Assessment guideline for electronic identification services

211/2023 O

Traficom Guideline

Contents

1 Introduction

This document applies to conformity assessments for electronic identification services and the assessment reports that are used to report the results of these assessments.

Attached to the document is a general set of criteria for the conformity assessment of strong electronic identification services and a set of criteria created especially for mobile applications.

The document also features a checklist for assessment report contents.

The document applies to identification services that are registered or intend to register as strong electronic identification services as required by sections 10 and 11 of the Identification Act. This applies to providers of electronic identification means as well as identification broker services.

1.1 Purpose of the Guideline

The document is intended for providers of strong electronic identification services and assessment bodies that provide assessment services for identification services.

The document is intended to clarify the requirements of service audits so that the audits cover all the required subject areas. Assessment criteria can be based on the criteria specified in this document, other criteria or combined criteria that cover all the subject areas that are required to be assessed. Following the model criteria presented here is therefore not a requirement; it is merely one way of ensuring that the scope of the assessment is sufficient.

As a result of the audit, an identification service assessment report is provided to Traficom. The purpose of this Guideline is to provide instructions and clarification for the minimum content and the presentation of the assessment report.

Under section 42 of the Act on Strong Electronic Identification and Electronic Trust Services (617/2009), it is Traficom's duty to monitor compliance with the Act and the EU's eIDAS Regulation[1]. This Guideline has been issued pursuant to the general guidance and monitoring authorisation referred to in section 42 of the Act.

A separate guideline has been published on the notifications to be submitted to Traficom (214/2023 O). The eIDAS Regulation and the Electronic Identification Assurance Level Regulation (LoA) provide for the conformity assessment of an electronic identification means to be notified to the EU.[2].

1.2 Entry into force of the Guideline

Guideline 211/2023 O will enter into force on 13th July 2023.

The Guideline is valid until further notice and may be supplemented and amended as necessary. In that case, the guideline number will remain the same, but the date and the year will be changed as required. The modified versions of the guideline are listed in the table below.

[1] Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.
[2] 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.

The current guideline is published on the Traficom website at https://www.kyberturvallisuuskeskus.fi/en/electronic-identification.

Version	Date	Description/change	Author
211/2023 O, Traficom/ 20767/ 09.02.00/2022	13 July 2023	3rd published version ▪ added criteria related to remote initial identification ▪ added criteria applicable to wallet solutions	Finnish Transport and Communications Agency (Traficom), NCSC-FI
211/2019 O	9 Oct 2019	2nd published combined version ▪ Amended the general criteria by reducing the number of items and by listing them based on regulatory requirements. ▪ Added a new set of special criteria for mobile apps used for electronic identification. ▪ Incorporated updated guidelines on assessment reports of identification services from document 215/2016 O.	Finnish Transport and Communications Agency (Traficom), NCSC-FI
211/2016 O Model criteria for identification service provider audits 215/2016 O Identification and trust service assessment reports	2 Nov 2016	First published versions	Finnish Communications Regulatory Authority (FICORA), NCSC-FI

1.3 References to regulations and standards; abbreviations

The overall assessment criteria of identification services is based on the requirements set for strong electronic identification.

The criteria for mobile apps is based on standards and has been complemented with additional criteria based on regulatory requirements. The mobile app criteria also include references to the applicable regulatory requirements.

The assessment report guidelines are based on regulatory requirements.

Provisions with requirements for identification services include:

- The Act on Strong Electronic Identification and Electronic Trust Services (617/2009, hereinafter referred to as the *Identification Act*, *ITSA* or *Identification and Trust Services Act*)

- Commission Implementing Regulation (EU) 2015/1502 (hereinafter referred to as *LoA* or the *Assurance Level Regulation*)
  - The sections on Assurance Level Regulation referenced in the Identification Act
  - LoA Guidance (unofficial guide for the application of the Assurance Level Regulation)[3]

- Traficom Regulation M72B/2022 (hereinafter referred to as *M72B*)[4]
  - This Regulation complements certain requirements set out in the Identification Act.

References to standards[5]:
- ISO/IEC 27001:2013/2017 Information security management
  - The requirements of the general criteria contain references to the relevant requirements of standard ISO 27001. The purpose of the references is to facilitate the integration of identification service conformity assessments into more general assessments of information security management.
- OWASP Mobile AppSec Verification v.1.4.2[6]
- ISO/IEC 29115
- ISO/IEC 15408-1
- ISO/IEC 18045
- ISO/IEC TS 29003:2018
- ISO/IEC 30107
- ETSI TS 102 165-1
- ETSI TS 119 461
- Common Criteria CCDB 2009 03

Assurance level abbreviations used in tables:
- S=substantial (corresponds to eIDAS2, *substantial*)
- H=high (corresponds to eIDAS3, *high*)

1.4 Definitions of identification service

Strong electronic identification means an identification service that meets the requirements of the Identification Act and the provision of which has been notified to the Finnish Transport and Communications Agency for registration.

Identification service is a combined term for identification means providers and identification broker services that are used in both the relevant regulations and this document.

Identification means provider offers electronic identification means to end users.

Identification broker services provide identification events for providers of eServices, i.e. for parties relying on electronic identification.

[3] https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/LoA_Guidance.pdf
[4] Regulation M72B/2022 on Electronic Identification and Trust Services https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/M72B_2022_M%C3%84%C3%84R%C3%84YS_72B_tunnistus-_ja_luottamuspalvelut_ENG_julkaistu.pdf
[5] The following background material has also been used in the preparation of the criteria: FIDO Security Reference: https://fidoalliance.org/specs/fido-v2.0-id-20180227/fido-security-ref-v2.0-id-20180227.html
[6] https://www.owasp.org/index.php/OWASP_Mobile_Security_Testing_Guide

Providers of strong electronic identification services, which have registered with Traficom (as required by the Identification Act) and meet the requirements of the law, form a *trust network* for electronic identification.

This document has been created from the perspective of the requirements that apply to the functions of the identification service, not from the perspective of the roles of the different parties. Section 2.3 provides a detailed definition of what is meant by an identification means and an identification scheme.

Definitions in provisions

ITSA, section 2 Definitions

1) strong electronic identification means the identification and verification of the authenticity and correctness of the identifying information of a person, legal person or a natural person representing a legal person by electronic means that fulfils the requirements of assurance level substantial referred to in Article 8 (2 b) of the EU Regulation on Electronic Identification and Trust Services or assurance level high in Article 8 (2 c);

3) identification service provider means a provider of an identification broker service or a provider of an identification means;

4) provider of an identification means means a service provider that offers or issues electronic identification means for strong electronic identification to the general public and offers in the trust network their electronic identification means for a provider of an identification broker service to be distributed;

5) provider of an identification broker service means a service provider that forwards strong electronic identification events to a party that relies on electronic identification;

10) trust network means a network of identification service providers that have submitted a notification to the Finnish Transport and Communications Agency.

1.5 Overall reliability of the service provider (not part of the criteria)

Independent audits are not required to cover the overall reliability of the service provider or the information concerning the service that is provided to the users and the relying parties, such as identification principles, terms and conditions, or price lists. Because of this, overall reliability is not addressed in these criteria.

These questions are adequately covered by a **self-prepared report submitted by the identification service provider** to Traficom for assessment. The matters that are required in the report are listed in section 16 of Regulation M72B.

The information to be submitted to Traficom with notifications on commencing, terminating or changing of operations is described in further detail in **Guideline 214/2023 O Electronic identification and trust service notifications**.

PROVISIONS

M72B, Section 16: Report on the reliability of the identification service provider and the published data

In a notification made in accordance with section 10 of the Identification and Trust Services Act, the identification service provider shall provide proof, by means of either a written self-declaration or an independent and qualified notification or assessment of its compliance with the following requirements related to the reliability of the identification service provider and the information provided on the identification service:

1) an established legal person in charge of the identification service and the competency and reliability of the persons in charge;

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

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

4) responsibility for subcontractors; as well as

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

2 Identification service assessment and the assessment report

2.1 Submission of the assessment report as an attachment to a notification

PROVISIONS

ITSA, section 10: An identification service provider's obligation to notify commencement of operations

An identification service provider based in Finland who intends to offer services shall, prior to commencement of such services, submit a written notification to the Finnish Transport and Communications Agency. Such notification may also be submitted by a consortium of identification service providers, if such services provided can be deemed as one and the same identification service.

The notification shall contain:

[…]

5) an assessment report on the independent audit drawn up by a conformity assessment body, other external assessment body or an internal assessment body pursuant to section 29;

[…]

The identification service provider shall notify the Finnish Transport and Communications Agency in writing and without delay of any changes to information referred to in subsection 2. A notification shall also be submitted if business operations are discontinued or transferred to a different service provider.

ITSA, section 11: An identification service provider based in another member state of the European Economic Area

The provisions of section 10 will not prevent an identification service provider based in the EEA from submitting a notification referred to in the section.

ITSA, section 31: Assessment report

The identification service provider and the Digital and Population Data Services Agency must obtain an assessment report of the conformity assessment and submit it to the Finnish Transport and Communications Agency.

The assessment report is in force for the period specified in the standard that was used in the assessment, but not longer than two years.

2.1.1 Commencement notification

When a new identification service provider notifies Traficom that it will commence operations, an assessment report must be submitted as an attachment to the notification.

2.1.2 Change notification

When an identification service provider notifies Traficom of a material change in the identification scheme, an assessment report must be submitted as an attachment to the notification.

If a material change in the operations occurs, an assessment must be carried out, and a notification of the change and an assessment report must be submitted before the change is transferred to production.

Examples of material changes include:

- Changes of the identification means, i.e. the authentication factors and the authentication mechanism.
- Technical changes in the identification scheme, i.e. changes in the structure of the maintenance and the production systems, key software components or other key components or elements.
- Changes in or replacement of subcontractors that supply maintenance services, hardware, systems or software.
- Changes in the mobile app and/or the related operating systems if the continuous risk management of the identification service and risk assessment suggest that such changes require an information security audit between the periodic assessments.

2.1.3 Periodic assessment

An assessment report must be submitted to Traficom when two years have passed since the completion of the previous assessment report.

According to law, the identification service assessment report is in force for the period defined in the standard that is applied, but no more than for two years. The validity of the assessment report, i.e. up to two years, is calculated from the date when the previous assessment report was completed. The identification service provider must submit a new assessment report to Traficom within two years of the completion of the previous assessment report, if it wishes to continue the provision of a strong electronic identification service.

The assessment report may be based, in whole or in part, on standards with a defined assessment frequency of less than two years. It is the responsibility of the identification service provider to ensure that in such cases, the frequency of assessments follows the one defined in the standard. The identification service provider must submit an informal notification to Traficom whenever an area of the assessment report has been reassessed and the new assessment is valid. The assessment report referred to in this Guideline must be submitted within two years of the completion of the previous assessment report.

Traficom aims to process the regular assessment reports of all identification service providers at the same time and publishes a date on which the assessment reports must be submitted at least six months prior to the date in question.

The minimum contents of the notification of commencing operations and change notifications are described in Traficom Guideline 214/2023 O.

2.2 Areas of identification services subject to assessment

An independent conformity assessment is required for the matters specified in the Identification Act and described in further detail in Traficom's Regulation M72B.

The assessment body may use the criteria set in these guidelines or another equivalent set of criteria or method, as long as the assessment body is able to prove in the assessment report that the method demonstrates compliance with the regulatory requirements.

Annex B of the document constitutes the general assessment criteria for identification services that cover all requirements independently of the implementation of the identification means and the identification scheme.

Annex C provides assessment criteria for mobile apps intended to complement the general criteria in cases where the identification means or the identification scheme incorporates a mobile app.

Section 16 of the Regulation specifies the requirement items on which the identification service provider may submit its own report.

All sections apply to providers of **identification means**.

Section 15, subsections 1a to 1e and subsection 2g of Regulation M72B apply to **identification broker services**.

PROVISIONS

ITSA, section 29: Conformity assessment of an electronic identification service

An identification service provider must regularly subject their service to an assessment by an assessment body referred to in section 28 to determine whether the identification service meets the requirements on interoperability, information security, data protection and other reliability laid down in this Act.

[…]

ITSA, section 42: General guidance and regulations by the Finnish Transport and Communications Agency

[…]

The Finnish Transport and Communications Agency may issue more detailed regulations on:

[…]

5) the criteria for assessing the conformity of an identification or trust service and the national node referred to in sections 29, 30 and 32;

[…]

M72B, section 15: Conformity assessment criteria

15.1 Identification scheme and identification means features to be assessed

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

1) certain properties of the functions affecting the provision of the identification service (the identification scheme), namely:

a) information security management;
b) record keeping and data processing;
c) facilities and staff;
d) technical measures (controls); and
e) interoperability in the trust network; as well as

2) the identification means, meaning certain properties of the identification means, namely:

a) application and registration;
b) identity proofing and verification of the applicant;
c) identification means characteristics and design;
d) issuance, delivery and activation;
e) suspension, revocation and reactivation;
f) renewal and replacement; and
g) authentication mechanisms.

15.2 Assessment criteria

The conformity assessment may be based on the assessment guideline issued by the Finnish Transport and Communications Agency or the rules and guidelines of the EU or other international body, published and universally or regionally applied information security guidelines, or widely adopted information security standards or procedures. The assessment may be based on a combination of several sources mentioned above.

2.3 Identification means, identification scheme and subcontractors

2.3.1 Definitions

Identification means refers to an identification means offered to the user and the technical implementation of identification events.

An identification means includes authentication factors and the authentication mechanism.

Identification scheme refers to the technical and organisational unit formed by the identification service, which is governed by the requirements set out in the regulations on strong electronic identification.

An identification scheme includes the identification service provider's own or subcontracted data connections, information systems, maintenance, data processing, information security management and other items specified in the regulations.

Definitions in provisions

ITSA, section 2: Definitions

2) identification means means an electronic identification means referred to in Article 3(2) of the EU Regulation on Electronic Identification and Trust Services;

Cf. ITSA, section 8: Requirements posed on the electronic identification scheme.

Cf. ITSA, section 8 a: Authentication factors used in the identification means.

Article 3 of the eIDAS Regulation

2) 'electronic identification means' means a material and/or immaterial unit containing person identification data and which is used for authentication for an online service;

4) 'electronic identification scheme' means a system for electronic identification under which electronic identification means are issued to natural or legal persons, or natural persons representing legal persons;

Cf. eIDAS, Article 7: Eligibility for notification of electronic identification schemes.

...c) the electronic identification scheme and the electronic identification means issued thereunder meet the requirements of at least one of the assurance levels set out in the implementing act referred to in Article 8(3);

Cf. eIDAS, Article 8: Assurance levels of electronic identification schemes.

PROVISIONS ON SUBCONTRACTING

ITSA, section 13: General obligations of an identification service provider

[...]

The identification service provider is responsible for the reliability and functionality of services and products provided by persons contributing to the identification service process.

2.3.2 Assessment and subcontractors

As the provision of identification services often comprises only a part of a company's or organisation's operations, information systems also used for other operations may be used for the provision of identification services. However, the conformity assessment must be carried out from the perspective of the identification service. The assessment must focus on the identification scheme of the organisation's strong electronic identification service, i.e. on all operations that have impact on the fulfilment of the requirements set for strong electronic identification.

The assessment must extend to subcontractors (including cloud services) to the extent that they implement parts of the identification service. The depth of subcontractor assessment can be proportioned to the criticality of the function in question in the overall identification scheme. Providers of initial identification are also part of the identification scheme.

When using cloud services, the identification service provider must ensure that Traficom can exercise its supervisory rights. It should be noted that international cloud services can also allow the NCSC-FI at Traficom to access information.

Requirements set for **identification means** with relevance to **identification broker services** include authentication mechanisms as far as the broker service relays identification events between the party providing the means of identification and the eService. Requirements set for authentication mechanisms are relevant for subcontractors of identification broker services to the extent that the subcontractor's systems influence the security of identification events.

The assessment criteria presented in the table do not include separate ISO/IEC 27001:2013/2017 references to subcontractors. In ISO-compliant assessments of information security management, subcontracting is integrated in section A.15.1 of the standard (Information security in supplier relationships).

Examples of identification means assessment:

- How does a key code application / mobile telephone work as a secondary authentication factor, and what is the first authentication factor in this case? The assessment must establish how identification is performed using the application and if there is more than one way to do it (especially from the perspective of the authentication factors). Is another information-based factor or set of factors always required in addition to the one-time password provided by the application? Are there other authentication factors bound to the mobile device in addition to the key code application or the one-time password provided by the key code application?

