018 M)

The regulations referred to in this document

Act on Strong Electronic Identification and Electronic Trust Services (617/2009, so-called **Identification Act or Identification and Trust Act**)

Government Decree on the Trust Network for Providers of Strong Electronic Identification Services 169/2016

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")

Commission Implementing Regulation (EU) 2015/1502 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 ("**Assurance Level Regulation**")

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 ("**Interoperability Regulation**")

Commission Implementing Decision (EU) 2015/296 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 ("**Cooperation Network Decision**")

Regulation referenced in the PSD2 comparison

COMMISSION DELEGATED REGULATION (EU) 2018/389 of 27 November 2017 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"**)

2 Regulation structure and other general matters

The regulation combines the assessment requirements concerning strong electronic identification and qualified trust services in compliance with the eIDAS Regulation. In addition to this, the regulation concerns certification bodies for creation devices of approved electronic signatures or seals in compliance with the eIDAS Regulation. These elements are all governed by the same regulation on the EU level and in Finland on the legislative level.

2.1 General questions

1) **Scope of the regulation.** In your opinion, is it functional to combine identification and trust services in the same regulation?
2) **Sections.** Is the regulation divided into clear and concise sections?
3) **Other technical guidance.** Do identification and trust services lack guidance by the authorities to promote their provision and acquisition? Which aspect would you like to see specified in the regulation, guidelines or at recommendation level?
4) **General.** Other comments on the regulation as a whole?

3 Information security requirements for the strong electronic identification scheme

3.1 What is the identification scheme and the identification mean?

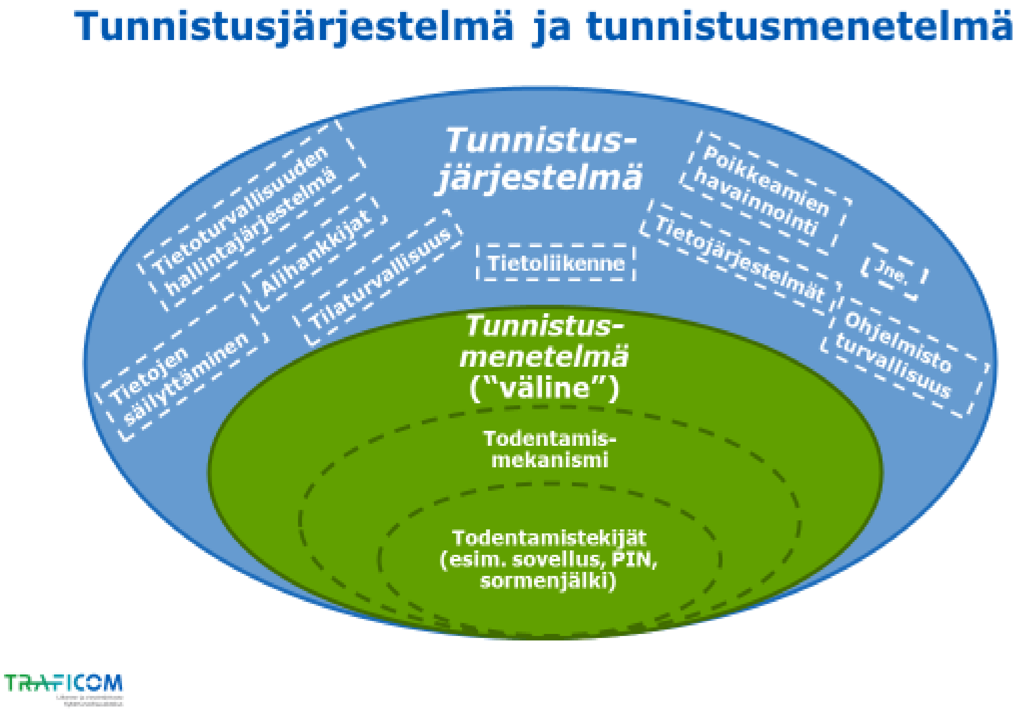


Image: Terms identification scheme and identification mean.

An **identification scheme** is a system in which electronic identification means are granted and produced 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 covers all subcontracted sections and functionalities of the system concerning the production of the identification service.

Identification means and identification method refer to the same thing in regulation: material and/or immaterial entities that contain personal identification data and that are used for identification related to online services. The identification scheme is based on **authentication factors** connected to the user's knowledge, physical attribute or possession as well as a **dynamic authentication mechanism** to ensure that each identification event is unique.

3.2 Requirements and questions concerning identification scheme and identification means/methods

3.2.1 Information security management requirements of an identification service provider (section 4)

Section 4 of the regulation provides general provisions on factors that need to be observed in information security management in an identification scheme. Providing an identification service covers the whole identification scheme.

Section 2.4.3 of Annex 1 of the EU 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.* Subparagraph 5 of section 8.1 of the Identification Act contains provisions governing information security management and references, for example, to section 2.4.3 of the Assurance Level Regulation.

The requirements of the Identification and Trust Service Act and the EU Assurance Level Regulation are refined in section 4.1 of the regulation. At least the ISO/IEC 27001 standard is a generally acknowledged and valid standard for information security management. Other standards or combination of standards may also be used, given that these combinations and standards concern the information security management. The standard may be international, such as ISO, but also national, such as KATAKRI.

The subsection 2 of section 4 lists all of the operative areas that must be covered by information security management. The requirements draw on the high level grouping found in standard ISO/IEC 27001.

In supervision, the Agency has found that the assessment of information security management has been considered sufficient in terms of assessing conformity, especially in the early days of applying the regulation. This is not true, because information security management is just one of the assessed areas, and the fulfilment of technical criteria specified in the regulations must also be assessed. This has been clarified in assessment guideline 211/2019.

5) **Information security management.** According to the Agency’s assessment, at least the explanation of the regulation must be supplemented and the relationship between information security management and technical requirements clarified. Do you agree?
6) **Information security management.** Do you think the requirements for information security control should be changed, supplemented or decreased in some manner and why?

3.2.2 Identification scheme security controls, assurance levels and incident management (sections 5–11)

Information systems, telecommunications and operational security. The identification scheme requirements specified in section 5.1 of the regulation are based on a general outline of the different aspects of information systems, telecommunications and operational security. The requirements for remotely controlled terminal devices are specified on substantial and high assurance level in section 5.2. The implementation and controls of the system must be proportioned to a moderate or high level of threat according to the desired assurance level.

Assurance levels. As a rule, the requirements pertaining to substantial and high assurance levels are not specified separately in the regulation. The implementation and controls of the system must be proportioned to a moderate or high level of threat according to the desired assurance level.

Separation as an information security measure. While the regulation was being prepared in 2016, it was assessed whether the following were 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.

The impact assessment concluded that the details of separation were to be implemented through general information security management, planning and audits. The specification of security requirements for terminals used in management networks and office networks raised so many questions during the drafting phase 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.

The general requirements laid down in subsection 1 of section 5 are specified in subsection 2 in terms of management connections and their remote use. Personnel terminal devices, which employees use to access the management systems, can easily become information security risks, unless the matter is addressed specifically. 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.

Identification schemes of different sizes and newcomers. The requirements for identification scheme and methods 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 predictability to ease the operation of identification services. According to the Agency, clear requirements also foster mutual trust in the information security of current and future identification services in the trust network.

Subcontractors. The regulation does not provide separate provisions for subcontractors. In accordance with section 13 of the Identification Act, the identification service provider must ensure that the services it subcontracts meet the requirements. The implementation of identification scheme and identification methods is usually subcontracted. In terms of assessing conformity, subcontracting is discussed in the identification service assessment guideline 211/2019.

Identification method characteristics and authentication factors. The identification method is the user’s identification means with the authentication factors and the authentication mechanism used to execute authentication during the identification. The identification method must employ at least two authentication factors from different categories (knowledge, possession, inherence). The authentication mechanism must be dynamic, meaning that each identification event must be unique.

Several authentication factors of different types work towards ensuring that the identification means is only used by the rightful owner. A dynamic authentication mechanism works towards ensuring that the identification is based on the right authentication factors and that the events cannot be replicated or forged. The implementation of the identification method and the authentication mechanism must be protected against information security risks and moderate or high-level attacks in accordance with the assurance level.

The authentication factors and mechanism are discussed in more detail in the comparison with the PSD2 regulation in section 3.4.

Encryption. Paragraph 2g) of subsection 1 of section 5 of the regulation lays down general provisions on encryption solutions and section 7 lays down provisions on encrypting traffic between the interfaces of identification service providers as well as between the interfaces of identification service providers and e-services. This means that the general requirement outlined in section 5 pertains to connections between the identification service and its subcontractor and the identification service’s own systems.

Section 7 of the regulation lays down provisions on acceptable encryption methods, parameters and encryption protocols used in TLS encryption. The impact assessment of the encryption regulation model completed in 2016 found that the development of secure algorithms is slow enough to allow for the provision of precise requirements in the sections of the regulation and amending the regulation, if necessary. During monitoring activities, the Agency has encountered new algorithms, such as Poly1305 and ChaCha20, and it is clear that the relevance of the requirements in section 7 must be reassessed.

Instead of providing very precise regulations on encryption algorithms, other models, which are as dynamic as possible, could also be reviewed if they are available. However, based on experience, the Agency considers it necessary to ensure the precision and predictability of the requirements, as replacing the TLS 1.0 protocol with insufficient information security, or the 3DES algorithm has not been carried out completely over the course of several years.

Interface security. The security requirements for communications interfaces mainly consist of the encryption requirements provided in section 7.

Section 8 of the regulation clarifies that the requirements pertain to the interface between the identification means issuer and identification broker service. Section 8 also provides that the parties are identified.

Section 9 of the regulation elaborates that the requirements pertain to the interface between identification services and e-services as well as the user of the identification service and identification means. There are no provisions governing identification of the e-service, but the requirement concerning message level encryption requires the exchange of encryption keys between the identification service and the e-service, which is aimed at also ensuring that e-services that have not made a contract with the identification broker service are unable to use the strong electronic identification service (unauthorised posing as an e-service).

The Tupas transition, in particular, and the implementation of message level encryption and the related key management with e-services resulted in the need to make changes in 2019.