- If a mobile identification application is used, it must be assessed in all respects that have impact on the compliance of the identification service. The assessment must establish how the binding between the application and the correct person is implemented in the mobile device and in the back-end system. If the application includes other features, these need not be included in the assessment insofar as they cannot influence the reliability of the identification.

- If authentication to an eService can be carried out using a mobile application only, it must be ensured that the authentication factors are sufficiently separated. In other words, the assessment must establish how the identification means ensures that an authentication factor based on information or property will not fall into the wrong hands if the mobile telephone is physically in the possession of another person or because of a data security violation. For example: what measures are taken to prevent the storing of a copy or a breakable hash of the PIN code that would put mobile phone-based identification at risk?

Examples of areas that need to be considered in the assessment of the identification scheme:

- the data centre
- application servers and server platforms (virtualisation platform)
- server platform access control
- office network (security of the control system of the identification service vs. the office network)
- data connection to server (control connection)
- information security on the virtual server (access control, updates)
- information security in the identification application (access control, updates)
- separation of administration and production systems
- information security of production/server environment (application traffic data security/customer interfaces)
- security of physical facilities, personnel, access, data communications and software related to the points above.

Cloud services

- An identification service may involve cloud services, the conformity of which can be verified either by conducting an internal assessment or by carefully examining the results of an assessment performed by another independent and competent assessment body. Therefore, it is important to specify all cloud service based services/products used in detail and examine related certificates and other documents.

2.3.3 Assessment report: A description that specifies the part of the identification means and/or the identification scheme covered by the assessment.

The assessment must focus on the part of the identification service provider's system in which the identification service is provided. The identification service provider may also order the assessment in several parts from two or more assessment bodies to have each of them assess a certain section of the identification scheme. It is essential that the assessment report is unambiguous in detailing whether the assessment report prepared by the assessment body covers the entire identification scheme or only a part of it. The assessment body must clearly identify the parts of the identification scheme covered by its assessment. Similarly, the assessment report shall make clear that all the parts of the systems of the identification service provider with which the identification service is provided have been audited.

2.3.4 Assessment report: Name(s) of the identification service to be assessed

The assessment report must specify the product or service names used by the users and the eServices to identify the services.

It is recommended to also include the names used internally in the identification service, if they are used in the assessment report or in the documentation of the identification service.

2.3.5 Assessment report: Description of identification means

The assessment report must include a description and/or documentation of the identification means and the authentication mechanism.

The descriptions must have sufficient technical detail that conclusions on all matters relevant for the assessment can be drawn based on them.

- ✓ What are the authentication factors used in the identification means (a minimum of two from different categories are required)?
- ✓ How is their independence of each other ensured?
- ✓ How are the authentication factors connected to the holder of the identification means?
- ✓ Authentication method (technical specification of how the identification events are implemented).

The descriptions must also cover all subcontractors.

2.3.6 Assessment report: Description of the identification scheme (system architecture)

The report must include a figure, a diagram or other clear presentation of the identification scheme's overall architecture. The reader must be able to verify, based on the description of the architecture and the report, that all relevant issues influencing the security of the system are taken into account in the assessment and the system architecture is secure. The descriptions must also cover all subcontractors.

- ✓ The system architecture description must indicate all system components related to identification operations.
- ✓ The reader must be able to understand the different sections of the identification scheme and their suppliers, connections/gateways between the sections, connection security policies, interfaces between the system sections and other related issues based on the report.
- ✓ The description of the architecture must indicate functional relations between all of the identification scheme components, such as the separation of data resources, the separation of the presentation layer and business logic, gateways/connections between environments and their protection, as well as security controls between the system and external parties.
- ✓ The description must indicate the network topology, L3-level components, such as firewalls, servers and connections to other environments, and management connections, if they have been separated.
- ✓ Data flows connected to the identification process should also be described.
- ✓ If the system uses productised components or products included in cloud services (Amazon Web Services, Google, Microsoft Azure, etc.), the product components must be named and the external components must be included in the scope of the subcontractor assessment.

2.4 Information on assessment body

PROVISIONS

ITSA, section 28: Conformity assessment bodies

The conformity pursuant to this chapter may be assessed by the following assessment bodies as laid down below:

1) a conformity assessment body;

2) other external assessment body operating in accordance with a commonly used procedure (other external assessment body); or

3) an independent assessment body operating within the service provider in accordance with a commonly used standard (internal assessment body).

The assessment report must be based on an assessment made by an assessment body referred to in Chapter 4 of the Identification and Trust Services Act. At the substantial level of assurance, the organisation assessing the identification service may be an external assessment body or an internal assessment body. At the high level of assurance, the assessment organisation must be an external assessment body.

The conformity assessment of an identification scheme may consist of an assessment performed by more than one assessment body. Of these, separate or combined assessment reports can be provided. Full details of all assessment bodies need to be provided.

The identification service assessment report must contain at least the following basic details.

2.4.1 Assessment report: Identifying information and contact information of assessment body

- ✓ Name of the company or the organisation and a unique registration number or identifier;
- ✓ If the company or organisation is located in an EEA state other than Finland: the register in which the foreign company or organisation has been entered;
- ✓ Postal address and contact persons; and
- ✓ E-mail addresses for enquiries by Traficom.

2.4.2 Assessment report or notification: Competence and independence of the assessment body

The report can be provided as part of the assessment report or separately in connection with the notification.

The report must specify proof of the independence and the competence of the assessment body (the standard that is followed or another proof of competence as specified in M72B, sections 18 and 19).

ITSA, section 42: General guidance and regulations by the Finnish Transport and Communications Agency

[…]

The Finnish Transport and Communications Agency may issue more detailed regulations on:

[…]

6) the qualification requirements for the conformity assessment body laid down in section 33, taking into account the provisions of the EU Regulation on Electronic Identification and Trust Services;

[…]

Regulation M72B, section 18: Requirements concerning an external assessment body of the identification service

18.1 Proving procedures

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

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

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

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

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

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

18.2 Competence

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

Regulation M72B, section 19: Requirements concerning an internal assessment body of the identification service

19.1 Independence

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

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

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

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

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

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

6) compliance with other comparable government regulations or standards concerning overall independent internal audit management.

19.2 Competence

Proof of the competence to assess identification schemes also requires demonstrating how, and to what extent, an internal audit arranged according to the rules, guidelines or standards referred to in section 19.1 concern the requirements set for the identification scheme.

2.5 Assessment implementation

2.5.1 Assessment report: Assessment time and duration of assessment in person work time

The dates of the assessment times must be reported, and the assessment duration must be reported in person-days or hours. The aim is to establish that the assessment is up to date and sufficiently thorough.

There is no minimum duration set for the assessment. Many factors affect the assessment and can lengthen or shorten the time needed for the assessment. If the service assessment can make use of several previously or currently valid assessments or certificates, the time used for the assessment is shortened. The assessment must cover the entire identification scheme and all areas listed in this document, and it must also feature technical sampling or assessment.

2.5.2 Assessment report: Assessment methods

The assessment report must describe the methods employed in the assessment of each area. There are no exact requirements on the number of sources that must be used in the assessment.

The assessment body and the identification service provider should use their own discretion in determining the sources used in the assessment and the areas to be verified on the basis of several sources.

However, the assessment of all areas solely on the basis of written documentation will not be considered adequate. **Traficom may consider the assessment methods inadequate if no technical observation external to the system or otherwise is made in the audit.**

Also, standard lists and references alone cannot be considered sufficient.

If the assessment is based on an assessment made by another assessment body, the assessment must be studied closely and the assessment report must establish which concrete matters the conformity assessment is based on, i.e. how the assessment body has studied the materials of the other assessments and assessed their quality, scope, corrections made on their basis and correction schedules.

2.5.3 Details of the documentation used in the conformity assessment

The assessment report must list the documentation items (of the service provider) that have been assessed.

It is not necessary to attach all materials related to the assessment to the assessment report submitted to Traficom. Traficom may request more detailed documents to be submitted where necessary. Traficom's right to obtain information is based on section 43 of the Identification and Trust Services Act, according to which Traficom has, secrecy provisions notwithstanding, the right to obtain the information necessary for performing its duties from anyone whose rights and obligations are laid down in said Act or anyone acting on their behalf.

The documentation to be drawn up during the assessment must be retained for at least the validity period of the assessment report. In addition, it shall be taken into consideration that the methods applied may also involve requirements on how and for how long the documentation shall be retained.

2.5.4 Identification means risk assessment

According to section 6.1.1 of Regulation M72B, the resistance must be based on a risk assessment including specific assessments of threats directed at an authentication mechanism and authentication factors based on possession, knowledge and inherence as well as assessment of security measures in place to protect against these threats.

Risk assessment can also include calculation of the likelihood of attack e.g. in accordance with Common Criteria CCDB 2009 03, part 3, or ETSI 102 165-1, clauses 6.6 and 6.7.

2.6 Commensurability between assessment, assurance levels and risks

Two assurance levels are defined for the reliability of strong electronic identification: substantial and high.[7] Assessment criteria tables use the abbreviations S=substantial (corresponds to eIDAS2 substantial) and H=high (corresponds to eIDAS3 high).

In regulation, different requirements are specified for different assurance levels, but this does not apply to all requirements.

A general requirement that distinguishes the different assurance levels is how effectively the identification means and the identification scheme protect the identification against different data security risks and threats. Risks and threats need to be taken into account for the entire lifecycle of the identification service and the identification means. The high level of assurance calls for the ability to protect against relatively advanced attack potentials. Even the substantial assurance level calls for very good resistance against attacks.

In the criteria, the assurance levels are primarily addressed together. If no separate high-level requirement or criterion is defined, the general high assurance level assessment guideline is to assess the identification service's operations and the ability to withstand attacks against a high attack potential.

The criteria may be updated in the future to provide more detail on the high assurance level when the experience of application in Finland becomes available and when standardised interpretation practices concerning the eIDAS regulation are established in Europe.

Identification and planned management of risks and threats, preparing for them and protecting against them using technical and organisational measures form the foundation of security.

CF.

LoA 2.3: Authentication

[7] The EU's Level of Assurance Regulation also specifies requirements for a low assurance level, but this level is not defined in the Finnish Identification Act. The reciprocity requirements of the eIDAS regulation do not apply to identification methods for the low assurance level. Taking them into account is voluntary.

This section focuses on the threats associated with the use of the authentication mechanism and lists the requirements for each assurance level. In this section controls are understood to be commensurate to the risks at the given level.

LoA Guidance, section 2.3

The authentication mechanisms used in the authentication phase cannot completely prevent all attacks; they can only offer resistance to attacks on a certain level of security/assurance. A standard way to quantify the resistance of different mechanisms is to rank them according to their resistance against attacks with a certain attack potential (i.e. strength of an attacker).

The Level of Assurance uses the terms "enhanced-basic", "moderate" and "high" to denote the different attack potentials. 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 regulation, some assessments of resistance against potential attacks should be carried out.

The assessment should take relevant threats into account. 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.

[…]

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.

[…]

LoA 2.4: Management and organisation

All participants providing a service related to electronic identification ... ("providers") shall have in place documented information security management practices, policies, approaches to risk management, and other recognised controls so as to provide assurance to the appropriate governance bodies for the electronic identification schemes in the respective Member States that effective practices are in place. Throughout section 2.4, all requirements/elements shall be understood as commensurate to the risks at the given level.

LoA Guidance, section 2.4

[…]

A general principle in risk management is that it is up to the organisation to choose which level of risk it finds acceptable. This general principle is modified by the requirement in 2.4,

since the organisation should have controls that are commensurate to the risks at the given level.

[…]

2.7 Accuracy of the assessment report

The assessment report must indicate how compliance with the requirements has been assessed.

The assessment report must include a verbal description of practical matters and observations that form the basis for the assessment of conformity of each requirement.

The assessment report must also contain a list of the service provider's documentation assessed on each of the points and the methods employed.

Precise information may be required especially concerning

- ✓ storing and processing of data
- ✓ technical measures
- ✓ authentication mechanisms
- ✓ the information security management system, and
- ✓ the assessment of the physical security of premises.

The high level of assurance requires more precise information compared to the substantial level of assurance.

The report must also cover the operations of subcontractors.

2.8 Reporting of irregularities in the assessment report

Irregularities and deviations are typically found during a conformity assessment and are corrected during the assessment or shortly thereafter.

As the identification and correction of irregularities is a key component in the maintenance and management of information security, it is recommended that the assessment report also includes information on the detection and correction of irregularities. These can be reported separately in connection with each requirement, or as a summary.

A reporting table in Excel format is attached to this document. It should be used as a tool in assessment and in reporting the findings to the Finnish Transport and Communications Agency. The table features the necessary sections for reporting observations and corrective measures.

Each irregularity that is observed must be provided with the assessment body's proposal for measures and the identification service provider's correction plan on corrective measures or compensating action. The measures taken to correct already fixed irregularities must also be reported.

Traficom will not prepare a scale indicating the severity of irregularities, but will leave their evaluation to the discretion of the identification service provider and the assessment body. Traficom makes the final assessment on whether the irregularities are acceptable due to their limited impact or the existence of an

adequate correction plan or compensating action. Traficom may also require that the irregularities that are observed are corrected.

2.9 Correcting irregularities and reporting corrections

Critical irregularities must be corrected immediately, and corrective measures must be carried out within six months of detecting an irregularity. The correction schedule and corrective measures must also be reported for other observed irregularities.

Corrective measures must be assessed in connection with the next assessment, or in case of critical irregularities, at the latest within six months of detecting the irregularity. The new assessment is delivered to the Finnish Transport and Communications Agency once it is complete.

3 Areas of assessment

This section lists the requirements for the various fields that are assessed and provides guidelines for the assessment work and the reporting of its results where applicable.

The general identification service assessment criteria follow this division. The general assessment criteria can be found in Annex B.

3.1 Characteristics of the identification means; authentication mechanism

The requirements are set out in the following provisions:

- ITSA, section 8 a: Authentication factors used in the identification means
- LoA Annex, section 2.2.1: Electronic identification means characteristics and design
- ITSA, section 8: Requirements posed on the electronic identification scheme. (subsection 1, paragraph 3)
- LoA Annex, section 2.3.1: Authentication mechanism
- LoA Annex, section 2.4.6: Technical controls (point 2)
- M72B, section 6: Information security requirements of the identification means
- M72B, section 7: Identification scheme interface encryption requirements
- M72B, section 8: Authenticating parties to the communications
- M72B, section 9: Integrity and confidentiality of authentication messages

- LoA Annex, section 1: Applicable definitions
- 2) 'authentication factor' means a factor confirmed as being bound to a person, which falls into any of the following categories […]
- (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.

The assessment report must specify how the characteristics of the identification means and the authentication mechanism as well as the identification means' capacity for protecting against data security threats and violations on the level required by the level of assurance have been assessed.

The provider of the identification means is responsible for the conformity of the characteristics of the identification means.

The identification broker service shares the responsibility for the conformity of the authentication mechanism, as the broker system is involved in the relaying of identification events.

In addition to the assessment report, a scanning report of the assessment (specified in M72B, section 7) that describes the TLS profiles and the encryption profiles of the identification scheme's external interface must be submitted.

3.2 Interoperability

The requirements are set out in the following provisions:

- ITSA, section 12 a: Trust network of identification service providers
- Government Decree 169/2016 on the trust network of strong electronic identification services providers, section 1 (technical interfaces of the trust network)
- M72B, section 12: Minimum set of data to be relayed in a trust network
- M72B, section 14: Data transfer protocol and other requirements

The assessment report must specify how the interfaces and the attributes (identifying information) that are offered in the trust network using the identification means are assessed. The assessment report must also specify how the capacity to offer optional attributes has been assessed.

The assessment of attributes only applies to the provider of the identification means.

3.3 Technical information security requirements

These requirements are assessed from the perspective of data communications, information system security and operator security.

The requirements are set out in the following provisions:

- ITSA, section 8: Requirements posed on the electronic identification scheme (subsection 1, paragraph 4)
- LoA Annex, section 2.3.1: Authentication mechanism
- LoA Annex, section 2.4.6: Technical controls, points 1, 2 and 3
- M72B, section 5: Information security requirements of an identification scheme

The assessment report must describe how the security of the design, the implementation and the maintenance of the identification scheme has been assessed in terms of data communications, information systems and operator security. The report must also specify how the technical measures that protect the system from the impacts of moderate or high-level data security threats or violations have been assessed.