According to an assessment by the Agency, the preparations for the regulation must at least assess more specific technical means of preventing users from being tricked into identifying with the wrong e-service.

Security incidents and disturbance notifications. In addition to what has been provided in section 5, there are no specific requirements governing the observation capability or management of security incidents. Section 11 of the regulation provides that disturbance notifications must be submitted to the Finnish Traffic and Communications Agency. The reporting threshold has not been specified in the regulation, but the explanation for the regulation contains implementation guidelines for various types of disturbances.

The Agency has received an increasing number of disturbance notifications in 2019 and 2020, whereas notifications were practically not submitted previously. In terms of the regulation, the Agency’s assessment remains that there is insufficient data on the disturbances to warrant specifying clear-cut thresholds on the regulation level. If thresholds were to be specified, there would have to be a way to configure them in the technical systems of the identification services and they should be relatively permanent in order to prevent unnecessary system costs to the identification services due to changes in regulation. Based on the Agency’s experience, such specifications governing information security risks and violations are by and large quite challenging, and other monitoring sectors (telecommunications operation, domain broker services, cloud services in compliance with the NIS directive) have also employed qualitative thresholds based on implementation guidelines.

3.2.3 General questions concerning the scope of technical requirements

7) **Scope.** In your opinion, does the scope of regulation concerning technical requirements cover the right things? Are the matters listed in section 5 relevant?
8) **Unnecessary requirements.** Does the regulation contain technical requirements that are unnecessary? Why? What do you consider the relationship to be between the requirements you deem unnecessary and completely new identification service providers entering the Finnish market?

9) **Missing requirements.** Does the implementation of the identification system or identification method contain areas which are missing from the regulation entirely and that should be regulated? Could any missing matters be controlled by issuing guidelines or recommendations?

3.2.4 Questions concerning assurance levels and separation

10) **Assurance levels.** Should the regulation issue separate specifications for technical requirements in keeping with the high assurance level? Which requirements and how?
11) **Assurance levels.** Can the application of the requirements pertaining to different assurance levels be anticipated by developing the guidance and interpretation instructions in Guideline 211/2019 O Model criteria for identification service provider audits, instead of within the regulation?
12) **Separation.** In your opinion, is it necessary to specify the separation of some areas of systems or tasks by way of issuing a regulation or guideline?

3.2.5 Questions concerning authentication factors

13) **Authentication factors.** Do the planning of the identification method characteristics and the security of authentication factors contain areas that should be assessed in the preparatory work of the Regulation? See also questions in section 3.3 concerning PSD2 comparisons.

3.2.6 Questions concerning encryption

14) **Encryption.** Are the definitions of the encryption requirements in section 5 and the references in the explanation to the regulation (ENISA, NIST, NCSA-FI, SANS) sufficient? Should the regulation or explanations be amended in some way? In your opinion, which is the most useful reference of the recommended encryption solutions?
15) **Encryption.** In your opinion, are the encryption requirements set out in section 7 up to date? Which changes do you suggest for the encryption methods, their parameters or the encryption protocols mentioned in the regulation? How would the ciphersuites found in the explanations for the regulation need to be updated?
16) **Encryption.** In your opinion, is the recommendation concerning high assurance level algorithms found in the explanatory notes for the regulation up to date? Should the recommendation be made binding and included in the regulation? How would this affect high assurance level identification usability, interoperability and e-services?
17) **Encryption.** Are there any technical issues or inconsistencies with implementing the encryption requirements in section 7? How have you solved them and how do you think the regulation should be changed?
18) **Encryption.** Do you think there are alternative models for regulating encryption requirements instead of defining the requirements in the regulation, as they are now? In your opinion, which consistently measurable and definable (predictable from the point of view of the regulatory requirements) models and references could be used in the regulation?
19) **Encryption.** Do communication channels have any other relevant security protocols in addition to TLS? Should they be observed in the regulation or implementation guidelines?

3.2.7 Questions concerning communication channels

20) **Authenticating parties.** In your opinion, are the internal communication channels' authenticating requirements of the trust network in section 8 clear?
21) **E-service links.** Have you been able to implement authentication and key exchange practices with e-services? How? Does this matter require technical guidance by way of a recommendation, guideline or regulation?

22) **User interfaces.** Do you think the user interface requirements need to be changed? How and why?

3.2.8 Questions concerning threat and disruption management

23) **Disruptions.** Are there any matters concerning the observation, management and reporting of information security threats, information security violations and disruptions that should be reassessed during the preparatory work of the Regulation?
24) **Threats, fraud.** In identification, are there any information security threats or fraud phenomena related to the user or the electronic services that should be addressed during the preparatory work of the Regulation?

3.2.9 Questions concerning feasibility and impact

25) **Feasibility.** Does the regulation contain technical requirements that are difficult to implement? Which requirements and in which situations? How should the matter be resolved – do compensating controls exist, for example?
26) **Feasibility.** Does the regulation contain technical requirements that contradict each other or whose implementation is technically impossible or difficult? How do you think the contradictions or feasibility issues could be resolved?
27) **Application.** Does the regulation contain requirements whose interpretation and application are unclear?
28) **Services.** Does the regulation contain requirements that are difficult to apply to the identification services you offer to users and e-services or that make developing those services more challenging?
29) **Impact.** How has the regulation impacted the maintenance and security of your identification scheme and means?
30) **Impact.** To your understanding, how has the regulation affected the security of other strong electronic identification service providers registered in the trust network? Do you trust that the identification schemes of the other members of the trust network are as secure as yours?

3.3 Parallel technical requirements found in PSD2 or other legislation

3.3.1 General

This section is a compilation of specific details from regulation concerning electronic identification. Reviewing these details may be necessary in order to identify differences between regulations concerning general, industry-independent identification (eIDAS) and regulations concerning the payment service industry (PSD2), as well as to assess the impact of these differences. The 2018 review is also attached to the survey.

In Finland, many strong electronic identification methods registered in accordance with the Identification Act are also used as strong electronic identification in accordance with payment service regulations. The content of the eIDAS Regulation and the Identification Act is neutral in terms of which industry and which services employ the identification.

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 industry (the Financial Supervisory Authority PSD2 co-operation group and the Traficom eIDAS work group) on the review. Based on the review and the statements, no impediments to using the same identification method within both of the regulatory frameworks were found. Since then, the policy issued by the Financial Supervisory Authority stating that online banking code lists are invalid without an additional authentication element has changed the situation somewhat.

In terms of the eIDAS Regulation, below you will find excerpts from the Assurance Level Regulation (EU) 2015/1502 (eIDAS Assurance Level Regulation) issued by the European Commission and the related LOA Guidance 2016 issued by the eIDAS Cooperation network.

In PSD2 regulations, the industry-specific strong electronic identification requirements are given in the 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").*

The European Banking Authority EBA published an opinion on the implementation of RTS SCA & CSC (EBA-Op-2018-04) in June 2018.

The European Banking Authority EBA published an opinion on the elements of strong customer authentication under PSD2 (EBA-Op-2019-06) in June 2019.

EBA has also published answers concerning RTS SCA & CSC regulations in accordance with the PSD2 Q&A process. On 25 May 2020, the service displayed 79 Q&As on implementation.

3.3.2 General information on authentication factors based on possession

See EBA-Op-2019-06

> *30. Table 2 summarises the views expressed above on what does or does not constitute a possession element under the RTS on SCA and CSC. The table is for illustrative purposes only and is not intended to be exhaustive; the possible elements included reflect current practices and developments in the market at the time of publication of the opinion.*
>
> *Possession of a device evidenced by an OTP generated by, or received on, a device (hardware or software token generator, SMS OTP) Yes**
> *Possession of a device evidenced by a signature generated by a device (hardware or software token) Yes**
> *Card or device evidenced through a QR code (or photo TAN) scanned from an external device Yes**
> *App or browser with possession evidenced by device binding — such as through a security chip embedded into a device or private key linking an app to a device, or the registration of the web browser linking a browser to a device Yes**
> *Card evidenced by a card reader Yes**
> *Card with possession evidenced by a dynamic card security code Yes**
>
> **Compliance with SCA requirements is dependent on the specific approaches used in the implementation of the elements.*

See LOA Guidance 2016

> *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. smartcards), or software*

> *token, uniquely identifiable token (e.g. the SIM card of a cell phone) or devices with one-time-passwords (e.g. "RSA-Token" or printed cards).*
>
> *Typical attacks on possession-based authentication factors are theft, duplication or tampering (manipulation), as well as attacks on the proof-of-possession during authentication.*

3.3.3 Banking code lists

Banking code lists are authentication factors based on possession, and they are very susceptible to phishing attacks, for example.

The Financial Supervisory Authority has issued a policy stating that a banking code list does not meet the requirements of authentication factors based on possession without a verification element, and identification means providers have e.g. added text message verification to payment transactions performed using banking code lists.

See also EBA-Op-2019-06

> *28. Following the publication of the EBA Opinion on the implementation of the RTS, which stated that the card details and card security code that are printed on the card cannot constitute a knowledge element, a number of industry participants have queried if such details could constitute a possession element. The EBA is of the view that such details cannot do so for approaches currently observed in the market, in particular given the requirements under Article 7 of the RTS, and it advises CAs to closely monitor their application. That being said, dynamic card security codes (where the code is not printed on the card and changes regularly) may provide evidence of possession in line with Article 7 of the RTS.*
>
> *29. The EBA is also of the view that printed matrix cards or printed OTP lists that are designed to authenticate the PSU are not a compliant possession element for approaches currently observed in the market, for similar reasons to those mentioned for card details above, namely that they are unlikely to comply with the requirements under Article 7 of the RTS.*

Under the Identification Act, the Agency has not found paper banking code lists to be in violation of the requirements on the *substantial* assurance level *for the time being*, but peer reviews of the Danish identification system in accordance with the eIDAS Regulation have highlighted the factor, resulting in Denmark announcing that it will discontinue the use of banking code lists. See eIDAS Cooperation network Opinion 1/2020

31) **PSD2 and eIDAS.** Is it necessary to review the banking code lists in connection with the preparatory work of the Regulation? Is their use going to be continued?

3.3.4 SMS OTP

A one-time password sent via SMS is an authentication factor based on the possession of the mobile phone, and it is susceptible to text message sender fraud and interception, for example.