The assessment report must specify the grounds of the assessment of the conformity of the components of the identification scheme supplied by subcontractors.

The assessment and the assessment report should pay attention to the following matters (as applicable):

- data connections
- control connections
- zoning of data connections
- data communication equipment and systems
- separation of production, maintenance and administration networks and the development environment
- filtering
- connections to the public network
- classification of information systems
- access rights and user identification
- high-risk job combinations
- hardening

- encryption solutions
- security of cryptographic materials
- specific requirements of remote workstations
- malware
- change management
- software vulnerabilities
- backup copies.

3.4 Security incident observation capacity; management of security incidents; disturbance notifications

The requirements are set out in the following provisions:

- ITSA, section 8: Requirements posed on the electronic identification scheme (subsection 1, paragraph 4)
- LoA Annex, section 2.4.6: Technical controls, points 1 and 4
- ITSA, section 16: Notifications of the identification service provider concerning threats or disruptions to their operations and protection of data
- M72B, section 5: Information security requirements of an identification scheme
- M72B, section 11: Incident notifications by the identification service provider to the Finnish Transport and Communications Agency

The assessment report must specify the grounds upon which the following matters are considered to fulfil the requirements:

- ✓ incident observation capacity
- ✓ collecting of event logs and administration logs
- ✓ monitoring for irregularities
- ✓ incident severity rating and organised response to incidents
- ✓ organised nature of corrective actions
- ✓ capacity to fulfil the incident notification duties to various parties

3.5 Storage and handling of data

The requirements are set out in the following provisions:

- ITSA, section 13: General obligations of an identification service provider
- LoA Annex, section 2.4.4: Record keeping, points 1 and 2
- ITSA, section 8: Requirements posed for the electronic identification scheme (subsection 1, paragraph 4)
- LoA Annex, section 2.4.6: Technical controls, point 1 (note especially the requirement concerning sensitive cryptographic materials on the substantial and high assurance levels) and point 5
- M72B, section 5: Information security requirements of an identification scheme
- M72B, section 7: Identification scheme interface encryption requirements
- ITSA, section 24: Storage and use of data regarding the identification event and means

The assessment report must specify the grounds upon which the following matters are considered to fulfil the requirements:

- ✓ classification of information related to identification and the identification scheme
- ✓ information access control
- ✓ risks caused by the centralised storage of information
- ✓ information security of data processing and storage (including encryption)
- ✓ information traceability and recoverability
- ✓ information lifecycle management including retention times and disposal.

3.6 Security of physical premises

The requirements are set out in the following provisions:

- ITSA, section 8: Requirements posed on the electronic identification scheme (subsection 1, paragraph 4)
- LoA Annex, section 2.4.5: Facilities and staff, points 3 and 4

The assessment report must specify the observations based upon which the security of physical premises affecting the security of the identification scheme has been assessed to meet the requirements.

The assessment and the assessment report should pay attention to the following matters (as applicable):

- ✓ protection from environmental hazards (fire, heat, gas, dust, vibration, water)
- ✓ prevention of unauthorised access (breaking and entering)
- ✓ power cuts
- ✓ protection from vandalism
- ✓ zoning
- ✓ structural protection
- ✓ access control
- ✓ quality of the security systems
- ✓ unauthorised devices and connections.

3.7 Sufficiency and competence of human resources

The requirements are set out in the following provisions:

- ITSA, section 13: General obligations of an identification service provider
- LoA Annex, section 2.4.5: Facilities and staff, points 1 and 2

The assessment report must specify the observations upon which it has been assessed that:

- ✓ the capacity of human resources is sufficient considering the nature of the electronic identification service (24/7/365)
- ✓ the expertise in the required competence areas, such as technical and legal competence (due to the processing of personal information), is sufficient
- ✓ the sufficiency and competence of subcontracted services (office systems, operating services, software, infrastructure...) is on an appropriate level.

3.8 Information security management

The requirements are set out in the following provisions:

- ITSA, section 8: Requirements posed on the electronic identification scheme (subsection 1, paragraph 5)
- LoA Annex, section 2.4: Management and organisation (Introduction)
- LoA Annex, section 2.4.3: Information security management
- LoA Annex, section 2.4.7: Compliance and audit
- M72B, section 4: Information security management system of the identification service provider

- LoA Annex, section 1: Applicable definitions
  4. 'information security management system' means a set of processes and procedures designed to manage to acceptable levels risks related to information security.

The assessment report must specify the grounds upon which the following matters are considered to fulfil the requirements:

- ✓ That the information security management of the identification service provider is comprehensive, consistent, organised and constantly monitored.

- ✓ That the requirements of the identification service (ITSA, the eIDAS LoA Regulation and Traficom Regulation M72B) are taken into account in the administration system.
- ✓ That the information security management of the subcontractors meets the requirements.

3.9 Identity proofing and verification of the applicant of identification means (initial identification)

The requirements are set out in the following provisions:

- ITSA, section 8: Requirements posed on the electronic identification scheme (subsection 1, paragraphs 1 and 2)
- ITSA, section 17: Identifying a natural person applying for an identification means
- LoA Annex, section 2.1.2: Identity proofing and verification (natural person)
- ITSA, section 7 b: Information on the validity of a passport or a personal identity card
- M72B, section 6: Information security requirements of the identification means

Requirements for the identification and verification of the identity of a legal person:

- ITSA, section 7 a: Using the data in the Business Information System
- ITSA, section 17 a: Identifying a legal person applying for an identification means
- LoA Annex, section 2.1.3: Identity proofing and verification (legal person)
- LoA Annex, section 2.1.4: Binding between the electronic identification means of natural and legal persons

- LoA Annex, section 1: Applicable definitions
  1. 'authoritative source' means any source irrespective of its form that can be relied upon to provide accurate data, information and/or evidence that can be used to prove identity.

The assessment report must specify how and on what grounds the initial identification procedures have been assessed as meeting the requirements.

Initial identification procedures available:

1) initial identification is based on the presentation of an identity document approved in Finland
2) initial identification using an electronic identification means
3) initial identification based on identification made for other purpose
4) initial identification by the police
5) remote [initial] identification, e.g. via a video link or a series of photos and the remote reading of an identity document.

3.10 About initial identification based on an identity document using a remote connection

NOTE! At the time of preparation of this document, no established interpretative practice by which the presentation of an identity document using a remote connection could fulfil the requirements of substantial or high assurance level was available.

Because of this, the document lists perspectives which need to be taken into account in the risk and threat assessment and in the planning of any implementations. Strong electronic identification means can be used for a variety of electronic transactions in numerous services. Because of this, ensuring that identification means are only issued to the right people requires stringent controls already at a substantial assurance level. At the high assurance level, the capacity to protect against high-level attacks must also be taken into account.

The list of observations in this Guideline is not exhaustive. Instead, it should only be taken as an example of matters that have been considered when the guideline was drafted.

In the initial identification based on an identity document (passport or identity card), matters such as the following need to be taken into account:

- Ensuring the authenticity of the identity documents
- Comparison of the (properties of the) individual presenting the identity document to the information of the identity document
    - Comparison of the portrait on the identity document and the individual's face. Comparison of signatures may also be used; the identity document may contain a digitised signature (the individual is requested to provide a signature).
- **Use of information from the Population Information System**
- **Checking the authenticity and the validity of identity documents from the databases that are available**
- If the identity document can be presented using a remote connection, a thorough assessment of risks and protection methods against the threat of forged identity documents or presentation of genuine identity documents by a wrong person is required. Factors that need to be taken into account include:
    - observations on the authenticity factors of the identity document and
    - verification of and observations of the authenticity of the photograph or video recording provided by the person.

Considerations for remote initial identification

- If the identity document can be presented using a remote connection, a thorough assessment of risks and protection methods against the threat of forged identity documents or presentation of genuine identity documents by a wrong person is required.

- Factors that need to be taken into account include observations of the authenticity factors of the identity document and verification of and observations on the authenticity of the photograph or video recording provided by the person.

- Only an identity document with a chip can be used for remote initial identification when issuing a strong electronic identification means.

    - The authenticity factors of identity documents are designed to be verified on the spot using instruments such as ultraviolet light. It may very well be impossible to verify the authenticity of an identity document based on a photograph of the document alone, because the security factors in the image are not transmitted properly. An image is mostly useful for verification of correct identity document layout.

    - Using a chip in the identity document changes the situation substantially. Passive authentication (verification of a signature) can be used to verify that the information is from an authentic document and has not been altered. All passports with a chip have this signature capacity.

- However, the data can be copied from the chip at any point. No specific attack potential is required for copying the chip, because the chip data is (with the exception of fingerprint data) freely readable.

- Passports and identity cards also have the possibility for active authentication or chip authentication, which can be used to ensure that the chip is authentic and that the data has not been copied – in other words that the genuine identity document is at the other end of the remote connection at that exact moment.

- Once the chip authenticity and uniqueness have been confirmed, the portrait that is read from the chip can be trusted. The portrait is high-definition and has much greater resolution than the image printed on the passport. This enables the portrait information to be trusted, and because of the greater resolution it is much more suited for facial comparison against a photograph and/or video provided in a remote identification event.

- The portrait on the document may not be stored on the chip of the electronic identity document and therefore cannot be read from the chip for authentication purposes. In biometric passports the image is stored on the chip.

- According to Section 7 of the Identification Act the provider of an identification means must use the Population Information System to obtain and update the data they need in order to be able to offer a service for identifying a natural person. The identification service provider shall also ensure that the data it needs for the purpose of offering identification services are up-to-date with the data in the Population Information System.

- According to Section 7 b of the Identification Act an identification service provider has the right to obtain via electronic means information from the information system of the Police about the validity of a passport or a personal identity card used for initial identification.

- If there is an opportunity to also use similar registers or services in other countries, containing information on the validity of identity documents and passports, and containing information that the claimed identity exists and that the person claiming the identity is one and the same, those registers can be utilised.

    - Cf. LoA, section 2.1.2 low, point 3: It is known by an authoritative source that the claimed identity exists and it may be assumed that the person claiming the identity is one and the same.

    - And substantial, point 2: An identity document is presented during a registration process in the Member State where the document was issued and the document appears to relate to the person presenting it and steps have been taken to minimise the risk that the person's identity is not the claimed identity, taking into account for instance the risk of lost, stolen, suspended, revoked or expired documents.

- In a situation where the information in the identity document does not match the information in the Population Information System (for example, the name or personal identity code has changed, or the document to be presented is issued by another EU country), the applicant's identity and the validity of the document must be confirmed by other means.

- The authenticity of the information about the individual presenting the identity document via the remote connection must be verified, and the

actual source of the information (the individual presenting the identity document) must be ensured. Factors that need to be taken into account include the reliability of the data communication and information system, the risk of a forged transmission and alteration of the visual appearance of the person in ways that are difficult to detect using the remote connection. As a general rule, the video link must be used via a mobile application, as a video link through a computer browser can be easily hacked.

- The lighting conditions and video quality requirements must be defined. The lighting must be appropriate, and any artefacts must be visible, as these can indicate video manipulation. The resolution must be appropriate throughout the remote initial identification event. If there are disturbances in the video link, the identification event must be interrupted and started again as necessary.

- Assessment of the lifelike appearance of the person who presents the identity document in the remote identification event can help confirm that the presenter of the identity document is present and that no forged recording is used. For example, the person could be requested to perform certain random gestures in real time. Different ways can be used to observe vitality, such as random inputs in video analysis or biosignals detected in the image. Staff must be provided with adequate training and comprehensive instructions on the assessment of the lifelike appearance of individuals. Machine assessment of lifelike appearance must be based on random events or requests targeted at the customer carrying out remote initial identification.

- Reliable comparison between information read from the identity document and the physical properties of the person at the other end of the remote connection transmitted via video or still image is a requirement (FAR value).

- However, how this can be performed in a manner that is reliable is not defined. In case of a remote connection this could, in principle, mean a comparison by a human agent or automatic electronic comparison by a back-end system that has access to both photographs. The reference point for comparison when assessing the reliability is that of an employee of the identification service comparing the information of the individual and the identity document on the spot whilst also able to observe the behaviour of the individual who presents the document.

- It must be noted that observation carried out by a computer is generally much more reliable than that carried out by a human. Therefore, a remote identification carried out only by a human agent is not sufficient.

Cf. also LoA Guidance:

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

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

Considerations for legislation on the reading of chips

- According to section 5a of the Passport Act 671/2006, passports feature a technical part referred to in the Council Regulation (EC) No 2252/2004 (EU

Passport Regulation) on standards for security features and biometrics in passports and travel documents issued by Member States.

The passport holder's portrait and fingerprints referred to in section 6a, along with the necessary additional information in accordance with the provisions of the EU Passport Regulation, are stored in the technical part. Information referred to in subsection 1 of section 5 can also be stored in the technical part. The EU Passport Regulation lays down provisions on the passport holder's right to verify their personal data contained in the technical part of their passport.

The EU Passport Regulation lays down provisions on the security features and biometric identifiers on passports. A passport that contains a biometric identifier has an indication of this on the cover.

- According to section 5b of the Passport Act, the fingerprints stored in the technical part of the passport can only be read in accordance with the EU Passport Regulation. Fingerprints can only be read by the passport authority referred to in section 10 and the police or border control authority. […]

  When reading fingerprints, the passport holder's data may only be processed as defined in the EU Passport Regulation and the Passport Act.

  In addition to the provisions of the Passport Act on the reading of fingerprints, the European Community's legislation and international agreements binding upon Finland are complied with.

- The Passport Act has similarly restricted the reading of fingerprints to the named authorities, but the reading of the portrait is not restricted.

- In accordance with section 5a of the Identity Card Act (663/2016), the fingerprints and portrait stored in the technical part of the identity card can only be read as provided in the EU ID Regulation. Fingerprints can be read by the identity card authority as referred to in section 18, the Police and the Finnish Border Guard. Fingerprints can also be read by the Finnish Customs when it is acting as a pre-trial investigation authority or performing tasks of the border control authority. […]

- In other words, the reading of fingerprints is restricted only for certain authorities, but the reading of the portrait is not restricted by legislation.

- According to Article 11(6) of the EU ID Regulation (EU) 2019/1157, biometric data stored in the storage medium of identity cards shall only be used in accordance with Union and national law, by the duly authorised staff of competent national authorities and Union agencies.

  According to recital 22 of the Regulation, biometric identifiers should be collected and stored in the storage medium of identity cards and residence documents for the purposes of verifying the authenticity of the document and the identity of the holder. Such a verification should only be carried out by duly authorised staff and only when the document is required to be produced by law. According to recital 19, as a general practice, Member States should, for the verification of the authenticity of the document and the identity of the holder, primarily verify the facial image and, where necessary to confirm without doubt the authenticity of the document and the identity of the holder, Member States should also verify the fingerprints. According to recital 17, security features are necessary to verify if a

document is authentic and to establish the identity of a person. The establishment of minimum security standards and the integration of biometric data in identity cards […] are important steps in rendering their use in the Union more secure. **The inclusion of such biometric identifiers should allow Union citizens to fully benefit from their rights of free movement.** Furthermore, according to recital 15, "This **Regulation does not affect the use of identity cards** and residence documents with eID function **by Member States for other purposes, nor does it affect the rules laid down in Regulation (EU) No 910/2014** of the European Parliament and of the Council, which provides for Union-wide mutual recognition of electronic identifications **in access to public services** and which helps citizens who are moving to another Member State, by requiring mutual recognition of electronic identification means subject to certain conditions. **Improved identity cards should ensure easier identification and contribute to better access to services."**

- Section 2.1.2 of the Annex of the Commission Implementing Regulation (EU) 2015/1502 (LoA or the Assurance Level Regulation) based on the eIDAS Regulation requires on the high assurance level that **where the person** has been verified to be in possession of photo or **biometric identification evidence** recognised by the Member State in which the application for the electronic identity means is being made and that evidence represents the claimed identity, **the evidence is checked** to determine that it is valid according to an authoritative source.

- Most of the data on identity cards is freely readable, but some are restricted without the correct certificate. The reading of fingerprints, in particular, is restricted by law to named authorities. Reading the portrait is generally not restricted, and there are many free applications on the market for reading portraits. (NOTE! These are not primarily usable as such as data-secure methods.)

- According to Article 9(1) of the General Data Protection Regulation, […] processing of biometric data for the purpose of uniquely identifying a natural person […] shall be prohibited. According to Article 9(2)(g), paragraph 1 shall not apply if processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

- Generally, in situations where the portrait would be read, the customer can refuse and instead opt for authentication in person. The customer can also approve the reading of the portrait as they wish and take care of identification via a remote connection.

- The European Banking Authority (EBA) has published instructions on the remote identification of customers (https://www.eba.europa.eu/eba-publishes-guidelines-remote-customer-onboarding).

    - Paragraph 35:
      "In situations where the device the customers use to prove their identity allows the collection of relevant data, for example because the data is contained in the chip of a national identity card, and it is technically feasible for the credit and financial institutions to access this data, credit and financial institutions should consider using this information to verify its consistency with the information obtained

through other sources, such as the submitted data or other documents submitted by the customer."

- Paragraph 39:
"Where the remote customer onboarding solution involves the use of biometric data to verify the customer's identity, credit and financial institutions should make sure that the biometric data is sufficiently unique to be unequivocally linked to a single natural person. [...]"

- According to EBA's interpretation, e.g. the portrait of a customer can and should be read in a remote identification situation.

- In its interpretation, Traficom relies on the EBA instructions and furthermore on the fact that e.g. the EU ID Regulation does not restrict the application of eIDAS, and that the Assurance Level Regulation based on eIDAS enables the reading of biometric data. Based on the above, Traficom states that reading the portrait from an identity card or passport does not appear to be prohibited by law and is even a prerequisite on assurance level high based on the Assurance Level Regulation. This makes it a good method for enabling the remote identification of a customer.

3.11 Lifecycle of identification means

The requirements are set out in the following provisions:

- Application and registration: ITSA, sections 7 and 20; M72B, section 6.3
- Issuance, delivery and activation: ITSA, sections 20 and 21; LoA, section 2.2.2
- Suspension, revocation and reactivation: ITSA, sections 25 and 26; LoA, section 2.2.3
- Renewal and replacement: ITSA, section 22; LoA, section 2.2.4

The assessment report must specify the method and the grounds of assessment used to ensure that:

- ✓ The personal data linked to the identification means is correct.

- ✓ The delivery, suspension, revocation, reactivation, renewal and replacement of the identification means are, as a whole, implemented so that the possession of the identification document by the correct holder is ensured.

In December 2018, Traficom published an advisory memorandum[8] on the verification of identity in maintenance situations.

3.12 Testing

The identification scheme and its components must be tested comprehensively and regularly. Each change must be tested before it is transferred to production. Negative test cases in particular also need to be tested to prevent the generation of erroneous events.

[8] See interpretative comment *Reg. No: Traficom/106/09.02.00/2019 (25.3.2019) Interpretation memorandum of the Finnish Transport and Communications Agency (Traficom) on using a driving licence to verify one's identity when an identification means has been locked or when an identification means or authentication factor is being renewed.* The memorandum is available online at https://www.kyberturvallisuuskeskus.fi/en/electronic-identification

ANNEX A: Assessment report checklist (guideline)

This annex contains a checklist of the contents listed in the assessment report guideline. The section addressing the matter in the guideline document is given in parentheses.

1. Identifying information and contact information of assessment body (2.4.1)

    1) Name of the company or the organisation and a unique registration number or identifier.

    2) If the company or organisation is located in an EEA state other than Finland: the register in which the foreign company or organisation has been entered.

    3) Postal address and contact persons.

    4) E-mail addresses for enquiries by Traficom.

2. Competence and independence of the assessment body (2.4.2)

    - The report can be provided as part of the assessment report or separately in connection with the notification.

3. Assessment time and duration of assessment in person work time (2.5.1)

4. Assessment methods (2.5.2)

5. Details of the documentation used in the conformity assessment (2.5.3)

6. A description that specifies the part of the identification means and/or the identification scheme covered by the assessment (2.3.3)

7. Name(s) of the identification service to be assessed (2.3.4)

8. Description of identification means (2.3.5)

9. Description of the identification scheme (system architecture) (2.3.6)

10. Irregularities (2.8–2.9)

11. Results of assessment specific to individual areas (3.1–3.12 as applicable)

Assessment guideline for electronic identification services

Traficom Guideline

211/2013 O Annex B General assessment criteria for identification services

ANNEX B: General assessment criteria for identification services

B 1 Characteristics of the identification means; authentication mechanism

KEY PROVISIONS

M72B, section 15.1: Identification scheme and identification means features to be assessed
The identification service assessment required in section 29 of the Identification and Trust Services Act must cover all of the requirements specified in the Act and in this regulation, which pertain to:
[…]
2) the identification means, meaning certain properties of the identification means, namely:
[…]
c) identification means characteristics and design;
[…]
g) authentication mechanisms.

M72B, section 6: Information security requirements of the identification means
6.1 Identification means characteristics and its resistance
6.1.1
The authentication factors, authentication mechanism and security measures of the identification means must be planned, executed and maintained so that they protect the integrity and confidentiality of the identification means. The identification means must be able to resist at least moderate or high-level threats and attack potential specified in section 2.3 of the appendix to the regulation on Level of Assurance in Electronic Identification in accordance with the assurance level of the identification ser-vice.
The resistance must be based on a risk assessment including specific assessments of threats directed at an authentication mechanism and authentication factors based on possession, knowledge and inherence as well as assessment of security measures in place to protect against these threats.

6.1.2
The features and security measures of the identification means must prevent the possibility that the compromise of one authentication factor would compromise the reliability of other authentication factors. The security measures protecting the identification means must separate and protect the authentication factors especially if they are used on the same terminal device.

6.1.3
The identification means and authentication must employ internationally or nationally recommended encryption methods. The communications connection between the identification means and the identification scheme must employ encryption methods specified in section 7 of the regulation, where technically applicable, unless resistance of the system assessed as a whole is otherwise realised by other security means.

6.2 Specific security measures
6.2.1

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

6.2.2
The identification service must present the identification means user with information concerning the relying party, for whom the identification is carried out, during the identification event. This information must be presented in identification means that have the technical ability to do so.

6.2.3
In this regulation, single sign-on refers to the identification service offering authentication to more than one relying party based on a single authentication of the holder using strong electronic identification means.
In planning, executing and maintaining single sign-on, the identification service must take care of the security measures based on the management of the length, trans-fer and ending of the session related to single sign-on. [...]

6.3 Connecting identification means to a person
6.3.1
The authentication factors of the identification means must be bound to the identification means holder in the identification scheme.

6.3.2
An identification means shall not be bound to an applicant before the applicant has passed initial identification or it has been otherwise ensured in the process of granting an identification means that the identification means is not functional before the initial identification referred to in section 17 of the Identification and Trust Services Act has been performed.

6.4 Processing identification means holder-specific data
6.4.1
The identification service provider shall ensure that secret data related to an identification means is not revealed to its staff under any circumstances.

6.4.2
The identification service provider shall not make copies of any secret data related to an identification means.

NO.	LEVEL OF ASSURANCE	REQUIREMENT PERTAINING TO THE IDENTIFICATION SERVICE (SUMMARY)	PROVISIONS	STANDARD REFERENCE	NOTES
1.	S,H	A risk assessment is available for the identification means (calculation of attack potential).	**ITSA, section 8: Requirements posed on the electronic identification scheme** Section 8.1, paragraph 3: The identification means can be used to verify that only the holder of the identification means can use the means in a	ISO 29115 ISO/IEC 15408-1	E.g. Common Criteria CCDB 2009 03, part 3, or ETSI TS 102 165-1, clauses 6.6 and 6.7 calculation of the likelihood of the attack.

			way that, at a minimum, meets the conditions for assurance level substantial laid down in sections 2.2.1 and 2.3 of the Annex to the Act on Level of Assurance in Electronic Identification. **LoA Annex, section 2.3.1: Authentication mechanism** 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. **M72B, section 6.1.1** The authentication factors, authentication mechanism and security measures of the identification means must be planned, executed and maintained so that they protect the integrity and confidentiality of the identification means. The identification means must be able to resist at least moderate or high-level threats and attack potential specified in section 2.3 of the appendix to the regulation on *Level of Assurance in Electronic Identification* in accordance with the assurance level of the identification service. The resistance must be based on a **risk assessment** including specific assessments of threats directed at an authentication mechanism and authentication factors based on possession, knowledge and inherence as well as assessment of security measures in place to protect against these threats.	ISO/IEC 18045, Annex B Common Criteria CCDB 2009 03, part 3 ETSI TS 102 165-1, clauses 6.6 and 6.7	The appropriate implementation of risk assessment is the basic premise for the calculation of attack potential.
2.	S, H	The identification means uses at least two authentication factors from different authentication factor categories.	**ITSA, section 8 a: Authentication factors used in the identification means.** […]		

			1) a knowledge-based authentication factor that the subject is required to demonstrate knowledge of; 2) a possession-based authentication factor that the subject is required to demonstrate possession of; 3) an inherent authentication factor that is based on a physical attribute of a natural person. […] **LoA Annex, section 2.2.1: Electronic identification means characteristics and design** The electronic identification means uses at least two authentication factors from different categories.		
3.	S,H	The authentication factors are independent of each other.	**LoA Annex, section 2.2.1: Electronic identification means characteristics and design** The electronic identification means is designed so that it can be assumed to be used only if under the control or possession of the person to whom it belongs. **M72B, section 6.1.2** The features and security measures of the identification means must prevent the possibility that the compromise of one authentication factor would compromise the reliability of other authentication factors. The security measures protecting the identification means must separate and protect the authentication factors especially if they are used on the same terminal device.		Mutual independence of authentication factors requires special attention especially in identification means used on mobile devices.
4.	S,H	Different threat types that target different authentication factors are taken into account in the planning of the identification means.	**LoA Annex, section 2.2.1: Electronic identification means characteristics and design** The electronic identification means is designed so that it can be assumed to be used only if under the control or possession of the person to whom it belongs.		

			M72B, section 6.1.2 The features and security measures of the identification means must prevent the possibility that the compromise of one authentication factor would compromise the reliability of other authentication factors. The security measures protecting the identification means must separate and protect the authentication factors especially if they are used on the same terminal device.		
5.	S,H	Secret information related to the identification means is not accessible to the personnel or the subcontractors of the identification service provider.	**M72B, section 6.4: Processing identification means holder-specific data** 6.4.1 The identification service provider shall ensure that secret data related to an identification means is not revealed to its staff under any circumstances. 6.4.2 The identification service provider shall not make copies of any secret data related to an identification means.		Secret information typically includes PIN codes and other information-based authentication factors. This requirement is intended to address the risk of dishonest personnel.
6.	S,H	Authentication factors are confirmed as being bound to a person.	**LoA Annex, section 1: Applicable definitions** 2) 'authentication factor' means a factor confirmed as being bound to a person, which falls into any of the following categories […] **LoA Annex, section 2.2.1: Electronic identification means characteristics and design** The electronic identification means is designed so that it can be assumed to be used only if under the control or possession of the person to whom it belongs. **M72B, section 6.3: Connecting identification means to a person** 6.3.1		Examples include binding of identification application to a person, chip personalisation or the linking of a pass code list or device to a person.

			The authentication factors of the identification means must be bound to the identification means holder in the identification scheme. 6.3.2 An identification means shall not be bound to an applicant before the applicant has passed initial identification or it has been otherwise ensured in the process of granting an identification means that the identification means is not functional before the initial identification referred to in section 17 of the Identification and Trust Services Act has been performed.		
7.	S,H	The authentication mechanism is designed so that each identification event has unique electronic proof.	**ITSA, section 8 a** […] Every identification means must use a dynamic authentication referred to in section 2.3.1 of the Annex to Act on Level of Assurance in Electronic Identification that changes in every new authentication event between the person and the system certifying their identity. **LoA Annex, section 1: Applicable 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. **LoA Annex, section 2.3.1: Authentication mechanism** The release of person identification data is preceded by reliable verification of the electronic identification means and its validity through a dynamic authentication process.		Also applies to identification broker services. LoA Guidance (extracts): 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. […] 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. […] 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.
8.	S,H	The electronic proof of each identification event is based on authentication factors bound to a person.	**LoA Annex, section 1: Applicable 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. **M72B, section 6.3: Connecting identification means to a person** 6.3.1 The authentication factors of the identification means must be bound to the identification means holder in the identification scheme. **LoA Annex, section 2.3.1: Authentication mechanism** Substantial: 1. The release of person identification data is preceded by reliable verification of the electronic identification means and its validity through a dynamic authentication process. 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		The authentication factors cannot be copyable.

			communication by an attacker with moderate attack potential can subvert the authentication mechanisms.		
9.	H	The user is able to protect the identification means and their authentication factors reliably against use by others.	**LoA Annex, section 2.2.1: Electronic identification means characteristics and design** The electronic identification means is designed so that it can be reliably protected by the person to whom it belongs against use by others. Also **LoA Annex, section 2.2.2: Issuance, delivery and activation** The activation process verifies that the electronic identification means was delivered only into the possession of the person to whom it belongs. **M72B, section 6.1: Identification means characteristics and its resistance** 6.1.1 The authentication factors, authentication mechanism and security measures of the identification means must be planned, executed and maintained so that they protect the integrity and confidentiality of the identification means. The identification means must be able to resist at least moderate or high-level threats and attack potential specified in section 2.3 of the appendix to the regulation on Level of Assurance in Electronic Identification in accordance with the assurance level of the identification service. […] 6.1.2 The features and security measures of the identification means must prevent the possibility that the compromise of one authentication factor would compromise the reliability of other authentication factors. The security measures protecting the identification means must separate and protect the authentication factors especially if they are used on the same terminal device.		Examples from LoA Guidance: 'reliably protected' refers to the efforts taken to prevent the electronic identification means from being used without the subject's knowledge and active consent. As an example, a private key in a cryptographic key token should not be usable by a machine process without the user's active consent (e.g. by using a PIN). This is a requirement to protect against: duplication, guessing, replay and manipulation of communication threats. Other techniques that might be used, in addition to those mentioned previously (see also LoA Guidance, section 2.2.1, high 1): - Strength of static passwords - Biometric verification of the user - Checks of the environment against malicious code - Out of band verification

			M72B, section 6.4: Processing identification means holder-specific data 6.4.1 The identification service provider shall ensure that secret data related to an identification means is not revealed to its staff under any circumstances. 6.4.2 The identification service provider shall not make copies of any secret data related to an identification means.		- For all secrecy-based authentication factors (static passwords, one-time password in hardware), guessing is a threat which should be mitigated in order to reach a very high level of resilience – e.g. by limiting the number of attempts/slowdown mechanisms and by ensuring sufficient entropy. LoA Guidance, section 2.2.2, high: For level High the activation process shall ensure that only the legitimate owner can activate the electronic identification means and that the activation process is protected from accidental loss and insider threats such as collusion. NOTE! The user must be able to ensure that the security factors, or e.g. a resetting code connected to the identification means, cannot be available to others. Any activation or resetting codes can only be used once.

					This ensures that a reusable activation code cannot be used to invalidate, i.e. overwrite, the knowledge-based authentication factor (PIN) without the user's knowledge. There is no reference in the Identification Act to section 2.2.3 of the LoA ("The existence of measures taken to prevent unauthorised suspension, revocation and/or reactivation." However, the one-time use of the code is a good practice, if unauthorized reactivation of the identification means cannot be protected in other ways.
10.	S,H	No identification data is released to the relying party (no identification event is performed) before the identification means is verified using dynamic authentication.	**LoA Annex, section 2.3.1: Authentication mechanism** The release of person identification data is preceded by reliable verification of the electronic identification means and its validity through a dynamic authentication process.	A.14.1 System acquisition, development and maintenance / Security requirements of information systems A.14.1.2 Securing application services on public networks A.14.1.3 Protecting	Also applies to identification broker services.

				application services transactions	
11.	S,H	The identification data (personal data) stored in the identification event is protected.	**LoA Annex, section 2.3.1: Authentication mechanism**Where person identification data is stored as part of the authentication mechanism, that information is secured in order to protect against loss and against compromise, including analysis offline. **M72B, section 7.1: Communications encryption methods** 7.1.1 Interfaces between identification service providers and interfaces between an identification service provider and relying parties shall be encrypted. [see methods later in the regulation] **M72B, section 9.1: Protecting messages between identification services and relying parties** 9.1.1 The **integrity and confidentiality of authentication messages containing personal data must be protected** in communications between identification services and between identification services and relying parties in one of the following ways: a) by ensuring the integrity and confidentiality of the communications connection by binding the parties' communications to digital certificates or keys provided in compliance with section 8, or b) by encrypting and signing the messages with a key provided in compliance with the procedure in section 8.		Also applies to identification broker services. All technical environments of the participants of the identification event where identification data is stored must be taken into account.
12.	S	The security measures used in the identification means provide	**ITSA, section 8: Requirements posed on the electronic identification scheme**	ISO 29115	Cf. criteria 1 risk assessment and

		protection against attacks of a moderate severity rating.	Section 8.1, paragraph 3: The identification means can be used to verify that only the holder of the identification means can use the means in a way that, at a minimum, meets the conditions for assurance level substantial laid down in sections 2.2.1 and 2.3 of the Annex to the Act on Level of Assurance in Electronic Identification. **LoA Annex, section 2.3.1: Authentication mechanism** 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.	ISO/IEC 15408-1 ISO/IEC 18045, Annex B Common Criteria CCDB 2009 03, part 3 ETSI TS 102 165-1, clauses 6.6 and 6.7	calculation of attack potential The assessment should take relevant threats into account. 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. 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. Common Criteria and ETSI 102 165-1 contain instructions for the calculation of attack potential.