EBA has issued an opinion on passwords provided via SMS in question 2018_4039 Qualification of SMS OTP as an authentication factor https://eba.europa.eu/single-rule-book-qa/-/qna/view/publicId/2018_4039

See also EBA-Op-2019-06

> *25. As stated in the EBA Opinion on the implementation of the RTS (paragraph 35), a device could be used as evidence of possession, provided that there is a 'reliable means to confirm possession through the generation or receipt of a dynamic validation element on the device'. Evidence could, in this context, be provided through the generation of a one-time password (OTP), whether generated by a piece of software or by hardware, such as a token, text message (SMS) or push notification. In the case of an SMS, and as highlighted in Q&A 4039, the possession element 'would not be the SMS itself, but rather, typically, the SIM-card associated with the respective mobile number'.*

The eIDAS Regulation does not contain an established position on the matter, but it has been estimated, in connection with some peer reviews, that SMS OTP does not meet the attack resistance requirements of the high assurance level.

32) **PSD2 and eIDAS.** Is it necessary to review SMS OTP in connection with the preparatory work of the Regulation?

3.3.5 Mobile app

The mobile app is an authentication factor based on the possession of the mobile phone, and its security depends on which data security features the phone and its operating system have and whether they are enabled. Security is also affected by the communication channels with the background system and the security of the background system.

Question 2018-4047 in the EBA Q&A concerns this matter, stating that there is a need to assess the security of the app and, for example, use the SEE element https://eba.europa.eu/single-rule-book-qa/-/qna/view/publicId/2018_4047

See also EBA-Op-2019-06

> *24. Article 4(30) of PSD2 defines possession as 'something only the user possesses'. Possession does not solely refer to physical possession but may refer to something that is not physical (such as an app). Recital 6 of the RTS refers to the requirement to have adequate security features in place and provides examples of possession, 'such as algorithm specifications, key length and information entropy'. Article 7 of the RTS refers to the requirement for PSPs to have mitigation measures to prevent unauthorised use and to have measures designed to prevent the replication of the elements.*
>
> *26. The EBA is of the view that approaches relying on mobile apps, web browsers or the exchange of (public and private) keys may also be evidence of possession, provided that they include a devicebinding process that ensures a unique connection between the PSU's app, browser or key and the device. This may, for instance, be through hardware crypto-security, web-browser and mobile-device registration or keys stored in the secure element of a device. By contrast, an app or web browser that does not ensure a unique connection with a device would not be a compliant possession element.*

The elements that are significant in terms of the supervision and interpretation of the requirements of the eIDAS Regulation and the Identification and Trust Services Act are specified in mobile application criteria C in guideline 211/2019. The review method corresponds to the cooperation network policies created in EU peer reviews on the security requirements of the regulation. Using the mobile app at high assurance level would require certifying the security elements.

33) **PSD2 and eIDAS.** In your opinion, are there any differences between the requirements on mobile app security in the PSD2 regulation and the requirements laid down in the Identification Act and the eIDAS Regulation? Do potential differences prevent the use of the same app for payment services and identification in general?

3.3.6 One-time-password generators

A one-time-password generator device is an authentication factor based on possession, and its security is affected by the device software, the algorithms used and the physical components.

eIDAS Assurance Level Regulation

> *Introductory paragraph (11) of regulation (EU) 2015/1502: IT security certification based on international standards is an important tool for verifying the security compliance of products with the requirements of this implementing act*

In its advisory memorandum 12/2018, Traficom demanded that the security of one-time-password generator devices be assessed in connection with the reviews scheduled for 2019.

EBA-Op-2018-04

> *35 …For a device to be considered possession, there needs to be a reliable means to confirm possession through the generation or receipt of a dynamic validation element on the device.*

34) **PSD2 and eIDAS.** Presumably, international device certifications are not dependant on which industry they are used in. Are there any differences between different sets of regulations governing one-time-password generator devices that should be reviewed during the preparatory work of the Regulation?

3.3.7 Authentication factor based on knowledge

EBA-Op-2019-06

> *31. Article 4(30) of PSD2 defines knowledge as 'something only the user knows'. Article 6 of the RTS refers to the requirement for PSPs to mitigate the risk that the element is 'uncovered by, or disclosed to, unauthorised parties' and to have mitigation measures in place 'in order to prevent their disclosure to unauthorised parties'.*
>
> *32. The EBA is of the view that the following elements could constitute a knowledge element: a password, a PIN, knowledge-based responses to challenges or questions, a passphrase and a memorised swiping path (as opposed to keystroke dynamics, namely the manner in which the PSU types or swipes, which may be considered an inherence element).*
>
> *34. The same opinion also stated that a user ID (username) would not constitute a compliant knowledge element. Neither would an email address.*
>
> *36. Table 3 summarises the views expressed above on what does or does not constitute a knowledge element under the RTS on SCA and CSC. The table is for illustrative purposes only and is not intended to be exhaustive; the possible elements included reflect current practices and developments in the market at the time of publication of the opinion.*
>
> *Password Yes**
> *PIN Yes*

*Knowledge-based challenge questions Yes**
*Passphrase Yes**
*Memorised swiping path Yes**

Email address or user name No
Card details (printed on the card) No
OTP generated by, or received on, a device (hardware or software token generator, SMS OTP) No (for approaches currently observed in the market)
Printed matrix card or OTP list No

**Compliance with SCA requirements is dependent on the specific approach used in the implementation of the elements.*

LOA Guidance 2016

The knowledge-based factor likely to be known only by the owner of the factor and the verifying entity, for example: PINs, passwords, memorable words or dates, pass phrases, pre-registered knowledge and other information likely to only be known by the subject. In some cases even the verifying entity may not know the actual knowledge-based factor, but are able confirm that they and the applicant know the exact same information, for example using the hash of a password.

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).

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 email without knowledge of the owner or the verifier.

3.3.8 Biometric authentication factor

Currently, the biometric authentication factors used are primarily mobile phone features, such as fingerprint scanning or face recognition features in mobile apps. Users do not generally have access to other biometric element scanners at the moment. The security of a biometric authentication factor depends on sensor accuracy and the implementation method of the software and device processing biometric data, among other things.

EBA-Op-2019-06

17. Article 4(30) of PSD2 defines inherence as 'something the user is'. Article 8 of the RTS on SCA and CSC refers to the 'authentication elements categorised as inherence and read by access devices and software' and recital 6 refers to the need to have 'adequate security features' in place that could, for example, be 'algorithm specifications, biometric sensor and template protection features'.

18. As stated in the Opinion on the implementation of the RTS, inherence may include behavioural biometrics identifying the specific authorised user. The EBA is of the view that inherence, which includes biological and behavioural biometrics, relates to physical properties of body parts, physiological characteristics and

> *behavioural processes created by the body, and any combination of these. In addition, it is (the quality of) the implementation of any inherence-based approach that will determine whether or not it constitutes a compliant inherence element. Inherence is the category of elements that is the most innovative and fastest moving, with new approaches continuously entering the market.*
>
> *20. The swiping path memorised by the PSU and performed on a device would not constitute an inherence element, but may rather constitute a knowledge element, something only the user knows.*
>
> *22. Table 1 summarises the views expressed above on what does or does not constitute an inherence element under the RTS on SCA and CSC. The table is for illustrative purposes only and is not intended to be exhaustive; the possible elements included reflect current practices and developments in the market at the time of publication of the opinion.*
> *Table 1 — Non-exhaustive list of possible inherence elements*
> *Fingerprint scanning Yes*
> *Voice recognition Yes V*
> *ein recognition Yes*
> *Hand and face geometry Yes*
> *Retina and iris scanning Yes*
> *Keystroke dynamics Yes*
> *Heart rate or other body movement pattern identifying that the PSU is the PSU (e.g. for wearable devices) Yes*
> *The angle at which the device is held Yes …*
> *…*
> **Compliance with SCA requirements is dependent on the specific approach used in the implementation of the elements.*

Neither the eIDAS Regulation or Regulation 72 contain any separate requirements for biometric authentication factors. Instead, the assessment of their reliability and security is part of the overall assessment of the attack resistance of the identification method and authentication mechanism. The 2019 peer reviews of the Belgian mobile app based identification method stated that biometric authentication factors are not sufficiently reliable to be used at *high* assurance level.
See eIDAS Cooperation Network Opinion 8/2019

35) **PSD2 and eIDAS.** Are there any differences between different sets of regulations governing biometric authentication factors that should be reviewed during the preparatory work of the Regulation?

3.3.9 Authentication factor independence

EBA-Op-2019-06

> *38. Another requirement under the RTS, in line with PSD2, is that the two elements used for SCA be independent. Independence under Article 9 of the RTS requires that the use of the elements 'is subject to measures which ensure that, in terms of technology, algorithms and parameters, the breach of one of the elements does not compromise the reliability of the other elements'.*

Neither the eIDAS regulation nor Regulation 72 contain any separate requirements for the independence of the authentication factors. Instead, it is part of the overall assessment of the characteristics of the identification method and the attack resistance of the authentication mechanism (Assurance Level regulation, Annex 2.2.1 Electronic identification means characteristics and design as well as 2.3.1 Authentication mechanism)

LOA Guidance 2016

> *If multi-factor authentication is used1, the different factors should be chosen in a way to counter different threats/attack vectors.*
> *Evaluating the strength of authentication needs to take into account not only the factor(s) itself, but also the mechanism to verify the factor(s).*
>
> *Using multiple authentication factors from different categories in a complementary manner can increase the overall security of the identification means. A common example is combining a possession-based token with a password or PIN to unlock the token. Even if the token is lost or stolen, it still cannot be used for authentication without the PIN.*
>
> *The authentication mechanisms used in the authentication phase cannot prevent all attacks completely, 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 their resistance against attacks with a certain attack potential (i.e. strength of an attacker).*
> *The Level of Assurance use the terms "enhanced-basic", "moderate" and "high" to denote the different attack potentials. This terminology is borrowed from 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).*
> *ISO/IEC 15408-1 defines "attack potential – measure of the effort to be expended in attacking a [mechanism], expressed in terms of an attacker's expertise, resources and motivation".*
>
> *Annex B.4 of 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 act, some assessment of resistance against potential attacks should be carried out.*
>
> *The assessment should take relevant threats into accounts. For example, ISO 29115 mentions: online guessing, offline guessing, credential duplication, phishing, eavesdropping, replay attack, session hijacking, man-in-the-middle, credential theft, spoofing and masquerading.*
>
> *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.*
>
> *For example*
> - *For LoA high, it is not sufficient that a smart card protects a cryptographic key against manipulation with high attack potential, also the cryptographic protocol should 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-*

[1] The Assurance Level regulation also specifies low assurance level requirements, which do not require authentication factors from different classifications.

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.*

> *Reasonable assumptions on the level of security of components used by, but not part of, the authentication scheme (e.g. the environment of the user, browser, smart phone, etc.) should be taken into account during the risk assessment. Components can be operated in different configurations with different security settings.*
> *As an example, the assessment might assume that the user operates a personal firewall and virus protection on his/her computer.*
>
> *As a counterexample, currently it would not be reasonable to assume that the browser of the user is configured to use only secure cipher suites for Transport Layer Security (TLS); however this can be enforced by the service.*
>
> *The assessment might presume reasonable settings for the components not part of the authentication scheme.*

3.3.10 Dynamic linking

In terms of regulation, the questions have concerned at least how the payment authentication requirements affect the opportunity to use the same identification method as a basis for general identification and payment services. Authenticating a payment requires identification and the *dynamic linking* of payment data to the identification event (to the *authentication code*).

EBA-Op-2019-06

> *40. The EBA also notes (as published in Q&A 4141) that an element used for the purpose of SCA may be reused within the same session for the purpose of applying SCA at the time that a payment is initiated, provided that the other element required for SCA is carried out at the time of the payment initiation and that the dynamic linking element is present and linked to that latter element.*

The EBA Q&A discusses this relationship between identification and payment transaction authentication, among other things, and based on question 2018-4141, it would seem that in terms of general identification, performing identification using the same method as in any other service and authenticating the payment at a later time during the event while identified in the manner required by RTS SCA & CSC is possible.

https://eba.europa.eu/single-rule-book-qa/-/qna/view/publicId/2018_4141

3.3.11 Session identifier, dynamic authentication/authentication code

The requirement concerns the fact that each identification event must be unique, and may not be reproducible. The event/authentication event is based on the use of authentication factors and encryption, for example.

The requirements of the Identification Act and eIDAS Regulation are contained in the requirement of general **dynamic authentication** and the attack resistance of the authentication mechanism:

eIDAS Assurance Level Regulation

> Annex section 1 Definitions
> *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;*
>
> Annex section 2.3.1 Authentication mechanism
> *Substantial assurance level*
> *1. The release of person identification data is preceded by reliable verification of the electronic identification means and its validity through a dynamic authentication.*
> *2. 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.*

LOA Guidance 2016

> *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 for 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 code (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.*

Article 4 of the RTS SCA & CSC regulation in PSD2 regulation

> *Introductory paragraph 4) Dynamic linking is possible through the generation of authentication codes which is subject to a set of strict security requirements. To remain technologically neutral a specific technology for the implementation of authentication codes*

> *should not be required. Therefore authentication codes should be based on solutions such as generating and validating one-time passwords, digital signatures or other cryptographically underpinned validity assertions using keys or cryptographic material stored in the authentication elements, as long as the security requirements are fulfilled.*
>
> *Article 4 Authentication code*
> *1. Where payment service providers apply strong customer authentication in accordance with Article 97(1) of Directive (EU) 2015/2366, the authentication shall be based on two or more elements which are categorised as knowledge, possession and inherence and shall result in the generation of an authentication code.*
>
> *The authentication code shall be only accepted once by the payment service provider when the payer uses the authentication code to access its payment account online, to initiate an electronic payment transaction or to carry out any action through a remote channel which may imply a risk of payment fraud or other abuses.*
>
> *2. For the purpose of paragraph 1, payment service providers shall adopt security measures ensuring that each of the following requirements is met:*
> *a) no information on any of the elements referred to in paragraph 1 can be derived from the disclosure of the authentication code;*
> *b) it is not possible to generate a new authentication code based on the knowledge of any other authentication code previously generated;*
> *c) the authentication code cannot be forged.*
>
> *3. Payment service providers shall ensure that the authentication by means of generating an authentication code includes each of the following measures:*
> *a) where the authentication for remote access, remote electronic payments and any other actions through a remote channel which may imply a risk of payment fraud or other abuses has failed to generate an authentication code for the purposes of paragraph 1, it shall not be possible to identify which of the elements referred to in that paragraph was incorrect;*
> *b) the number of failed authentication attempts that can take place consecutively, after which the actions referred to in Article 97(1) of Directive (EU) 2015/2366 shall be temporarily or permanently blocked, shall not exceed five within a given period of time;*
> *c) the communication sessions are protected against the capture of authentication data transmitted during the authentication and against manipulation by unauthorised parties in accordance with the requirements in Chapter V;*
> *d) the maximum time without activity by the payer after being authenticated for accessing its payment account online shall not exceed 5 minutes.*
> *…*

The authentication code requirement laid down in Article 4 of RTS SCS & CSC pertains to the same things as the requirements concerning dynamic authentication and the authentication mechanism's attack resistance specified in the eIDAS Regulation. This is evident in EBA Q&A 2018-4053 below, which discusses the security of the authentication code. The encryption requirement in section 7 of the regulation, for example, also governs the same issue in terms of the eIDAS Regulation.

> https://eba.europa.eu/single-rule-book-qa/-/qna/view/publicId/2018_4053
>
> *Article 4(2) of the Commission Delegated Regulation (EU) 2018/389 states that no information on any of the two elements necessary for strong customer authentication can be derived from the disclosure of the authentication code; that no new authentication code should be generated based on the knowledge of any other authentication code previously generated and that such code cannot be forged. Article 4(3) and 4(4) of the Delegated Regulation provides further requirements on authentication codes. Recital 4 of the Delegated Regulation states that "authentication codes should be based on solutions such as generating and validating one-time passwords, digital signatures or other cryptographically underpinned validity assertions using keys or cryptographic material stored in the authentication elements, as long as the security requirements are fulfilled". The*

Delegated Regulation does not specify the length for the authentication code. Accordingly, a three decimal-digit authentication code could be valid, providing that it complies with the requirements under the Delegated Regulation and in particular, that it is resistant against the risk of being forged in its entirety or by disclosure of any of the elements from which the code was generated.

Further, given that 'the authentication code shall be only accepted once' as stated in Article 4(1) phrase 2 of the Delegated Regulation meaning a 3-decimal digit authentication code would only give 1000 combinations, and since Article 4(3)(b) of the Delegated Regulation specifies the maximum of 5 failed authentication attempts, there is a higher probability of guessing the value of the authentication code.

3.3.12 Network security in identification service connections between the user and e-services.

The eIDAS Regulation and Regulation 72 require that telecommunications are secure (interfaces between the parties are discussed in more detail later on). Section 7 of the regulation defines the minimum level of TLS, the encryption requirement of the communications and the approved encryption algorithms. Encryption is also required on the message level to safeguard confidentiality.

Assurance Level Regulation Annex
2.3.1 Authentication mechanism
2. 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.

2.4.6 Technical controls
2. Electronic communication channels used to exchange personal or sensitive information are protected against eavesdropping, manipulation and replay.

LOA Guidance 2016

It has to be considered that communication channels may arise between different parties involved within an identification scheme, e.g. between the owner of the identification means and a service or between municipality and manufacturer.

One possibility for technical controls for communication channels are technical guidelines issued by an authority that gives requirements on cryptography and security measures to be used. This will typically be achieved using cryptographic protocols with described verification steps.

Requirements for communication channels between nodes of the eIDAS Interoperability Framework are given in the eIDAS Technical Specification for the framework.

For an information security management system according to ISO/IEC 27001:2013, this requirement is covered as part of the controls A.10 'Cryptography', A.13 'Communications security' and A.18.1.5 'Regulation of cryptographic controls', which may also include references to technical guidelines as stated above.

RTS SCA & CSC

Article 35 Security of communication session

> *1. Account servicing payment service providers, payment service providers issuing card-based payment instruments, account information service providers and payment initiation service providers shall ensure that, <u>when exchanging data by means of the internet, secure encryption is applied between the communicating parties throughout the respective communication session in order to safeguard the confidentiality and the integrity of the data, using strong and widely recognised encryption techniques.</u>*
>
> *2. Payment service providers issuing card-based payment instruments, account information service providers and payment initiation service providers shall keep the access sessions offered by account servicing payment service providers as short as possible and they shall actively terminate any such session as soon as the requested action has been completed.*
>
> *3. When maintaining parallel network sessions with the account servicing payment service provider, account information service providers and payment initiation service providers shall ensure that those sessions are securely linked to relevant sessions established with the payment service user(s) in order to prevent the possibility that any message or information communicated between them could be misrouted.*
>
> *4. Account information service providers, payment initiation service providers and payment service providers issuing card-based payment instruments with the account servicing payment service provider shall contain unambiguous references to each of the following items:*
> *a) the payment service user or users and the corresponding communication session in order to distinguish several requests from the same payment service user or users;*
> *b) for payment initiation services, the uniquely identified payment transaction initiated;*
> *c) for confirmation on the availability of funds, the uniquely identified request related to the amount necessary for the execution of the card-based payment transaction.*
> *[...]*

EBA statement EBA-Op-2018-04 makes some references to network security. The references may be connected to a dedicated interface offered to payment initiation service providers or account information service providers, which may, however, be a different interface than the interface offered to general identification or other payment service operators.

EBA-Op-2018-04

> 12
> *Table 1. Main requirements for dedicated interfaces and API initiatives*
>
> *Enabling a secure data exchange between the ASPSP and the PISP, AISP and CBPII, mitigating the risk of any misdirection of communication to other parties Articles 28 and 35 RTS*
>
> *Ensuring security at transport and application levels Article 97(3) PSD2 Articles 30(2)(c) and 35 RTS*

EBA Q&A 2018-4054 concerns encryption.