					The authentication mechanism needs to take the threat of identification requests initiated by incorrect eServices or the hijacking of an identification session (phishing) into account. See description in LoA Guidance, section 2.3.1 Also applies to identification broker services.
13.	H	The security measures used in the identification means provide protection against attacks of high severity rating.	**ITSA, section 8: Requirements posed on the electronic identification scheme** Section 8.1, paragraph 3: The identification means can be used to verify that only the holder of the identification means can use the means in a way that, at a minimum, meets the conditions for assurance level substantial laid down in sections 2.2.1 and 2.3 of the Annex to the Act on Level of Assurance in Electronic Identification. **LoA Annex, section 2.2.1: Electronic identification means characteristics and design** The electronic identification means protects against duplication and tampering against attackers with high attack potential. **LoA Annex, section 2.3.1: Authentication mechanism** 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 high attack	See above.	Also applies to identification broker services. All security considerations related to the authentication mechanism should be proportioned for attack potentials of a high severity rating.

			potential can subvert the authentication mechanisms.		
14.	S, H	The authentication mechanism displays the name of the eService in the means and identification process stages where possible.	**M72B, section 6.2.2** The identification service must present the identification means user with information concerning the relying party, for whom the identification is carried out, during the identification event. This information must be presented in identification means that have the technical ability to do so. **M72B, section 12.1: Mandatory set of data** The following minimum set of data shall be relayed at the interface between the identification means provider and the provider of an identification broker service: [...] 4) name of the relying party authenticated by the identification broker service.		Also applies to identification broker services.
15.	S, H	The authentication mechanism displays the session identifier in the means and identification process stages where possible.	**M72B, section 6.2.1** The identification service must present the user with information during the identification event, based on which the user may ensure that the identification request received in the identification means by the user is connected to the user's event. This information must be presented in identification means that have the technical ability to do so.		Also applies to identification broker services.
16.	S,H	The authentication mechanism follows the mandatory encryption requirements between the **identification means provider and the identification broker services.**	**LoA Annex, section 2.4.6: Technical controls** 2. Electronic communication channels used to exchange personal or sensitive information are protected against eavesdropping, manipulation and replay. **M72B, section 7.1: Identification scheme interface encryption requirements** 7.1.1 Interfaces between identification service providers and interfaces between an identification service provider and relying parties shall be encrypted. The following methods shall be used in the encryption, key exchange, digital certificates and signing:	A.10.1.1 Policy on the use of cryptographic controls A.13.2.3 Communications security / Information transfer: Electronic messaging	Also applies to identification broker services.

			1) Key exchange: In key exchange, DHE methods or ECDHE methods with elliptic curves shall be used. The size of the finite field to be used in calculations shall be at least 2,048 bits in DHE and at least 224 bits in ECDHE. 2) Signature or asymmetric encryption: When using the RSA for electronic signatures or encryption, the key length shall be at least 2,048 bits. When using the ECDSA or EdDSA methods with elliptic curves, the size of the finite field must be at least 224 bits. 3) Symmetrical encryption: The encryption algorithm must be AES, Serpent or ChaCha20. The key length shall be at least 128 bits. The encryption mode must be CBC, CCM, GCM or CTR. 4) Hash functions: The hash function or authentication code must be SHA-2, SHA-3, Whirlpool or Poly1305. 7.1.2 In addition to methods and values mentioned in section 7.1.1, methods and values that have been assessed as secure in use specified in subsections 1–4 in the current versions of the following documents may also be complied with: a) Kryptografiset vahvuusvaatimukset luottamuksellisuuden suojaamiseen - kansalliset turvallisuusluokat (Dnro 190/651/2015) instruction (in Finnish) issued by the Crypto Approval Authority operating within the Finnish Transport and Communications Agency, or b) SOG-IS Crypto Evaluation Scheme Agreed Cryptographic Mechanisms of the SOGIS-MRA (Senior Officers Group for Information Systems, Mutual Recognition Agreement), an agreement between		

			certain certification bodies of EU or EEA Member States. 7.1.3 Encryption settings shall be technically forced to the minimum levels listed above to avoid a situation where settings weaker than the minimum levels are adopted following connection handshakes. **7.2 Communications encryption protocol** If the TLS protocol is used, version 1.2 of TLS or newer shall be used. The integrity and confidentiality of messages containing personal data shall be protected by encryption referred to paragraph 1 above and also at a message level in accordance with paragraph 1. **M72B, section 8: Authenticating parties to the communications** **8.1 Verification of the parties to the communications connection** The authenticity and integrity of the digital certificates or keys used to encrypt the communications or messages as well as their holders must be verified in establishing communications connections between identification services and identification services and relying parties. The authentication must be based on a qualified electronic signature or a qualified electronic seal in compliance with the eIDAS Regulation or a direct bilateral procedure. Authentication may not only be based on a generally trusted digital certificate. **8.2 Certificate and key renewal**		

			The digital certificates and keys referred to in section 8.1 above must be regularly renewed. In order to ensure the authenticity and integrity of new digital certificates and keys, the renewal must be carried out in one of the following ways: a) in accordance with the procedure in section 8.1; b) by providing new keys via a communications connection, whose integrity and confidentiality has been ensured by binding the parties' communications to digital certificates or keys provided in accordance with section 8.1; or c) by signing a new key using a key provided in accordance with section 8.1 or a key chained from such a key. **M72B, section 9: Integrity and confidentiality of authentication messages** **9.1: Protecting messages between identification services and relying parties** 9.1.1 The integrity and confidentiality of authentication messages containing personal data must be protected in communications between identification services and between identification services and relying parties in one of the following ways: a) by ensuring the integrity and confidentiality of the communications connection by binding the parties' communications to digital certificates or keys provided in compliance with section 8; or b) by encrypting and signing the messages with a key provided in compliance with the procedure in section 8. 9.1.2		

			Authentication messages between identification broker services and relying parties must be authenticated with signatures. **9.2 Protecting messages in the user interface** If the authentication messages are relayed via the user's browser or terminal device, the messages must be encrypted and signed in accordance with subsection 9.1.1.b). **9.3 Encryption algorithms and procedures** The encryption and signing of messages must employ the procedures specified in section 7.1, where applicable.		
17.	S,H	The authentication mechanism follows the mandatory encryption requirements **between the identification service and the eService.**	**LoA Annex, section 2.4.6: Technical controls** 2. Electronic communication channels used to exchange personal or sensitive information are protected against eavesdropping, manipulation and replay. **M72B, sections 7–8 (above)** **M72B, section 9: Integrity and confidentiality of authentication messages** **9.1: Protecting messages between identification services and relying parties** 9.1.1 The integrity and confidentiality of authentication messages containing personal data must be protected in communications between identification services and between identification services and relying parties in one of the following ways: a) by ensuring the integrity and confidentiality of the communications connection by binding the parties' communications to digital certificates or keys provided in compliance with section 8, or	A.10.1.1 Policy on the use of cryptographic controls A.13.2.3 Communications security / Information transfer: Electronic messaging A 14.1.1. Information security requirements analysis and specification A 14.1.2 Securing application services	Note! Also applies to identification broker services.

			b) by encrypting and signing the messages with a key provided in compliance with the procedure in section 8. **9.2 Protecting messages in the user interface** If the authentication messages are relayed via the user's browser or terminal device, the messages must be encrypted and signed in accordance with subsection 9.1.1.b). **9.3 Encryption algorithms and procedures** The encryption and signing of messages must employ the procedures specified in section 7.1, where applicable.	on public networks	
18.	S,H	The authentication mechanism follows the mandatory encryption requirements **on the user interface (browser, mobile device).**	**LoA Annex, section 2.4.6: Technical controls** 2. Electronic communication channels used to exchange personal or sensitive information are protected against eavesdropping, manipulation and replay. **M72B, section 7 (above)** **M72B, section 9.2: Protecting messages in the user interface** If the authentication messages are relayed via the user's browser or terminal device, the messages must be encrypted and signed in accordance with subsection 9.1.1.b). **M72B, section 9.3: Encryption algorithms and procedures** The encryption and signing of messages must employ the procedures specified in section 7.1, where applicable.	A.10.1.1 Policy on the use of cryptographic controls A.13.2.3 Communications security / Information transfer: Electronic messaging	Note! Also applies to identification broker services.
19.	H	The authentication method follows the **recommended** tightened/high level encryption requirements between the identification means service and identification brokering service,	**MPS72B, section 4.7.1.3 (20 May 2022) recommendation** At the high level of assurance, instead of using the requirements for substantial level of assurance provided in section 7.1 of the	A.10.1.1 Policy on the use of cryptographic controls	Note! Also applies to identification broker services.

		between the identification service and the eServices and in the user interface (browser, mobile device).	Regulation, it is recommended to apply the following values in parentheses, **which will meet the minimum assurance level of 128 bits**, to the identification scheme: 1) **Key exchange**: In key exchange, DHE methods or ECDHE methods with elliptic curves shall be used. The size of the finite field to be used in calculations shall be at least 2,048 (**4,096 at high level of assurance**) bits in DHE and at least 224 (**256 at high level of assurance**) bits in ECDHE. The DH groups 14 to **21**, 23, 24 and 26 (**from 16 to 21** at high level of assurance) of IANA's IKEv2 specifications meet the above requirements. 2) Signature or asymmetric encryption: When using the RSA for electronic signatures or encryption, the key length shall be at least 2,048 (**3,072 at high level of assurance**) bits. When using the elliptic curve method ECDSA or EdDSA, the underlying field size shall be at least 224 (**256 at high level of assurance**) bits. 3) Symmetrical encryption: The encryption algorithm must be AES, Serpent or ChaCha20 (***AES or Serpent* at high level of assurance**). The key length shall be at least 128 (**128 at high level of assurance**) bits. The encryption mode must be CBC, CCM, GCM or CTR. 4) Hash functions: The hash function or authentication code must be SHA-2, SHA-3, Whirlpool or Poly1305. SHA-2 refers to functions SHA224, SHA256, SHA384 and SHA512 (**SHA-3-256, SHA-3-384, SHA-3-512 at high level of assurance**).	A.13.2.3 Communications security / Information transfer: Electronic messaging	

B 2 Interoperability

KEY PROVISIONS

ITSA, section 29: Conformity assessment of an electronic identification service
An identification service provider must regularly subject their service to an assessment by an assessment body referred to in section 28 to determine whether the identification service meets the requirements on interoperability, information security, data protection and other reliability laid down in this Act.
[…]

M72B, section 15: Conformity assessment criteria
The identification service assessment shall cover the requirements concerning the following:
1) certain properties of the functions affecting the provision of the identification service (the identification scheme), namely:
   d) technical measures (controls)
   e) interoperability in the trust network

ITSA, section 12: Register related to an identification service provider
[…]
Identification service providers must collaborate to ensure that the technical interfaces of the members of a trust network are interoperable and that they enable the provision of interfaces that implement commonly known standards to the relying parties.
[…]

M72B, section 12: Minimum set of data to be relayed in a trust network
12.1 Mandatory set of data
The following minimum set of data shall be relayed at the interface between the identification means provider and the provider of an identification broker service:
1) in identification events concerning natural persons: at least the first name, family name, date of birth and the unique identifier of the person authenticated by the identification means provider;
2) in identification events concerning legal persons: at least the first name, family name and the unique identifier of the natural person representing the legal person as well as the unique identifier of the organisation authenticated by the identification means provider;
3) an indication of whether the level of assurance is substantial or high; as well as
4) name of the relying party authenticated by the identification broker service.

12.2 Optional information
The interface between the identification means provider and the provider of an identification broker service must have the technically planned possibility to relay the following information:
1) indication of whether the identification event concerns a public administration eService or a private eService;
2) in identification events concerning natural persons: forename(s) and surname(s) at the time of birth, place of birth, current address and gender; and
3) in identification events concerning legal persons:

a) current address;
b) VAT registration number;
c) tax reference number;
d) the identifier related to Article 3(1) of Directive 2009/101/EC of the European Parliament and of the Council;
e) Legal Entity Identifier (LEI) referred to in Commission Implementing Regulation (EU) No 1247/20122;
f) Economic Operator Registration and Identification (EORI) referred to in Commission Implementing Regulation (EU) No 1352/20133; and
g) excise number provided in Article 2(12) of Council Regulation (EC) No 389/20124.

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

14 Data transfer protocol and other requirements
14.1 Data transfer protocol
The identification service provider must enable the chaining of initial identification in accordance with section 17 of the Identification and Trust Services Act and relaying identification events within the trust network in accordance with section 12 a of the Identification and Trust Services Act using an interface conforming to at least either the Open IDConnect or SAML protocol.

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

NO.	LEVEL OF ASSURANCE	REQUIREMENT PERTAINING TO THE IDENTIFICATION SERVICE (SUMMARY)	PROVISIONS	STANDARD REFERENCE	NOTES
20.	S, H	The identification service provider offers at least one interface in the trust network that complies with a universally applied standard.	**Government Decree 169/2016 on the trust network of strong electronic identification services providers** **Section 1: Technical interfaces of a trust network** Technical interfaces referred to in section 12 a, paragraph 2 of the Act on Strong Electronic Identification and Electronic Signatures (617/2009), hereinafter referred to as the Identification Act, are: 1) interface between identification means providers;		**Application: M72B, section 14.1: stricter requirement of "an interface conforming to at least either the OpenID Connect or SAML protocol"** The Finnish Transport and Communications Agency has provided recommended profiles for the SAML and Open IDConnect protocols taking

			2) interface between an identification means provider and an identification broker service provider; 3) interface between an identification broker service provider and an identification service relying party. The identification service providers in a trust network may agree on an interface required for the transmission of a charge for identification data referred to in section 12 a, paragraph 3 of the Identification Act or other interface necessary for the operation of the trust network. An identification service provider belonging to a trust network shall, in both the interfaces referred to in subsection 1, paragraphs 1 and 2, provide at least one technical interface that meets a universally applied standard. **M72B, section 14: Data transfer protocol and other requirements** **14.1 Data transfer protocol** The identification service provider must enable the chaining of initial identification in accordance with section 17 of the Identification and Trust Services Act and relaying identification events within the trust network in accordance with section 12 a of the Identification and Trust Services Act using an interface conforming to at least either the Open IDConnect or SAML protocol.		into account recommendations given by the trust network collaboration group. Recommendation 212/2023 S Finnish Trust Network SAML Protocol Profile Recommendation 213/2023 S Finnish Trust Network OpenID Connect Protocol Profile The recommendations are available online at https://www.kyberturvallisuuskeskus.fi/en/electronic-identification
21.	S, H	The identification means provider offers the required information (attributes) for the identification of **natural persons**.	**M72B, section 12: Minimum set of data to be relayed in a trust network** **12.1 Mandatory set of data** The following minimum set of data shall be relayed at the interface between the identification means provider and the provider of an identification broker service: 1) in identification events concerning natural persons: at least the first name, family name, date of birth and the unique identifier of the		The broker service can enrich or filter the data received from the identification means provider as needed (see M72B, section 12.3). In any case, the identification means provider must relay data in accordance with M72B, section 12.1.

			person authenticated by the identification means provider; […] 3) an indication of whether the level of assurance is substantial or high; […]		
22.	S, H	The identification means provider has the required **planned capacity** to provide the optional data for the identification of **natural persons**.	**M72B, section 12: Minimum set of data to be relayed in a trust network** **12.2 Optional information** The interface between the identification means provider and the provider of an identification broker service must have the technically planned possibility to relay the following information: 1) an indication of whether the identification event concerns a public administration eService or a private eService; 2) in identification events concerning natural persons: forename(s) and surname(s) at the time of birth, place of birth, current address and gender; […]		MPS72, section 12.1: explanation, p. 56: Being prepared to relay optional attributes means that the processing of optional attributes in the interface and identification schemes must be designed in a way where the identification service provider knows which technical measures are needed for the introduction of the attributes. Technical implementation of optional attributes in systems is not required. However, in the technical configurations, it should be ensured that the optional attributes will not impede identification events, even in those cases where their use has not been agreed upon. A documented plan must, however, be made for supervisory purposes.
23.	S, H	The identification means provider offers the required information (attributes) for the identification of **legal persons**.	**M72B, section 12: Minimum set of data to be relayed in a trust network** **12.1 Mandatory set of data** The following minimum set of data shall be relayed at the interface between the identification means provider and the provider of an identification broker service:		Only if strong electronic identification of legal persons is offered.

			[…] 2) in identification events concerning legal persons: at least the first name, family name and the unique identifier of the natural person representing the legal person as well as the unique identifier of the organisation authenticated by the identification means provider; and 3) an indication of whether the level of assurance is substantial or high; […]		
24.	S, H	The identification means provider has the required planned capacity to provide the optional data for the identification of **legal persons**.	**M72B, section 12: Minimum set of data to be relayed in a trust network** **12.2 Optional information** The interface between the identification means provider and the provider of an identification broker service must have the technically planned possibility to relay the following information: 1) an indication of whether the identification event concerns a public administration eService or a private eService; 2) […] 3) in identification events concerning legal persons: a) current address; b) VAT registration number; c) tax reference number; d) the identifier related to Article 3(1) of Directive 2009/101/EC of the European Parliament and of the Council; e) Legal Entity Identifier (LEI) referred to in Commission Implementing Regulation (EU) No 1247/2012; f) Economic Operator Registration and Identification (EORI) referred to in Commission Implementing Regulation (EU) No 1352/2013; and g) excise number provided in Article 2(12) of Council Regulation (EC) No 389/2012.		

B 3 Technical information security requirements

KEY PROVISIONS

M72B, section 15.1: Identification scheme and identification means features to be assessed
The identification service assessment required in section 29 of the Identification and Trust Services Act must cover all of the requirements specified in the Act and in this regulation, which pertain to:
1) certain properties of the functions affecting the provision of the identification service (the identification scheme), namely:
d) technical measures (controls)

ITSA, section 8: Requirements posed on the electronic identification scheme
4) The identification scheme is reliable and safe so that, at a minimum, it meets the conditions for assurance level substantial laid down in sections … 2.4.6 of the Annex to the Act on Level of Assurance in Electronic Identification and takes into account the threats to the information security of the technology available at the time

LoA Annex, section 2.4.6: Technical controls
1) The existence of proportionate technical controls to manage the risks posed to the security of the services, protecting the confidentiality, integrity and availability of the information processed.

M72B, section 5: Technical information security measures of the identification scheme
5.1 The resistance of the identification scheme
5.1.1
The communications and information systems of the identification scheme and their operation must be planned, executed and maintained throughout the lifecycle of the service so that the integrity and confidentiality of the identification service are protected. The identification service must be able to resist at least moderate or high-level threats and attack potential specified in section 2.3 of the appendix to the regulation on Level of Assurance in Electronic Identification in accordance with the assurance level of the identification service.

5.1.2
The encryption requirements concerning communications connections between identification service providers and the identification service and the relying party are specified in section 7. The encryption of other communications connections of the identification scheme and information systems and data must employ encryption methods specified in section 7 of the regulation, where technically applicable, unless the overall ability of the system to protect itself is otherwise realised by other security means.

5.2 Communications security
The identification scheme communications must be planned, executed and maintained with:
a) structural network security;
b) zoning of the communications network;

c) filtering rules according to the principle of least privilege;
d) administration of filtering and control systems;
e) secure administration connections; as well as
f) employing internationally or nationally recommended encryption methods.

5.3 Information systems security
The identification scheme information systems must be planned, executed and maintained with:
a) access control according to the principle of least privilege;
b) unique identification of the users of the systems;
c) hardening of the systems;
d) malware protection;
e) ability to trace security events and tracing procedure;
f) ability to detect security incidents and repair procedure; as well as
g) employing internationally or nationally recommended encryption methods.

5.4 Safety of operation
The identification scheme operation must be planned, executed and maintained with:
a) change management;
b) confidential data processing environment and storage based on data classification;
c) protecting remote use and administration from threats in the remote use environment;
d) software development and software vulnerability management;
e) backup procedures; and
f) employing internationally or nationally recommended encryption methods.

5.5 Administration and remote connections of the production network of the identification scheme
The production network together with its administration connections and remote access and remote administration referred to in subsections 5.2.e) and 5.4.c) above must be implemented in such a way that the information security threats caused by other services of the organisation, such as e-mail or web browsing, or information security threats caused by other functions than those essential to administration in a terminal used for the administration, are
a) specifically assessed and minimised at a substantial assurance level, and
b) prevented when assessed as a whole at a high assurance level.

B 3.1 Communications security

3.1 Communications security					
NO.	**LEVEL OF**	**REQUIREMENT PERTAINING TO THE IDENTIFICATION SERVICE (SUMMARY)**	**PROVISIONS**	**STANDARD REFERENCE**	**NOTES**

	ASSURANCE				
25.	S, H	Security of data communication: The **data communication connections, control connections and processes** (data communications of subprocesses related to the production of identification services, including the administration of the service) and their **security policies** are **identified, documented and maintained**. Zoning of the communications network and the filtering rules used in the identification scheme must follow the principles of least privilege and defence in depth.	**M72B, section 5.2: Communications security** The identification scheme communications must be planned, executed and maintained with: a) structural network security; b) zoning of the communications network; c) filtering rules according to the principle of least privilege; d) administration of filtering and control systems; e) secure administration connections; as well as f) employing internationally or nationally recommended encryption methods. **LoA Annex, section 2.4.6: Technical controls** 2. Electronic communication channels used to exchange personal or sensitive information are protected against eavesdropping, manipulation and replay.	A.8.1.1 Inventory of assets A.13.1 Communications security / Network security management: A.13.1.1 Network controls A.13.1.3 Segregation in networks	The overall architecture of the identification scheme must ensure the security of data communication. Important: The planning of the identification scheme must also take all relevant data communications with subcontractors (infrastructure, software applications, operator services, ID card production, etc.) into account. The notification/ **assessment report** must include a description of the system architecture including the data communications between different system components and their protection policies. The documentation must clearly describe the network areas of various security levels as well as the filter and control systems between them.
26.	S, H	Security of data communication: The **data communication equipment and systems** of the identification scheme are identified and documented.	**M72B, section 5.2: Communications security** The identification scheme communications must be planned, executed and maintained with: a) structural network security	A.8.1.1 Inventory of assets	

27.	S, H	Security of data communication: The **production network** must be **separated** from the administration and maintenance network. The administration and maintenance network must be separated from office networks. A development environment separate from the production environment is in place.	**M72B, section 5.2: Communications security** The identification scheme communications must be planned, executed and maintained with: a) structural network security b) zoning of the communications network; […] **5.5 Administration and remote connections of the production network of the identification scheme** The production network together with its administration connections and remote access and remote administration referred to in subsections 5.2.e) and 5.4.c) above must be implemented in such a way that the information security threats caused by other services of the organisation, such as e-mail or web browsing, or information security threats caused by other functions than those essential to administration in a terminal used for the administration, are a) specifically assessed and minimised at a substantial assurance level, and b) prevented when assessed as a whole at a high assurance level.	A.12.1.4 Operations security: Separation of development, testing and production environments A.13.1.3 Segregation in networks	The separation can be implemented logically or physically. On the whole, the level of separation that is required depends on the criticality of each network and the information processed using the network in question. The aim of this requirement is to reduce risks to network integrity, confidentiality and availability arising from data communication connections.
28.	S, H	Security of data communication: The data communication connections of the identification scheme are **filtered** based on the least privilege principle.	**M72B, section 5.2: Communications security** The identification scheme communications must be planned, executed and maintained with: […] c) filtering rules according to the principle of least privilege; d) administration of filtering and control systems; […]	A.13.1.1–3 Communications security / Network security management: A.13.1.1 Network controls A.13.1.2 Security of network services A.13.1.3 Segregation in networks	

				See also access control	
29.	S, H	Security of data communication: **Links from the production network to the public network** must be risk-based and used only to enable the functionalities of the service.	**M72B, section 5.2: Communications security** The identification scheme communications must be planned, executed and maintained with: a) structural network security b) […] c) filtering rules according to the principle of least privilege; d) administration of filtering and control systems; e) secure administration connections; as well as f) […] **5.5 Administration and remote connections of the production network of the identification scheme** The production network together with its administration connections and remote access and remote administration referred to in subsections 5.2.e) and 5.4.c) above must be implemented in such a way that the information security threats caused by other services of the organisation, such as e-mail or web browsing, or information security threats caused by other functions than those essential to administration in a terminal used for the administration, are a) specifically assessed and minimised at a substantial assurance level, and b) prevented when assessed as a whole at a high assurance level.	See previous row.	Any other links except those necessary for operations are expressly prohibited or must be closed.
30.	S, H	Security of data communication: **Cryptographic key materials** and **metadata** is exchanged safely between the identification services and the relying parties.	**M72B, section 8: Authenticating parties to the communications** **8.1 Verification of the parties to the communications connection** The authenticity and integrity of the digital certificates or keys used to encrypt the communications or messages as well as their holders must be verified in establishing	A.10.1.2 Cryptography / Key management	cf. PSD2/RTS eIDAS art45 or eSeal certificate requirements for the identification of the parties. A predefined process exists between the parties

			communications connections between identification services and identification services and relying parties. The authentication must be based on a qualified electronic signature or a qualified electronic seal in compliance with the eIDAS Regulation or a direct bilateral procedure. Authentication may not only be based on a generally trusted digital certificate. **8.2 Certificate and key renewal** The digital certificates and keys referred to in section 8.1 above must be regularly renewed. In order to ensure the authenticity and integrity of new digital certificates and keys, the renewal must be carried out in one of the following ways: a) in accordance with the procedure in section 8.1; b) by providing new keys via a communications connection, whose integrity and confidentiality has been ensured by binding the parties' communications to digital certificates or keys provided in accordance with section 8.1; or c) by signing a new key using a key provided in accordance with section 8.1 or a key chained from such a key. **LoA Annex, section 2.4.6: Technical controls** 1. The existence of proportionate technical controls to manage the risks posed to the security of the services, protecting the confidentiality, integrity and availability of the information processed. 2. Electronic communication channels used to exchange personal or sensitive information are protected against eavesdropping, manipulation and replay. […]		for establishing safe trust, authenticating parties and exchanging permanent keys/secrets. The processes and practices of private key management are documented and appropriately implemented. The processes require at least the use of cryptographically strong keys, secure key distribution, secure key storage, regular key exchanges, replacement of old or revealed keys and the prevention of unauthorised key exchanges. KATAKRI 2015 (I12)

			5. All media containing personal, cryptographic or other sensitive information is stored, transported and disposed of in a safe and secure manner. **LoA Annez, section 2.4.6: Technical controls** Substantial: Sensitive cryptographic material, if used for issuing electronic identification means and authentication, is protected from tampering. **LoA Liite, section 2.3.1: Authentication mechanism** Substantial: 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 enhanced-moderate attack potential can subvert the authentication mechanisms.		
31.	H	Security of data communication: Cryptographic key materials and metadata is exchanged safely between the identification services and the relying parties.	Cf. above and **LoA Annex, section 2.3.1: Authentication mechanism** High: 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 high attack potential can subvert the authentication mechanisms.	A.10.1.2 Cryptography / Key management	
32.	S, H	The identification messages of the identification service (broker service or relaying own means) provider and relying party must be authenticated.	**M72B, section 9.1.2** Authentication messages between identification broker services and relying parties must be authenticated with signatures.		
33.	S, H	The integrity and confidentiality of authentication messages is ensured.	**M72B, section 9.1.1** The integrity and confidentiality of authentication messages containing personal data must be protected in communications between identification services and between identification		Section 8 describes different methods for implementing the required communications security.

			services and relying parties in one of the following ways: a) by ensuring the integrity and confidentiality of the communications connection by binding the parties' communications to digital certificates or keys provided in compliance with section 8, or b) by encrypting and signing the messages with a key provided in compliance with the procedure in section 8. **LoA Annex, section 2.4.6: Technical controls** 1. The existence of proportionate technical controls to manage the risks posed to the security of the services, protecting the confidentiality, integrity and availability of the information processed. 2. Electronic communication channels used to exchange personal or sensitive information are protected against eavesdropping, manipulation and replay.		
34.	S, H	Security of data communication: **Administration of the filtering and control systems** of the network connections used in the identification scheme are well organised.	**M72B, section 5.2: Communications security** The identification scheme communications must be planned, executed and maintained with: […] d) administration of filtering and control systems; e) secure administration connections; as well as […]	A.13.1 Communications security / Network security management: A.13.1.1 Network controls	
35.	S	Communications security / management: Information security threats from e-mail and web browsing as well as information security threats caused by other functions than those essential to management	**M72B, section 5.2: Communications security** The identification scheme communications must be planned, executed and maintained with: […] d) administration of filtering and control systems;	A.6.2.2 Teleworking A.9.4 System and application	MPS72: Internet and office networks are considered non-trusted networks unless the office network falls within the scope of a conformity assessment. The data transfer channel must be protected during

		in a terminal used for the management **are assessed and minimised** in the remote operation and administration of the identification scheme.	e) secure administration connections; as well as […] **5.4 Safety of operation** The identification scheme operation must be planned, executed and maintained with: […] c) protecting remote use and administration from threats in the remote use environment; […] **5.5 Administration and remote connections of the production network of the identification scheme** The production network together with its administration connections and remote access and remote administration referred to in subsections 5.2.e) and 5.4.c) above must be implemented in such a way that the information security threats caused by other services of the organisation, such as e-mail or web browsing, or information security threats caused by other functions than those essential to administration in a terminal used for the administration, are a) specifically assessed and minimised at a substantial assurance level, and […]	access control: A.9.4.1 Information access restriction A.9.4.4 Use of privileged utility programmes A.13.1.3 Network controls: Segregation in networks	remote use and the risks caused by the office network must be taken into consideration. The requirements associated with the substantial level of assurance are usual and they are already covered by the requirements of ISO 27001, for instance, if the standard is applied.
36.	H	Communications security / management: Information security threats from e-mail and web browsing as well as information security threats caused by other functions than those essential to the operation of a terminal used for the management are **prevented** in the remote operation and	**M72B, section 5.2: Communications security** The identification scheme communications must be planned, executed and maintained with: […] d) administration of filtering and control systems; e) secure administration connections; as well as […] **5.4 Safety of operation**	See previous row.	

		administration of the identification scheme (production network).	The identification scheme operation must be planned, executed and maintained with: […] c) protecting remote use and administration from threats in the remote use environment; […] **5.5 Administration and remote connections of the production network of the identification scheme** The production network together with its administration connections and remote access and remote administration referred to in subsections 5.2.e) and 5.4.c) above must be implemented in such a way that the information security threats caused by other services of the organisation, such as e-mail or web browsing, or information security threats caused by other functions than those essential to administration in a terminal used for the administration, are […] b) prevented when assessed as a whole at a high assurance level. **MPS72B Explanatory Notes:** At the high level of assurance, the requirements may be met at least by disabling access of a workstation in remote use to other services of the organisation, such as e-mail, and preventing the workstation from using other functions than those essential to the operation of the management network. In practice, this means that there shall be a separate workstation for management. The assessment as a whole required at the high level of assurance means that if other workstations than such hardened workstations described above are used, the separation of the production system and other means for managing information security threats are taken into		

			account in the implementation. In principle, such case requires a virtual termination or a KVM solution. The key point here is what is done on the terminal taking the virtualised connection, and therefore, a two-factor VPN connection to a virtualised workstation alone is not a sufficient solution, for example. Using antivirus and web proxy is not sufficient, either. When transferring necessary files from one terminal to another, the risk of malware shall also be taken into account, for instance, by ensuring the use of reliable sources only and safeguarding information security (integrity) using all appropriate methods.		