> https://eba.europa.eu/single-rule-book-qa/-/qna/view/publicId/2018_4054
>
> *Are EMV (Europay, MasterCard, Visa) transactions (for which the application cryptogram is not enciphered during its transmission) compliant with the RTS on strong customer authentication?*
>
> *In accordance with Article 22(1) of the Commission Delegated Regulation (EU) 2018/389 payment service providers are required to "ensure the confidentiality and integrity of the personalised security credentials of the payment service user, including authentication codes, during all phases of the authentication".*

> *In that regard, in the case where the issuer uses a cryptogram, which contains personalised security credentials, including authentication codes, the issuer would need to protect the confidentiality and integrity of the respective personalised security credentials in accordance with Article 22 of the Delegated Regulation, including during the transmission of the cryptogram. This also applies when the cryptogram is used as an authentication code.*
> *The issuer is responsible for ensuring compliance with the requirements of Article 22 of the Delegated Regulation.*

3.3.13 Authenticating parties to the communication channels

In PSD2 regulation, certain third-party operators utilising identification are required to use a qualified certificate in compliance with the eIDAS Regulation (electronic seal, i.e. a certificate for the 'system signature' or certificate for the authentication of the website).

The eIDAS Regulation does not contain similar specific requirements. Section 8 of Regulation 72 lays down general provisions on identifying parties within the trust network.

3.3.14 Other PSD2 matters

See EBA-Op-2018-04, which notes that the identification service can also be produced by some other operator besides the bank keeping the account.

EBA-Op-2018-04

> Section 38. *The articles mentioned above are to be read in conjunction with one another, which means that the PSP applying SCA is the PSP that issues the personalised security credentials. It is consequently also the same provider that decides whether or not to apply an exemption in the context of AIS and PIS. The ASPSP may, however, choose to contract with other providers such as wallet providers or PISPs and AISPs for them to conduct SCA on the ASPSP's behalf and determine the liability between them. The EBA also notes that a number of governmental (national) agreements on universal sets of personalised security credentials that can be used by PSUs with multiple PSPs already exist in some Member States.*

3.3.15 Questions concerning sections 3.3.9.–3.3.14

36) **PSD2 and eIDAS.** Does the PSD2 regulation contain general requirements on network encryption, which cannot be implemented technically, if the requirements on TLS (at least TLS 1.1) and encryption algorithms in section 7 of Regulation 72 are met?
37) **PSD2 and eIDAS.** Do sections on authenticating communicating parties (identification means provider, broker service, e-services) contain contradictory requirements or differences that should be reviewed?
38) **PSD2 and eIDAS.** The compatibility of the regulations has already been reviewed in connection with the 2018 interoperability review. Do the regulations contain technical requirements or differences concerning technical reliability or interoperability that should be reviewed in connection with the preparatory work of the Regulation due to potential compatibility issues?
39) **PSD2 and eIDAS.** Does a technical requirement connected to the PSD2 and eIDAS regulations prevent the provision and use of the same identification mean in general identification and payment transaction service identification?

3.4 Blockchain and self sovereign identity

3.4.1 The SSI eIDAS Legal Report issued by the European Commission

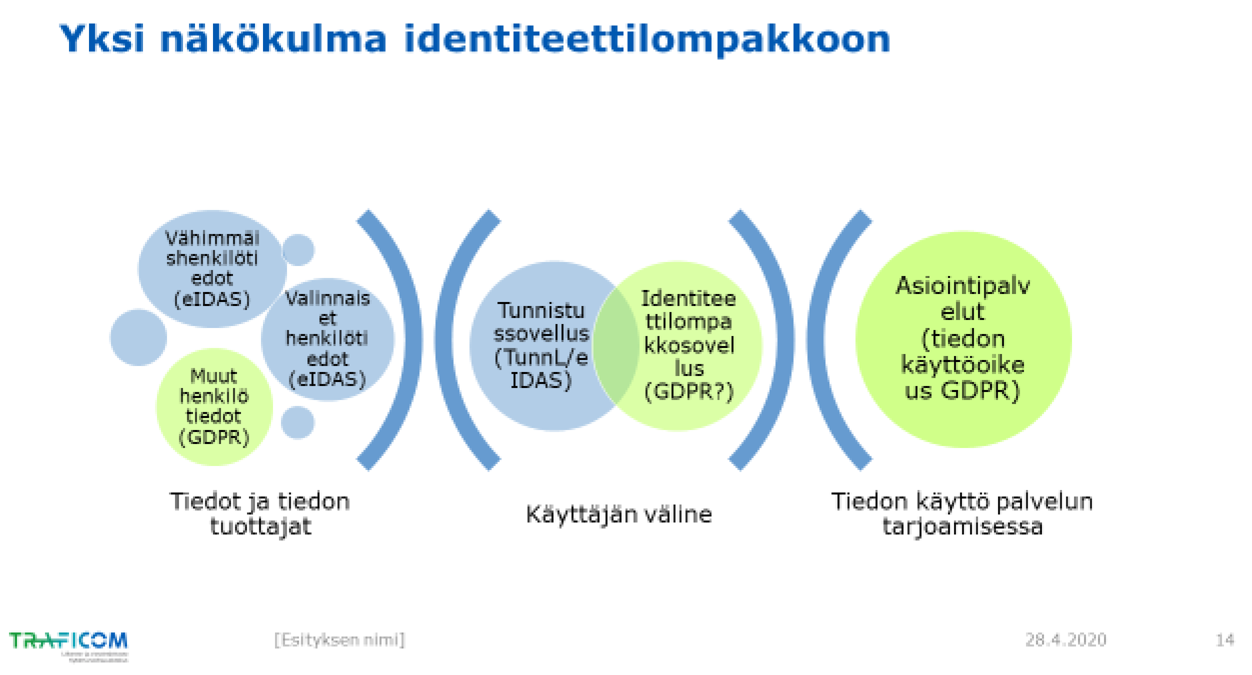
The current basic model of an electronic identification service could be characterised as follows: the identification service provider collects the personal data of the person applying for the identification means from reliable sources and connects them technically to the authentication factors of the identification means. During the service provision event, the person is authenticated to a relying party based on the authentication factors.

A blockchain may be considered a technical implementation method that identification services could utilise to process and authenticate data. SSI, in turn, could be considered a modern identification means that would allow the user to control the attestation of their personal data in various identification situations better than with the methods currently available without the identification service provider having to transmit the data between the parties. Apparently, in significantly more advanced development, the fundamental change of blockchain technology and PKI architecture can be seen to render the role of current identification services obsolete.

The European Commission has recently published a report on the relationship between blockchain technology, self sovereign identity and the eIDAS Regulation: *SSI eIDAS Legal Report, How eIDAS can legally support digital identity and trustworthy DLT-based transactions in the Digital Single Market* https://joinup.ec.europa.eu/sites/default/files/document/2020-04/SSI_eIDAS_legal_report_final_0.pdf

The report illustrates the technical foundation and the legal eIDAS foundation. It assesses various short-term and long-term development options and their relationship to the eIDAS Regulation. The short-term focus of the report is to assess the blockchain and SSI implementations in light of the valid eIDAS Regulation.

3.4.2 Image: identity wallet and personal data



Yksi näkökulma identiteettilompakkoon

Vähimmäi
shenkilöti
edot
(eIDAS)

Vallinnais
et
henkilöti
edot
(eIDAS)

Muut
henkilö
tiedot
(GDPR)

Tunnistu
ssovellus
(TunnL/e
IDAS)

Identitee
ttilompa
kkosovel
lus
(GDPR?)

Asiointipalv
elut
(tiedon
käyttöoike
us GDPR)

Tiedot ja tiedon tuottajat

Käyttäjän väline

Tiedon käyttö palvelun tarjoamisessa

TRAFICOM [Esityksen nimi] 28.4.2020 14

3.4.3 Questions concerning blockchain and SSI

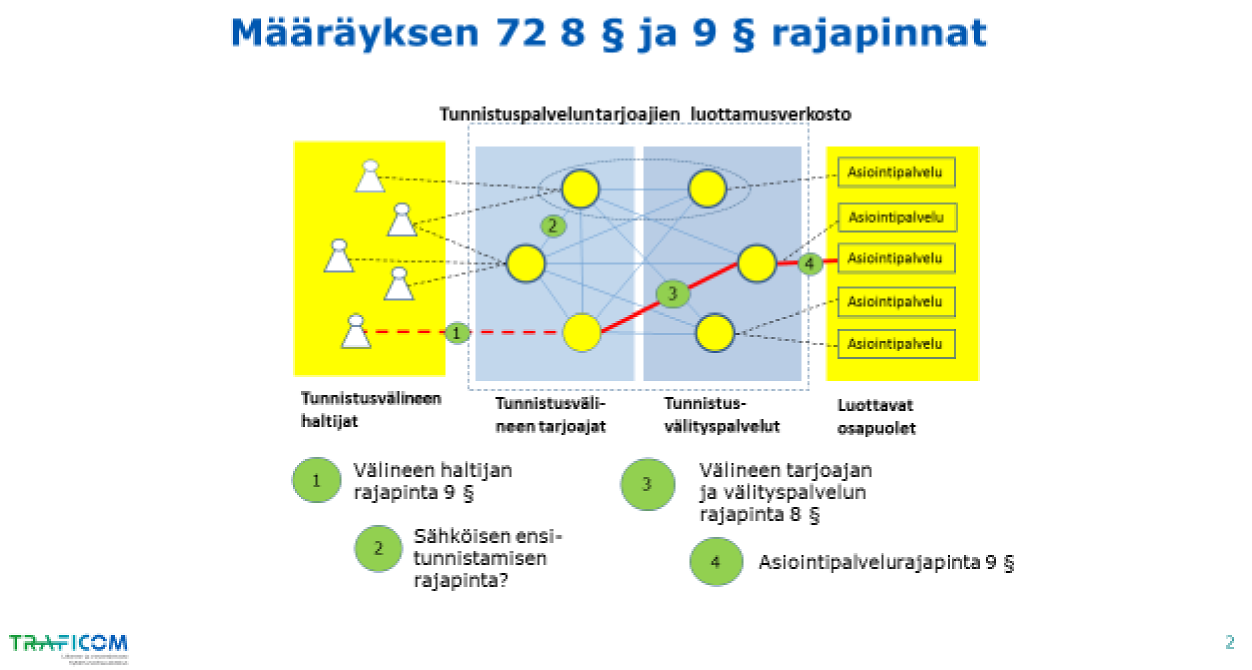
The following questions aim at determining the general maturity of the development and starting preparations for potential changes. According to the view of the Agency, the development and the European interpretation are not mature enough to promote the application and development of new technology by way of issuing regulations. We aim to determine whether the time is right for other technical guidance, information exchange or application discussions.