B 3.2 Information system security

3.2 Information system security					
NO.	**LEVEL OF ASSURANCE**	**REQUIREMENT PERTAINING TO THE IDENTIFICATION SERVICE (SUMMARY)**	**PROVISIONS**	**STANDARD REFERENCE**	**NOTES**
37.	S, H	Information system security: The **information systems and processes** (processes using information systems that are related to the production of identification services, including the administration of the service) of the identification scheme are **identified, documented and maintained**. The information systems of the identification scheme are **classified** based on the	**M72B, section 5.3: Information systems security** The identification scheme information systems must be planned, executed and maintained with: a) access control according to the principle of least privilege; b) unique identification of the users of the systems; […]	A.8.1.1 Asset management / Responsibility for assets: Inventory of assets A.8.2.1 Asset management / Information classification	Classification of information: the acceptable use of equipment, software application and other assets must be defined.

		information processed by the systems and the actions that they enable. In the classification of the systems, the entire lifecycle of the protected information must be taken into account. The data processing environment used for control operations must be separated from other environments.			
38.	S, H	Information system security: **Access privileges** of the identification scheme are defined and documented. The access privileges are **based** on the classification of information systems and the tasks of each person/user. Access must only be granted based on tasks following the principle of least privilege.	**M72B, section 5.3: Information systems security** The identification scheme information systems must be planned, executed and maintained with: a) access control according to the principle of least privilege; b) unique identification of the users of the systems; c) hardening of the systems; […]	A.9.1.1 Business requirements of access control: Access control policy A.9.1.2 Access to networks and network services A.9.4.1 System and application access control: Information access restrictions	Access rights management is used to limit access to information and data processing environments in a systematic and documented manner.
39.	S, H	Information system security: The users of the information systems of the identification scheme **are identified** using a technique or method that is known and considered safe.	**M72B, section 5.3: Information systems security** The identification scheme information systems must be planned, executed and maintained with: a) access control according to the principle of least privilege; b) unique identification of the users of the systems; c) hardening of the systems;	A.9.4.2 System and application access control: Secure log-on procedures	Such as certificates and two-factor authentication. Generally something other than a password, but if a password is involved, adequate password length and individual (not shared) passwords and user

			d) […] e) ability to trace security events and tracing procedure; f) […]		accounts are a requirement.
40.	S, H	Information system security: Access privileges are controlled and **maintained so they are up to date**.	**M72B, section 5.3: Information systems security** The identification scheme information systems must be planned, executed and maintained with: a) access control according to the principle of least privilege; b) unique identification of the users of the systems; c) hardening of the systems; d) […] e) ability to trace security events and tracing procedure; f) ability to detect security incidents and repair procedure; as well as g) […]	A.9.2 User access management A.9.2.1 User registration and de-registration A.9.2.3 Management of privileged access rights A.9.2.5 Review of user access rights A.9.2.6 Removal or adjustment of access rights	
41.	S, H	Information system security: Staff **duties and functions must be defined** to prevent a situation where one person could cause a severe security incident through their own actions deliberately or by accident (high-risk job combinations).	**M72B, section 5.3: Information systems security** The identification scheme information systems must be planned, executed and maintained with: a) access control according to the principle of least privilege; b) unique identification of the users of the systems; c) hardening of the systems; d) […] e) ability to trace security events and tracing procedure; f) ability to detect security incidents and repair procedure; as well as g) […]	A.6.1.2 Segregation of duties	For example, the possibility of a dishonest or negligent employee granting an identification means in violation of the requirements can be prevented through task definitions and other controls that reduce the risk of error and abuse. As for other sections, the assessment must take both moderate and high attack potentials into account as required by the assurance levels for each identification means.

42.	S, H	Information system security: **Hardening** of the identification scheme is ensured; a procedure is in place for the systematic installation of systems, resulting in a hardened installation. The identification scheme **only** uses the services, functions, processes, equipment and components specifically **required** for its operation. Their usage is defined so that all unnecessary access rights and functions/elements are removed from the installations.	**M72B, section 5.3: Information systems security** The identification scheme information systems must be planned, executed and maintained with: […] c) hardening of the systems; […]	A.12.5. Control of operational software	See also data communications. Guideline 211/2016 included the following criteria, which are included here for reference: A hardened installation only contains the components and services as well as user and process rights that are essential for meeting operational requirements and ensuring security. Only the functions, hardware and services essential for operating requirements and data processing are in use.
43.	S, H	Information system security: Identification, prevention and correction of adverse impacts and threats caused by **malware** is ensured.	**M72B, section 5.3: Information systems security** The identification scheme information systems must be planned, executed and maintained with: […] d) malware protection; e) ability to trace security events and tracing procedure; f) ability to detect security incidents and repair procedure; as well as […]	A.12.2 Protection from malware A.12.6 Technical vulnerability management	See also incident observation capacity.
44.	S, H	Information system security: The identification scheme uses fully recommendable **encryption solutions**.	**M72B, section 5.3: Information systems security** The identification scheme information systems must be planned, executed and maintained with: […] g) employing internationally or nationally recommended encryption methods.	A.10.1 Cryptographic controls A.18.1.5 Regulation of	The MPS72 mentions the following sources: - SOGIS-MRA - NCSA-FI - NIST - Enisa - SANS

				cryptographic controls	Guideline 211/2016 included the following observations, which are included here for reference: The processes require at least the use of cryptographically strong keys, secure key distribution, secure key storage, regular key exchanges, replacement of old or revealed keys and the prevention of unauthorised key exchanges. KATAKRI 2015 (I12)
45.	S, H	Information system security: Cryptographic materials are protected over their entire lifecycle.	**LoA Annex, section 2.4.6: Technical controls** 3) Access to sensitive cryptographic material, if used for issuing electronic identification means and authentication, is restricted to the roles and applications strictly requiring access. It shall be ensured that such material is never persistently stored in plain text. Substantial: Sensitive cryptographic material, if used for issuing electronic identification means and authentication, is protected from tampering. **M72B, section 5.3: Information systems security** The identification scheme information systems must be planned, executed and maintained with: a) access control according to the principle of least privilege; b) unique identification of the users of the systems; c) hardening of the systems; […]	A.8.2.1 Classification of information A.10.1.1 Policy on the use of cryptographic controls A.10.1.2 Cryptography / Key management	Guideline 211/2016 included the following observations, which are included here for reference: Private keys shall only be available to authorised users and processes. The processes and practices of private key management are documented and appropriately implemented. The processes require at least the use of cryptographically strong keys, secure key distribution, secure key storage, regular key exchanges, replacement of

			g) employing internationally or nationally recommended encryption methods. **M72B, section 5.4: Safety of operation** The identification scheme operation must be planned, executed and maintained with: […] b) confidential data processing environment and storage based on data classification; […] f) employing internationally or nationally recommended encryption methods.		old or revealed keys and the prevention of unauthorised key exchanges. KATAKRI 2015 (I12)

B 3.3 Operator security

3.3 Operator security					
NO.	**LEVEL OF ASSURANCE**	**REQUIREMENT PERTAINING TO THE IDENTIFICATION SERVICE (SUMMARY)**	**PROVISIONS**	**STANDARD REFERENCE**	**NOTES**
46.	S, H	Operator security: **Change management** of the identification scheme is planned and careful.	**M72B, section 5.4: Safety of operation** The identification scheme operation must be planned, executed and maintained with: a) change management; […]	A.12.1.2 Operations security / Operational procedures and responsibilities : Change management A.14.2.2 System acquisition, development and maintenance / Security in development and support	Clear processes have been defined for change management. In the implementation of new features or changes, the testing plan also takes into account negative test cases. Testing is not based solely on automatic tests.

				processes: System change control procedures A.14.2.3 Technical review of applications after operating platform changes A.14.2.4 Restrictions on changes to software packages	
47.	S, H	Operator security: Management of the **software vulnerabilities** of the identification scheme is planned and systematic. Detection, prevention and correction of adverse impacts and threats caused by **software vulnerabilities** are ensured in the identification scheme.	**M72B, section 5.4: Safety of operation** The identification scheme operation must be planned, executed and maintained with: […] d) software development and software vulnerability management; […]	A.12.5.1 Operations security: Installation of software on operational systems A.12.6.1 Operations security: Management of technical vulnerabilities A.14.2 System acquisition, development and maintenance / Security in development and support processes	The organisation must maintain a database or listing of all different software components of the identification scheme. The organisation must have a process for the detection and monitoring of software vulnerabilities. Exposed software components must be updated to current versions. The software used in the identification scheme must comply with secure programming principles. New versions of the identification scheme must be tested, also by

				A.14.2.1 Secure development policy A.14.2.2 System change control procedures A.14.2.3 Technical review of applications after operating platform changes A.14.2.4 Restrictions on changes to software packages A.14.2.5 Secure system design principles A.14.2.6 Secure development environment A.14.2.7 Outsourced development A.14.2.8 System security testing A.14.2.9 System acceptance testing	including negative test cases.

48.		Operator security: The identification scheme operation must be planned, executed and maintained with: Software development management	**M72B, section 5.4: Safety of operation** The identification scheme operation must be planned, executed and maintained with: a) change management; […] d) software development and software vulnerability management; […]	See previous	The management of software development must pay particular attention to the supply chain structure and maintain information about the different components of the software and monitor their updates. Safe software development Testing
49.	S, H	Operator security: **Backup copies** of the identification scheme are organised in a planned and systematic manner. Backup procedures take information categories (personal information, cryptographic information, etc.), system recoverability and storage of backup copies into account.	**M72B, section 5.4: Safety of operation** The identification scheme operation must be planned, executed and maintained with: […] e) backup procedures; and […]	A.12.3.1 Information backup	Guideline 211/2016 included the following observations, which are included here for reference: The physical location of back-up copies is sufficiently separate from the actual system.

B 4 Security incident observation capacity; management of security incidents; disturbance notifications

KEY PROVISIONS

M72B, section 15.1: Identification scheme and identification means features to be assessed
The identification service assessment required in section 29 of the Identification and Trust Services Act must cover all of the requirements specified in the Act and in this regulation, which pertain to:
1) certain properties of the functions affecting the provision of the identification service (the identification scheme), namely:
d) technical measures (controls)

General requirements

ITSA, section 8: Requirements posed on the electronic identification scheme
4) The identification scheme is reliable and safe so that, at a minimum, it meets the conditions for assurance level substantial laid down in sections … 2.4.6 of the Annex to the Act on Level of Assurance in Electronic Identification and takes into account the threats to the information security of the technology available at the time

LoA Annex, section 2.4.6: Technical controls
1. The existence of proportionate technical controls to manage the risks posed to the security of the services, protecting the confidentiality, integrity and availability of the information processed.
4. Procedures exist to ensure that security is maintained over time and that there is an ability to respond to changes in risk levels, incidents and security breaches.

ITSA, section 16: Notifications of the identification service provider concerning threats or disruptions to their operations and protection of data
Notwithstanding any secrecy provisions, an identification service provider shall inform the parties relying on their identification service, holders of identification means, other agreement parties operating in the trust network and the Finnish Transport and Communications Agency without undue delay of all significant threats or disruptions to the operation of the service, information security or the use of an electronic identity. […]
The notification specified in subsection 1 above shall also include information about measures the parties involved have for use to counter such threats and risks, as well as the estimated expenses incurred by these measures.
[…]

The requirements are specified in M72B, sections 5 and 11.

NO.	LEVEL OF ASSURANCE	REQUIREMENT PERTAINING TO THE IDENTIFICATION SERVICE (SUMMARY)	PROVISIONS	STANDARD REFERENCE	NOTES
50.	S, H	**Capacity** and **predefined processes** for observing deviations in the identification scheme exist. The specifications take into account the importance/criticality/classification of the scheme's data communication connections, information system components and the ability to trace security-	**M72B, section 5.2: Communications security** The identification scheme communications must be planned, executed and maintained with: […] d) administration of filtering and control systems; […] **M72B, section 5.3: Information systems security** The identification scheme information systems must be planned, executed and maintained with:	A.12.4.1 Operations security: Event logging A.12.4.2 Operations security: Protection of log information A.12.4.3 Operations security:	The processes contain both automatic and manual means. The processes are maintained.

		related incidents also in retrospect. The identification scheme collects and stores **event logs** on the scheme's operation and any events and irregularities that have impact or are related to information security.	a) access control according to the principle of least privilege; b) unique identification of the users of the systems; […] e) ability to trace security events and tracing procedure; f) ability to detect security incidents and repair procedure; as well as […]	Administrator and operator logs A.16.1 Information security incident management / Management of information security incidents, events and weaknesses A.16.1.1 Responsibilities and procedures A.16.1.6 Learning from information security incidents	
51.	S, H	The **control logs** of the identification scheme are defined and separated from other log data. Their integrity is ensured.	**M72B, section 5.2: Communications security** The identification scheme communications must be planned, executed and maintained with: […] d) administration of filtering and control systems; e) secure administration connections; as well as […] **M72B, section 5.3: Information systems security** The identification scheme information systems must be planned, executed and maintained with: a) access control according to the principle of least privilege;	A.12.4.1 Operations security: Event logging A.12.4.2 Operations security: Protection of log information A.12.1.4 Separation of development, testing and	Information on changes implemented in the identification scheme are saved in control logs.

			b) unique identification of the users of the systems; […] e) ability to trace security events and tracing procedure; f) ability to detect security incidents and repair procedure; as well as […]	operational environments	
52.	S, H	The operation, changes and events in the identification scheme are **monitored** to detect any irregularities and information security violations. **Irregularities and malfunctions of the identification scheme are processed and analysed**, and their impact/severity is classified in a systematic and organised manner.	**M72B, section 5.2: Communications security** The identification scheme communications must be planned, executed and maintained with: […] d) administration of filtering and control systems; […] **M72B, section 5.3: Information systems security** The identification scheme information systems must be planned, executed and maintained with: […] e) ability to trace security events and tracing procedure; f) ability to detect security incidents and repair procedure; as well as […]	A.16.1 Information security incident management / Management of information security incidents, events and weaknesses: A.16.1.2 Reporting information security events A.16.1.3 Reporting information security weaknesses A.16.1.4 Assessment and decision on information security events	All observations are discussed and their impact is classified according to predetermined criteria. Log analysis is performed with automatic processes/tools, such as SIEM.
53.	S, H	**Corrective actions** required by irregularities and malfunctions of the identification scheme are systematic and effective.	**M72B, section 5.2: Communications security** The identification scheme communications must be planned, executed and maintained with: […]	A.16.1 Information security incident management /	Corrective measures must be documented. Service-level agreements (SLA) are contractual

		Planning of the continuity of operations includes preventive and corrective actions that are used to minimise the impact of significant malfunctions or exceptional events.	d) administration of filtering and control systems; […] **M72B, section 5.3: Information systems security** The identification scheme information systems must be planned, executed and maintained with: […] e) ability to trace security events and tracing procedure; f) ability to detect security incidents and repair procedure; as well as […]	Management of information security incidents, events and weaknesses: A.16.1.5 Response to information security incidents 7.5 Documented information 10.1 Nonconformity and corrective action	matters. Their non-discriminatory nature must be ensured.
54.	S, H	The incident management processes feature a **requirement to report to other identification services within the trust network.**	**ITSA, section 16: Notifications of the identification service provider concerning threats or disruptions to their operations and protection of data** Notwithstanding any secrecy provisions, an identification service provider shall inform […] other agreement parties operating in the trust network […] without undue delay of all significant threats or disruptions to the operation of the service, information security or the use of an electronic identity. […] An identification service provider can, without prejudice to secrecy provisions, notify all members of a trust network of the threats and disruptions referred to in subsection 1 and of service providers of whom there is reason to believe that they are seeking unauthorised financial gain, giving false or misleading	A.16.1.2 Information security incident management / Management of information security incidents, events and weaknesses: Reporting information security events	Responsibilities related to incidents and stakeholder communications have been defined.

			information that is significant or processing personal data illegally. **Application:** The trust network collaboration group has drafted a joint policy for malfunction situations requiring mutual notification as well as notification thresholds.		
55.	S, H	The incident management process features a **requirement to notify users and relying parties.**	**ITSA, section 16: Notifications of the identification service provider concerning threats or disruptions to their operations and protection of data** An identification service provider shall inform the parties relying on their identification service, holders of identification means, […] without undue delay of all significant threats or disruptions to the operation of the service, information security or the use of an electronic identity. The notification shall also include information about measures the parties involved have for use to counter such threats and risks, as well as the estimated expenses incurred by these measures.	A.16.1.2 Information security incident management / Management of information security incidents, events and weaknesses: Reporting information security events	Responsibilities related to incidents and stakeholder communications have been defined. Relying parties mean eServices.
56.	S, H	The incident management process features a **requirement to notify the Finnish Transport and Communications Agency.**	**ITSA, section 16: Notifications of the identification service provider concerning threats or disruptions to their operations and protection of data** Notwithstanding any secrecy provisions, an identification service provider shall inform […] the Finnish Transport and Communications Agency without undue delay of all significant threats or disruptions to the operation of the service, information security or the use of an electronic identity. The notification shall also include information about measures the parties involved have for use to counter such threats and risks, as well as the estimated expenses incurred by these measures.	A.16.1.2 Information security incident management / Management of information security incidents, events and weaknesses: Reporting information security events	The document on the notification threshold defined by the trust network is complied with. Responsibilities related to incidents and stakeholder communications have been defined.