40) **Blockchain and SSI.** How do you view the relationship between blockchain technology and self sovereign identity and the supply of strong electronic identification services in general?
41) **Blockchain.** Do the current technical requirements concerning identification regulations contradict the utilisation of blockchain technology? Do you think this possible contradiction prevents the use of technology or is it rather that the application practice concerning blockchain technology is unclear?
42) **SSI.** Do the current technical requirements concerning identification regulations contradict SSI implementations? Do you think this possible contradiction prevents SSI implementations or is it rather that the application practice is unclear?
43) **Other technical development phenomena.** Are there any other developmental directions that should be taken into account in the technical regulations concerning identification services?

4 The interoperability of strong electronic identification (interfaces and attributes)

4.1 The trust network interfaces governed by the regulation

Image Trust network interfaces



Määräyksen 72 8 § ja 9 § rajapinnat

Tunnistuspalveluntarjoajien luottamusverkosto
Asiointipalvelu
Asiointipalvelu
Asiointipalvelu
Asiointipalvelu
Asiointipalvelu
1
2
3
4
Tunnistusvälineen haltijat
Tunnistusväli-neen tarjoajat
Tunnistus-välityspalvelut
Luottavat osapuolet

1 Välineen haltijan rajapinta 9 §

2 Sähköisen ensi-tunnistamisen rajapinta?

3 Välineen tarjoajan ja välityspalvelun rajapinta 8 §

4 Asiointipalvelurajapinta 9 §

The specified information security requirements of the regulation pertain to the following interfaces:

The interface between the identification means provider and identification broker service in image (3)
Information security requirements and recommended protocol for the interface.

The interface between the identification broker service and e-services in image (4)
Information security requirements pertaining to the interface.

4.1.1 Interface between the identification means holder and identification means provider

The interface between the identification broker service and identification means holder in image (1)
Information security requirements in section 9 pertain the interface. In addition to this, the requirements related to the security of the identification method and authentication mechanism affect the security requirements set for the interface.

See the assessment from the 2016 preparatory work of the Regulation:

The authority to issue regulations only covers the interface between the identification means provider and the identification broker service, which they offer from the trust network to e-services and identification means holders outside the network. As the various links within the identification event are executed within the same event from the point of view of the identification means holder, the requirements for the interfaces mentioned above also pertain to the interface between the e-services and the identification means holder indirectly.

The browser of the identification means holder is connected to the e-services, the identification broker service and the identification means provider during the course of the identification event. The connection between the identification means holder and the e-services could initially use http, but during the identification event, all identification means connections must utilise https and TLS version 1.2., or version 1.1. in exceptional circumstances, in accordance with section 7 of the regulation. In practice, the requirements are the same as between the identification means provider and the identification broker service provider.

4.2 Interfaces with no regulated technical requirements

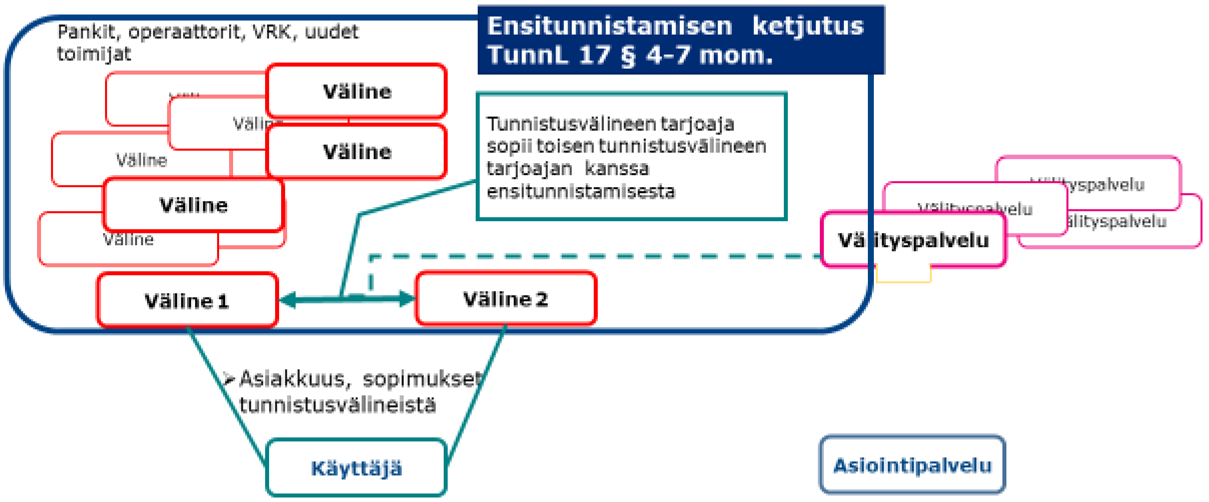
4.2.1 Initial enrolment

The interface in image (2) in section 4.1 depicting the interface between identification means providers refers to **the interface used for initial enrolment**. Other interfaces between identification means providers can be interpreted as interfaces between the identification means provider and the identification broker service, meaning that the requirements concerning those interfaces are also applied to these interfaces.

See the assessment from the 2016 preparatory work of the Regulation:

The interface for initial electronic enrolment (SAML/TUPAS) has been in use for several years now, because initial electronic enrolment was enabled in the Identification Act (section 17) before the trust network regulation was drafted. That is why it was not deemed meaningful to add requirements for the initial electronic enrolment interface to the regulation. The drafting process did, however, reveal long-term hopes that the interface could be used to transmit information on initial enrolment (e.g. the grounds on which electronic initial identification has been based: passport, identity card, electronic ID).

Image Initial enrolment using strong electronic identification means



Ensitunnistamisen ketjutus TunnL 17 § 4-7 mom.

Tunnistusvälineen tarjoaja sopii toisen tunnistusvälineen tarjoajan kanssa ensitunnistamisesta

- Ensitunnistus = tunnistusvälineen hakijan henkilöllisyyden varmistaminen (*verification, proofing*)
- Säännellyillä tunnistuspalveluilla tarjontavelvollisuuden, sopimusehtojen ja hinnan sääntely tunnistuslaissa
- Ensitunnistamisen ketjutus on vain yksi ensitunnistusmenettelyistä.

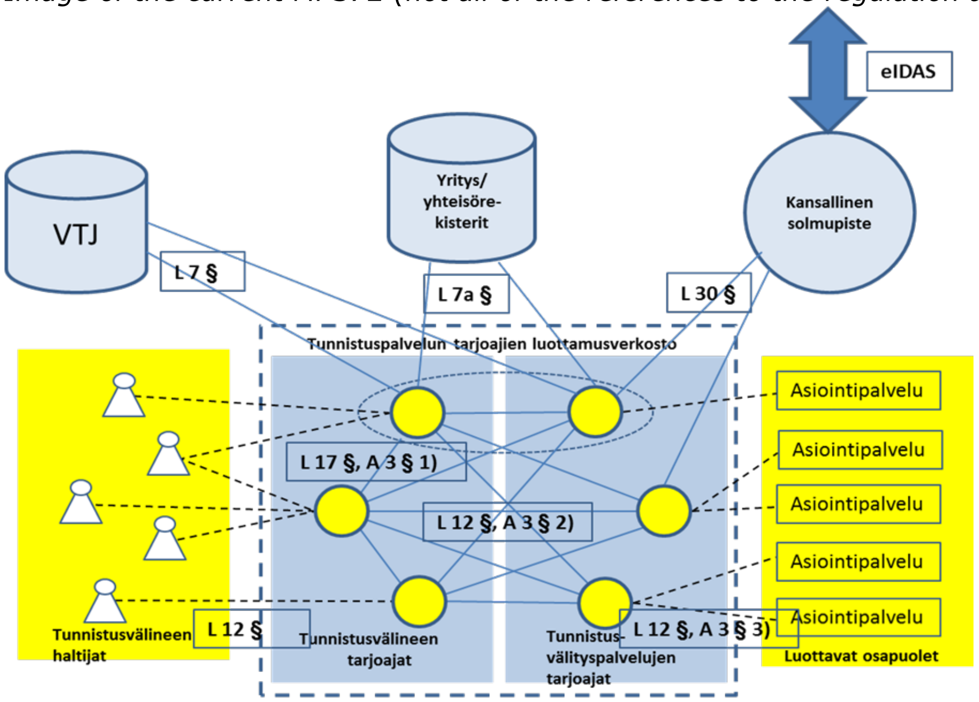
4.2.2 The interfaces of the population register system and the Business Information System

The Digital and Population Data Services Agency and the Finnish Patent and Registration Office determine their own interfaces for their customers.

4.3 The national node and suomi.fi

Section 10 of the regulation issues provisions on information security requirements between the identification broker service and the national node. In practice, the Digital and Population Data Services Agency maintains the national node in connection with or alongside suomi.fi identification. Suomi.fi is one of the e-services in the image. The following image also depicts the national node, the Population Information System and the Business Information System.

Image of the current MPS72 (not all of the references to the regulation are up to date)



4.4 Interface protocols (OIDC and SAML)

The regulation does not issue provisions on which protocol the regulated interfaces should employ. Section 14 of the regulation includes an informative provision stating that identification services must agree on the protocol and any features not specified in the regulation among themselves.

This freedom of contract is affected by the regulations within the Identification and Trust Services Act and the Government Decree on the trust network (the references to regulations in the decree predate the amendments to the Identification Act (412/2019), after which the obligations have been moved to different sections of the Identification Act).

> *Government Decree on the Trust Network for Providers of Strong Electronic Identification Services 2016/169*
>
> *Section 1 Luottamusverkoston tekniset rajapinnat* (Trust network technical interfaces)

> *Technical interfaces specified in subsection 2 of section 12 a of the act issued on strong electronic identification and electronic signatures (617/2009), hereinafter referred to as the Identification Act, are:*
> *1) interface between identification means providers;*
> *2) interface between an identification means provider and an identification broker service provider;*
> *3) interface between the identification broker service provider and relying party to the identification service.*
>
> *The identification service providers that belong to the trust network can agree on any interfaces needed to transmit transactions related to charges for identification data or on any other interfaces required for the trust network in compliance with subsection 3 of section 12 a of the Identification Act.*
>
> *Identification service providers belonging to the trust network must offer a technical interface that complies with an equally generally implemented standard on both interfaces specified in subparagraphs 1 and 2 of subsection 1.*

In the explanatory notes for the regulation, the Agency recommends that providers use the SAML 2.0 or Open ID Connect protocol and their nationally drafted profiles, which the Agency shall publish as separate recommendations (212/2018 S and 213/2018 S).

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 OpenIDConnect interface in some interfaces. As it is, OpenIDConnect is the prevalent protocol, but SAML is also used to some extent.

The interface recommendations 212 and 213 are being updated, and they may possibly be used to implement any necessary changes.

4.5 Questions concerning interfaces

44) **Regulation requirements concerning interfaces.** Do interface recommendations contain matters that need to be harmonised or streamlined by including them in the regulation? Which matters and why?
45) **E-service interface.** Should technical instructions (recommendations) be drafted for e-service interfaces?
46) **User interface.** Should technical instructions (regulation, guideline, recommendation) be drafted for user interfaces?
47) **Agreement on protocol.** Is section 14 of the regulation necessary?
48) **National node interface.** The interface between the node and the trust network may be significant, if any of the trust network identification means is notified to the Commission or if the node and identification broker service could be used to broker the identification of a foreign identification means user to a private, Finnish e-service. Does regulating the information security of the interface between the national node and the trust network (section 10) remain pertinent considering that the interface between the trust network and suomi.fi is covered by the requirements in section 9?

4.6 Attributes, filtering and enrichment

4.6.1 Attributes transmitted during identification (section 12)

The minimum information that a strong electronic identification service must be able to produce pursuant to section 12 of the regulation are an identifying ID (personal identity code or FINUID), name and date of birth. In addition to this, the regulation specifies certain voluntary data that the identification service may offer.

The minimum information and the voluntary information in the regulation correspond to the eIDAS requirements governing cross-border identification. The significance of this specific data compared to other possible personal data is that it has been determined in the Agency's recommended interfaces (recommendations 212 and 213/2018) and it corresponds to the eIDAS Regulation, which promotes cross-border interoperability. The production of this specified data in identification is also included in the trust network price regulations pursuant to section 12 c of the Identification Act.

The most common method of offering strong electronic identification is to transmit and verify the personal data of the user to the relying party during the event, which will allow for the individualisation of the identity. **However, the regulations concerning strong electronic identification are neutral in that the data may be filtered during the identification process to only verify that the user is over 18, for example.** Such verifications can be connected to the person based on the statutory log data of the identification service, meaning that even though they are anonymous to the e-service, they are pseudonymous in terms of personal data legislation.

In addition to the regulated data, the identification service may offer other **enriched data** in accordance with regulations concerning personal data protection or any industry-specific regulations. The enriching may be performed by the identification means provider or the identification broker service.
For the time being, strong electronic identification in Finland is only executed as transmitting the basic name and personal identity code combination.

4.6.2 Voluntary attributes

Tangible obligations to execute the optional attributes were assessed in 2018 in connection with the partial reform of the regulation (extending the Tupas transfer period).

The ability to transmit optional attributes means that the processing of optional attributes must be planned in the interface and the identification scheme so that the identification service provider has a concept of the technical operations required for the implementation.

The optional attributes do not require technical execution in the systems. Technical configurations must, however, observe the fact that the optional attributes included in identification messages may not impede with the identification event even when their use has not been agreed on.

Assessments from 2018 found that there is no need to require national identification to process the public/private attribute in national identification in any way differently than any other optional attributes would be processed or require it to be implemented according to an accelerated schedule.

4.6.3 Identification service provider insights 2018

The Agency surveyed the views of identification service providers and the Digital and Population Data Services Agency on the need to prepare for cross-border identification in connection with the preparatory work of the Regulation in spring 2018. In the Agency regulation, the matter is related to the determination of mandatory and optional attributes in the trust network interfaces.

The following is an excerpt from the summary of the statement published by the Agency on 3 May 2018.

Contrasting views were expressed on the necessity to determine optional attributes in general. Preparations for activities in accordance with the eIDAS Regulation were deemed well-founded and appropriate (the Population Register Centre) or unnecessary operations that would only generate costs (OP Financial Group). It was deemed useful to keep the requirements in the regulation to ensure that the matter is processed efficiently (the Finnish Competition and Consumer Authority), whereas there was one statement in favour of amending the requirements into recommendations (OP Financial Group).

Most statements did not deem the public/private attribute necessary on a national level at this stage (Finance Finland, Danske, Nordea, OP Financial Group). However, one opinion found the attribute necessary (Ålandsbanken) and one opinion was in favour of direct contact between the identification means provider and suomi.fi in investigating disruptions and fraud, which would speak for the necessity of separation (Nordea). On the other hand, there were opinions in favour of preparing for cross-border identification in this regard, as well (the Population Register Centre).

Even though optional attributes were not considered necessary at this time, the need and demand for cross-border identification in terms of both natural and legal persons were considered essential in terms of business operations (Danske, Nordea, OP Financial Group, Nets, Signom). The statements highlighted wishes to extend national node services to the private sector (OP Financial Group, Signom).

4.7 Questions concerning attributes

49) **Relationship between a recommendation and a regulation.** There are recommendations concerning the specification of attributes on SAML and OpenIDConnect interfaces designed to harmonise the processing of minimum and optional attributes. Are there any issues in the relationship between a regulation and a recommendation that should be reviewed in connection with the preparatory work of the Regulation?
50) **Minimum attributes.** Is there any information in addition to attributes harmonised with EU regulations that should be reviewed in connection with the preparatory work of the Regulation?
51) **Optional attributes.** Is there any information in addition to attributes harmonised with EU regulations that should be reviewed in connection with the preparatory work of the Regulation?
52) **Public/private relying party**. Do you think there is a need in national identification for information on whether a private or a public e-service has requested identification – e.g. due to disruption data exchange, information security or pricing?
53) **Legal persons.** Are there any matters related to the strong electronic identification of legal persons that need to be reviewed during the preparatory work of the Regulation?
54) **Foreign identified parties.** Do operators in the private sector e-services need strong electronic identification for foreign natural persons and legal persons? Which attributes would be best for these situations?
55) **General information on attributes.** What else would you like to express about attributes?

5 Cross-border identification

5.1 The eIDAS Regulation and the national node

Cross-border identification refers to the user identifying themselves using an identification means issued in one country in an e-service in another country. The notification regulation in the eIDAS Regulation only pertains to public e-services, meaning that there needs to be a differentiation of cross-border identification between public and private sector e-services.

In the future, identification means notified by Finland may be used for identifying with foreign public e-services, and conversely, identification means notified abroad may be used to identify with Finnish public sector e-services thanks to the notification process. Finland has not notified an identification means as of yet.

Identification events between Finland and other countries are transmitted via the national node (PEPS, Pan European Proxy Server) maintained by the Digital and Population Data Services Agency.

Identification means providers identify in *foreign public sector* e-services through the national node using Finnish means and an identification broker service. Identification in *Finnish public sector services* using a foreign identification means is executed through the national node and suomi.fi identification.

The technical interoperability of the interfaces and the uniform specification of the transmitted data are essential to enable identification in practice. The interoperability and security requirements of cross-border identification in accordance with the eIDAS Regulation are laid down in Commission Regulation (EU) 2015/1501.

Section 13 of the Agency's regulation on Electronic Identification and Trust Services discusses cross-border identification from the trust network through the national node. The interface between the nodes is defined in EU cooperation, but the national interface between the identification broker service (trust network) and the node must be specified nationally. According to the regulation concerning the interface, the same general requirements as those pertaining to the interface between the identification means provider and identification broker service are applied to the interface. Otherwise, the identification broker service provider and the party implementing the node must agree on the characteristics of the interface together. It is appropriate, though, that the selected protocol is a protocol that is already being used by the trust network (OpenID Connect or SAML).

The Agency's regulation on Electronic Identification and Trust Services promotes cross-border identification by way of specifying the mandatory and optional attributes transmitted in the trust network interfaces in section 12 and harmonising them with the eIDAS Regulation. The optional attributes are likely to be very useful in cross-border identification as additional information, as the Finnish personal identity code may not be sufficient to identify a person in another country.

In addition to the above, section 17 of the regulation specifies the ISO/IEC 27001 standard and the European Commission Implementing Regulation (EU) 2015/1501 as assessment criteria for the information security of the national node.

56) **Cross-border identification for the public sector.** Is the above assessment based on the preparatory work of the Regulation from 2016 and 2018 correct?
57) **Cross-border identification for the public sector.** Does section 13 of the regulation need to be amended?
58) **Assessment criteria.** Should the national node information security assessment criteria be reviewed during the preparatory work of the Regulation?

5.2 Cross-border identification broker services in the private sector (private identification broker services)

There are currently no regulations or harmonised definitions pertaining to the use of the national node for identification to private e-services in the EU or in Finland.

In the first phase, the national node will focus on identification in public administration e-services, and only in the second phase will the possibilities of implementing identification in private e-services be explored in more detail.

Because the national node is not available for identification with private e-services for the time being, identifying customers using foreign identification means in Finnish e-services can be executed contractually, much like using Finnish identification means for identification in foreign private sector e-services. The reliability of foreign identification services could be verified based on the notification process, any control measures or regulations issued by the home country of the identification service, or contractually.

If an identification service within the trust network wants to start brokering strong electronic identification services abroad, the same requirements that pertain to service provision to domestic e-services are also applied to the interface between the identification broker service and the e-services, as well as their contractual relationship. In this event, the regulation and monitoring performed by the Finnish Traffic and Communications Agency cover the requirements for identification broker services laid down in the Identification Act and the Agency regulation.

According to the Agency, the identification broker services of the trust network also provide the identification of Finnish customers in other countries, but the Agency has not investigated the scope of the activities. Many identification broker services are provided by Nordic companies (e.g. Nets, Signicat, Danske, Nordea, Telia), meaning that they also have other activities in several countries.

59) **Private cross-border identification.** Is the above assessment correct?
60) **Private cross-border identification.** Do cross-border identification broker services contain aspects that should be examined in connection with the preparatory work of the Regulation?

6 Assessing the conformity of identification services

6.1 Assessment bodies

According to the Identification and Trust Services Act and the eIDAS Regulation, assessing the conformity of identification services is mandatory and must be reported to the supervisory authority by way of issuing an assessment or auditing report. Depending on the service, the assessor may be a FINAS accredited conformity assessment body, other external assessment body or an internal inspection body.

The regulation specifies the criteria according to which the independence and competence of the conformity assessor can be assessed objectively. The criteria are primarily based on general, international and national standards, regulations and instructions.

Sections 18 and 19 of the regulation determine examples of international standards or regulatory or self-regulatory frameworks on which the independence and competence of the assessment body may be based. These listings are not exhaustive, and a similar objective standard or set of rules may also be used to demonstrate competence.

6.1.1 Standards for demonstrating the independence and competence of an assessment body

> ***Section 18 Requirements concerning an external assessment body of the identification service***
>
> *The independence and competences of an assessment body, referred to in section 33 of the Identification and Trust Services Act, may be proven through one of the following:*
> *1) accreditation based on standard ISO/IEC 27001 or other proof of the competence to perform assessments according to the standard;*
> *2) competence proven according to an internationally renowned self-regulation arrangement based on WebTrust guidelines;*
> *3) accreditation based on the PCI DSS payment card standard or other proof of the competence to perform assessments according to the standard;*
> *4) competence proven according to the ISACA standards and IT management framework; or*

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

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

The independence of an internal notified body, referred to in section 33 of the Identification and Trust Services Act, may be proven through one of the following:
1) *compliance with the IIA standards for professional practice (independence and objectivity of internal auditing, including organisational independence);*
2) *compliance with the ISACA standards and IT management frameworks;*
3) *compliance with the BIS (Bank for International Settlements) internal audit guidelines;*
4) *compliance with the guidelines on internal auditing of the FIN-FSA Regulations and Guidelines;*
5) *compliance with the regulations and guidelines on internal auditing of the FIN-FSA Regulations and Guidelines;*
6) *compliance with instructions or regulations issued by the corresponding supervisory authorities of other EEA Member States; or*
7) *compliance with other comparable standards concerning public control or overall independent internal audit management.*

61) **Assessment body requirements.** Are the lists of standards and regulations in sections 18 and 19 of the regulation up to date? Are the sources listed relevant? Is anything missing?
62) **Assessment body requirements.** Which of the listed standards and regulations do you or your assessment body utilise?

6.1.2 Assessment standards

During the preparatory work of the Regulation, the working group for the explanatory notes of the Regulation was asked to provide examples of standards and other sources that companies entered in the identification service register use for assessment according to the survey. These standards could also be suitable for the identification system assessment. Neither the drafting process nor explanatory notes specify the grounds for independence or competence or provide an assessment of which parts of the sources could be used for identification system requirement assessment.

Example list
- ISO 27001
- PCI DSS, PCI/QSA
- Webtrust Trust Services Principles and Criteria for Certification Authorities and Webtrust for Certification Authorities - SSL Baseline Requirements Audit Criteria
- Information Security Forum (ISF) "Standard of Good Practice"
- ISF IRAM criteria (Information Risk Analysis Methodology)
- ETSI TS 101456 (CA policy)
- ISRS 4400 and ISAE 3000
- KATAKRI
- Vahti
- Regulations or instructions issued by the European Central Bank or the Financial Supervisory Authority
- Financial Supervisory Authority regulation and guideline 2.4 'Customer due diligence; Prevention of money laundering and terrorist financing'
- European Central Bank Cybersecurity questionnaire 2015
- BIS (Bank for International Settlements) guideline External audits of banks

63) **Assessment requirements.** Are the sources in the explanatory notes on the regulation relevant? Is anything missing?
64) **Assessment requirements.** Which of the listed standards and regulations do you or your assessment body utilise?
65) **Assessment guideline.** Would it be more appropriate to move the standard examples and sources to Guideline 211/2019 from the explanatory notes?

6.2 Assessment criteria

The following matters were discussed in the 2016 preparatory work of the Regulation: How precise should the identification service assessment criteria, i.e. auditing criteria, be in the regulation? The options were a detailed uniform set of criteria or a more general set of criteria, which would be completed with an application recommendation.

Based on the impact assessment, a headline-level list of things that the assessment must cover was included in section 15 of the regulation. The matters on the list would need to be drafted in general terms and they should be based on the requirement grouping in accordance with the EU Assurance Level Regulation.

> *Section 15 Assessment criteria*
>
> *(Subsection 1) The identification service assessment shall cover the requirements concerning the following:*
> 1) *certain properties of the functions affecting the provision of the identification service (the identification scheme), namely:*
>   a) *information security management*
>   b) *record keeping*
>   c) *facilities and staff*
>   d) *technical measures*
> 2) *the identification method, meaning certain properties of the identification means, namely:*
>   a) *application and registration*
>   b) *identity proofing and verification of the applicant*
>   c) *identification means characteristics and design*
>   d) *issuance, delivery and activation*
>   e) *suspension, revocation and reactivation*
>   f) *renewal and replacement*
>   g) *authentication mechanisms.*
>
> *(Subsection 2) The assessment of the aspects referred to in paragraph 1 above shall be based on the requirements of the Identification and Trust Services Act and this Regulation, the rules and guidelines of the EU or other international body, published and universally or regionally applied information security guidelines, or widely adopted information security standards or procedures.*

The purpose is to enable operators to utilise those sets of assessment criteria that they would otherwise use flexibly. On the other hand, the operators must assess and ensure that the sets of criteria they employ based on various standards truly do cover all of the required areas of assessment applied to identification systems. While performing its duty of overseeing audit reports, the Agency must assess that this is realised.

The Agency has drafted 'Guideline 211/2019 Model criteria for identification service provider audits' in cooperation with the industry. It was drafted to update the previous instructions in guideline 211/2016 on the auditing criteria and guideline 215/2016 on electronic identification and trust services audit reports.

It is the Agency's understanding that section 15 of the regulation and the updated identification service assessment guideline 211/2019 form a functional framework, which still allows for the utilisation of information security assessment carried out for other reasons. In the Agency's estimate, it is not necessary to change this framework considerably to allow for establishing the practices in assessments performed every two years.

66) **Assessment criteria.** In your opinion, is the level of accuracy concerning the assessed matters in section 15 of the regulation practical?
67) **Assessment criteria.** Do you think the criteria or assessment criteria should be reviewed during the preparatory work of the Regulation? Do the criteria need to be specified in some regard?
68) **Identification systems and subcontractors.** Should the preparatory work of the Regulation review questions concerning identification system architecture and subcontracting?
69) **Assessment guideline.** Is the assessment guideline practical or does it need to be amended?

6.3 Declaration of compliance with other requirements (section 16)

Section 16 of the regulation is a collection of areas related to the reliability of identification service providers. Compliance with these requirements can be demonstrated with a report by the company in connection with a start or change notification. This means that these requirements do not warrant an assessment or audit by an independent assessment body.

> *Section 16 Declaration of compliance with other requirements*
>
> *The identification service provider shall provide proof, by means of either a written self-declaration or an assessment referred to in section 15 above, of its compliance with the following requirements related to the reliability of the identification service provider and the information provided on the identification service:*
> 1) *published notices and user information, such as identification principles, price lists and terms and conditions*
> 2) *established organisation*
> 3) *preparedness to bear risks of damage*
> 4) *sufficient financial resources*
> 5) *responsibility for subcontractors*
> 6) *planning for the termination of operations.*

Agency Guideline 214/2016 O on electronic identification and trust service notifications discusses data or annexes that must be attached to the notification. There is, however, no detailed application guideline concerning this data.

70) **Other requirements for identification service providers.** Do the regulation or notification guidelines contain sections that need to be changed and reviewed in connection with the preparatory work of the Regulation?

7 Trust services and their assessment in the eIDAS Regulation

Chapters 6–8 of the regulation lay down provisions on the qualified trust services specified in the eIDAS Regulation, their compliance assessment bodies as well as electronic signature or seal creation tool certification.

Chapter 6 Qualified trust services
Section 20 Assessment criteria for a qualified trust service provider
Section 21 Assessment criteria for a qualified trust service

Chapter 7 Conformity assessment bodies of trust services
Section 22 Evaluation of the competence of assessment bodies

Chapter 8 Certification of qualified electronic signature or electronic seal creation devices
Section 23 Requirements for electronic signature or seal creation devices
Section 24 Requirements for certification bodies

The purpose of the regulation is to

- complete the requirements set for qualified electronic trust services and the independence and competence criteria of their compliance assessment insofar as they are not regulated by European Union legislation, and
- complete the certification criteria of electronic signature or seal creation tools insofar as they are not regulated by European Union legislation.

The authority to regulate is restricted and it must carefully observe EU regulations and the status of international standards.

According to an estimate by the Agency, the amendment to the regulation must first and foremost observe the progress of ETSI standardisation work. The preparatory work of the Regulation must also pay attention to the ongoing re-evaluation of the eIDAS Regulation and any Commission implementing regulations concerning trust services and assessment bodies.

The following are pertinent sources:

Link: ETSI Digital signature

Link: ETSI standards and full list

Link: Commission eIDAS-observatory

Link: Commission eIDAS website

Link: Commission page on the eIDAS Regulation and implementing regulations

Link: Commission consultations (the eIDAS consultation will be executed in June based on preliminary information)

The Agency has requested a separate statement on matters related to trust services and assessment bodies in relation to the eIDAS Regulation (Register number Traficom/9355/09.02.00/2020), and any replies will be observed in assessing the need to make changes to the regulation.

71) **Qualified trust services.** Does the regulation need to be changed in terms of trust services? Do you think the conformity of qualified trust services should be assessed based on some other standards besides ETSI? Which ones?
72) **Accredited assessment bodies.** Does the regulation need to be changed in terms of assessment bodies?
73) **Certification bodies.** Does the regulation need to be changed in terms of certification bodies?
74) **Impact.** Has the regulation had an impact on the supply of qualified trust services?