			M72B, section 11: Incident notifications by the identification service provider to the Finnish Transport and Communications Agency **11.1 Significant threats and disruptions** Significant disruptions to the identification service that need to be reported to the Finnish Transport and Communications Agency according to section 16 of the Identification and Trust Services Act include events that are connected to incorrectness or abuse of electronic identity or to an information security threat or disruption that compromises the integrity and reliability of identification. Unforeseeable disruptions with greater than minor effects on the trust network are also considered significant. **11.2 Reported information** Notifications of significant threats or disruptions provided to the Finnish Transport and Communications Agency shall contain at least the following information: 1) identification means or identification broker service affected by the disruption or threat; 2) description of the disruption or threat and any known reasons for it and its duration; 3) description of the impact of the disruption or threat, including the impact on the issuance of new identification means, their users, relying parties, other parties of the trust network, and cross-border use; 4) description of corrective measures; and 5) description of the provision of information on the disruption or threat to relying parties, identification means holders and the trust network as well as information on notifying other authorities. **11.3 Reporting procedure**		

			Significant disruptions or threats must be reported to the Finnish Transport and Communications Agency electronically by using an online form, e-mail or secure e-mail. The report may be amended later on if all of the information is not available at the time of the initial report submitted without undue delay in accordance with section 16 of the Identification and Trust Services Act. **MPS72B explanatory note on the threshold of notification to the Finnish Transport and Communications Agency,** chapter 4.11.1 Provision 11.1: Section 11.1 of the Regulation defines, at a general level, the factors deemed relevant in judging the significance of the disturbance or threat, i.e. the notification threshold. Such significant disturbances include: - issuing an identification means to the wrong person - disturbances related to the functioning of a revocation list in which an up-to-date revocation list is not available - intrusions in the systems of the service provider - disclosure of the identification means provider's certificate signature keys - serious abuse of identification means, such as incidents related to the chaining of identification means - serious internal misconduct. The threshold for deeming faults or abuse related to electronic identities significant is very low, and the same applies to vulnerabilities or flaws that compromise the correctness of the identification data. With respect to usability or quality issues, on the other hand, the notification threshold is, in principle, somewhat higher, and they are deemed more significant mainly in the cases where the		

			issue affects other trust network parties. Such issues include extended disruptions in the identification means or identification broker service that prevent the provision of identification services to e-services. Extended disruptions preventing the chaining of initial identification are significant.		

B 5 Storage and handling of data

KEY PROVISIONS

M72B, section 15.1: Identification scheme and identification means features to be assessed
The identification service assessment required in section 29 of the Identification and Trust Services Act must cover all of the requirements specified in the Act and in this regulation, which pertain to:

1) certain properties of the functions affecting the provision of the identification service (the identification scheme), namely:
   b) record keeping and data processing;
   d) technical measures (controls)

General requirements

ITSA, section 13: General obligations of an identification service provider
The storage of data, the personnel and subcontracted services used by an identification service provider in association with identification shall, at a minimum, meet the requirements laid down for assurance level substantial in sections 2.4.4 and 2.4.5 of the Annex to the Act on Level of Assurance in Electronic Identification.
[…]
The identification service provider shall also protect personal data referred to in section 32 of the Personal Data Act and ensure adequate information security.

LoA Annex, section 2.4.4: Record keeping

1. Record and maintain relevant information using an effective record-management system, taking into account the applicable legislation and good practice in relation to data protection and data retention.
2. Retain, as far as it is permitted by national law or other national administrative arrangement, and protect records for as long as they are required for the purpose of auditing and investigation of security breaches, and retention, after which the records shall be securely destroyed.

ITSA, section 8: Requirements posed on the electronic identification scheme
4) The identification scheme is reliable and safe so that, at a minimum, it meets the conditions for assurance level substantial laid down in sections … 2.4.6 of the Annex to the Act on Level of Assurance in Electronic Identification and takes into account the threats to the information security of the technology available at the time

LoA Annex, section 2.4.6: Technical controls

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

Substantial: Sensitive cryptographic material, if used for issuing electronic identification means and authentication, is protected from tampering.

NO.	LEVEL OF ASSURANCE	REQUIREMENT PERTAINING TO THE IDENTIFICATION SERVICE (SUMMARY)	PROVISIONS	STANDARD REFERENCE	NOTES
57.	S, H	**The management of information** related to the identification scheme and the identification itself **is organised and systematic** and is **based on the classification of information.**	**LoA Annex, section 2.4.4: Record keeping** 1. Record and maintain relevant information using an effective record-management system, taking into account the applicable legislation and good practice in relation to data protection and data retention. **LoA Annex, section 2.4.6: Technical controls** 1. The existence of proportionate technical controls to manage the risks posed to the security of the services, protecting the confidentiality, integrity and availability of the information processed. Substantive: Sensitive cryptographic material, if used for issuing electronic identification means and authentication, is protected from tampering. **M72B, section 5.4: Safety of operation** The identification scheme operation must be planned, executed and maintained with: […] b) confidential data processing environment and storage based on data classification; […]	A.8.2.1 Asset management / Information classification: Classification of information A.18.1.4 Compliance / Compliance with legal and contractual requirements: Privacy and protection of personally identifiable information	The classification takes cryptographic information, identification event information, personal data, business secrets and information related to system security into account.
58.	S, H	Planning of information management takes the entire **lifecycle** of the information into account.	**LoA Annex, section 2.4.4: Record keeping** 2. Retain, as far as it is permitted by national law or other national administrative arrangement, and protect records for as long as they are required for the purpose of auditing and investigation of	A.8.1.1 Inventory of assets A.18.1.4 Compliance /	Matters such as traceability of security-related events and needs arising from the *corresponding* processing principles specified in

		Information **retention times** are defined.	security breaches, and retention, after which the records shall be securely destroyed. **M72B, section 5.4: Safety of operation** The identification scheme operation must be planned, executed and maintained with: […] b) confidential data processing environment and storage based on data classification; […]	Compliance with legal and contractual requirements: Privacy and protection of personally identifiable information	section 24 of the Identification Act need to be taken into account. As a detail, using the attribute ftn_chain_level in connection with initial identification. Guideline 211/2016 included the following observations, which are included here for reference: A sufficiently long time shall be determined for the storage of log data in case of later inspection.
59.	S, H	Compliance with the **specific data retention obligations specified in section 24 of the Identification Act** is ensured.	**ITSA, section 24: Storage and use of data regarding the identification event and means** The identification service provider shall store: 1) data required for performing an individual authentication event and an electronic signature; 2) data on preclusions or restrictions on the use of identification means referred to in section 18; and 3) data content of the certificate as set out in section 19. The provider of an identification means shall store the necessary data about the initial identification of an applicant referred to in section 17 and 17 a and the document or electronic identification used therein. The data referred to above in section 1 subsection 1 shall be stored for five years from the authentication event. Other data referred to	A.12.4.1 Operations security: Event logging	"*…only issues identification means (devices)*" in the Act refers to identification services such as the Digital and Population Data Services Agency's certificate where the provider of the identification means does not relay identification messages in an identification event.

			above in section 1 subsection 2 shall be stored for five years from the termination of a permanent customer relationship. Personal data generated during the authentication event shall be destroyed after the event, unless they are required to be kept to verify an individual authentication event. The identification service provider may process stored data only to perform and maintain the service, for invoicing, to protect its rights in case of disputes, to investigate misuse of personal data as well as upon request by the service provider using the identification service or the holder of the identification means. The identification service provider shall store data on processing, the time, reason, and person processing it. If the service provider only issues identification means (devices): 1) subsection 1, paragraph 1 and subsection 4 do not apply to the provider; 2) The five-year record-keeping period referred to in subsection (3) above will then be calculated from the date the identification means validity expires.		
60.	S, H	**A special requirement of section 24** of the Identification Act on storing of information related to the processing of information that is required to be stored.	**Provisions on identification events and processing related to the identification service are given in section 24 of the Identification Act.** **ITSA, section 24** […] The identification service provider may process stored data only to perform and maintain the service, for invoicing, to protect its rights in case of disputes, to investigate misuse of personal data as well as upon request by the service provider using the identification service or the holder of the	A.12.4.1 Operations security: Event logging A.12.4.3 Administrator and operator logs	The traceability of processing information and log data integrity must be ensured.

			identification means. The identification service provider shall store data on processing, the time, reason, and person processing it. […]		
61.	S, H	**Technical measures are taken to ensure the integrity and confidentiality of the information that is processed and stored** in the identification scheme.	**ITSA, section 8: Requirements posed on the electronic identification scheme** […] 4) The identification scheme is reliable and safe so that, at a minimum, it meets the conditions for assurance level substantial laid down in sections … 2.4.6 of the Annex to the Act on Level of Assurance in Electronic Identification and takes into account the threats to the information security of the technology available at the time **LoA Annex, section 2.4.6: Technical controls** 1. The existence of proportionate technical controls to manage the risks posed to the security of the services, protecting the confidentiality, integrity and availability of the information processed. Substantial: Sensitive cryptographic material, if used for issuing electronic identification means and authentication, is protected from tampering. **M72B, section 5.4: Safety of operation** The identification scheme operation must be planned, executed and maintained with: […] b) confidential data processing environment and storage based on data classification; […] e) backup procedures; and f) employing internationally or nationally recommended encryption methods. **M72B, section 7: Identification scheme interface encryption requirements** **7.1 Communications encryption methods** 7.1.1	A.9.1.1 Access control policy A.9.1.2 Access to networks and network services A.10.1.1 Policy on the use of cryptographic controls A.12.4.2 Operations security: Protection of log information	Data encryption and/or access control. Separation as required (cf. especially cryptographic material). Backup copies/recoverability. Key exchange as defined in the recommendation may be relevant between the identification service and its subcontractors although it is not relevant in drive encryption. Managing and securing the secrets underlying the trust. Storage must take the separation of the physical storage space from the actual system into account.

			Interfaces between identification service providers and interfaces between an identification service provider and relying parties shall be encrypted. The following methods shall be used in the encryption, key exchange, digital certificates and signing: 1) Key exchange: In key exchange, DHE methods or ECDHE methods with elliptic curves shall be used. The size of the finite field to be used in calculations shall be at least 2,048 bits in DHE and at least 224 bits in ECDHE. 2) Signature or asymmetric encryption: When using the RSA for electronic signatures or encryption, the key length shall be at least 2,048 bits. When using the ECDSA or EdDSA methods with elliptic curves, the size of the finite field must be at least 224 bits. 3) Symmetrical encryption: The encryption algorithm must be AES, Serpent or ChaCha20. The key length shall be at least 128 bits. The encryption mode must be CBC, CCM, GCM or CTR. 4) Hash functions: The hash function or authentication code must be SHA-2, SHA-3, Whirlpool or Poly1305. 7.1.2 In addition to methods and values mentioned in section 7.1.1, methods and values that have been assessed as secure in use specified in subsections 1–4 in the current versions of the following documents may also be complied with: a) Kryptografiset vahvuusvaatimukset luottamuksellisuuden suojaamiseen - kansalliset turvallisuusluokat (Dnro 190/651/2015) instruction (in Finnish) issued by the Crypto Approval Authority operating within the Finnish Transport and Communications Agency, or		

			b) SOG-IS Crypto Evaluation Scheme Agreed Cryptographic Mechanisms of the SOGIS-MRA (Senior Officers Group for Information Systems, Mutual Recognition Agreement), an agreement between certain certification bodies of EU or EEA Member States. 7.1.3 Encryption settings shall be technically forced to the minimum levels listed above to avoid a situation where settings weaker than the minimum levels are adopted following connection handshakes. **7.2 Communications encryption protocol** If the TLS protocol is used, version 1.2 of TLS or newer shall be used.		
62.	H	Strict/substantial-level encryption requirements as specified in the **recommendation** are followed in the processing and storage of data.	**MPS72B, section 4.7.1.3 (20 May 2022) recommendation** At the high level of assurance, instead of using the requirements for substantial level of assurance provided in section 7.1 of the Regulation, it is recommended to apply the following values in parentheses, **which will meet the minimum assurance level of 128 bits**, to the identification scheme: 1) **Key exchange**: In key exchange, DHE methods or ECDHE methods with elliptic curves shall be used. The size of the finite field to be used in calculations shall be at least 2,048 (**4,096 at high level of assurance**) bits in DHE and at least 224 (**256 at high level of assurance**) bits in ECDHE. The DH groups 14 to **21**, 23, 24 and 26 (**from 16 to 21** at high level of assurance) of IANA's IKEv2	See above.	Key exchange between the identification service and its subcontractors may be relevant here.

			specifications meet the above requirements. 2) Signature or asymmetric encryption: When using the RSA for electronic signatures or encryption, the key length shall be at least 2,048 (**3,072 at high level of assurance**) bits. When using the elliptic curve method ECDSA or EdDSA, the underlying field size shall be at least 224 (**256 at high level of assurance**) bits. 3) Symmetrical encryption: The encryption algorithm must be AES, Serpent or ChaCha20 (***AES or Serpent* at high level of assurance**). The key length shall be at least 128 (**128 at high level of assurance**) bits. The encryption mode must be CBC, CCM, GCM or CTR. 4) Hash functions: The hash function or authentication code must be SHA-2, SHA-3, Whirlpool or Poly1305. SHA-2 refers to functions SHA224, SHA256, SHA384 and SHA512 (**SHA-3-256, SHA-3-384, SHA-3-512 at high level of assurance**).		
63.	S, H	All **media** containing personal, cryptographic or other sensitive information is stored, transported and disposed of in a safe and secure manner.	**LoA Annex, section 2.4.6: Technical controls** 5) All media containing personal, cryptographic or other sensitive information is stored, transported and disposed of in a safe and secure manner. **M72B, section 5.4: Safety of operation** The identification scheme operation must be planned, executed and maintained with: […] b) confidential data processing environment and storage based on data classification; […]	A.8.3 Asset management / Media handling A.11.2.6 Security of equipment and assets off-premises A.11.2.7 Secure disposal or re-use of equipment	Management, disposal and transfer.

B 6 Security of physical premises

KEY PROVISIONS

M72B, section 15.1: Identification scheme and identification means features to be assessed
The identification service assessment required in section 29 of the Identification and Trust Services Act must cover all of the requirements specified in the Act and in this regulation, which pertain to:
1) certain properties of the functions affecting the provision of the identification service (the identification scheme), namely:
c) facilities and […]

ITSA, section 8: Requirements posed on the electronic identification scheme
4) The identification scheme is reliable and safe so that [...] the premises used for providing an identification service are safe in compliance with the provisions laid down in section 2.4.5 of the Annex to the Act on Level of Assurance in Electronic Identification.

NO.	LEVEL OF ASSURANCE	REQUIREMENT PERTAINING TO THE IDENTIFICATION SERVICE (SUMMARY)	PROVISIONS	STANDARD REFERENCE	NOTES
64.	S, H	**Security of physical premises** Facilities of the identification scheme are divided into security zones based on the confidentiality and criticality of the information that is processed.	**LoA Annex, section 2.4.5: Facilities and staff** 3. Facilities used for providing the service are continuously monitored for, and protected against, damage caused by environmental events, unauthorised access and other factors that may impact the security of the service. 4. Facilities used for providing the service shall ensure access to areas holding or processing personal, cryptographic or other sensitive information is limited to authorised staff or subcontractors.	A.11.1 Secure physical and environmental areas / Security perimeters: A.11.1.1 Physical security perimeter	All facilities related to or affecting the production of the identification services, including subcontractors. By default, KATAKRI compliance is sufficient, if the identification service is produced in said facilities. The scope of other standards has not been established.
65.	S, H	The hardware used to produce the identification service **is protected** against break-ins, vandalism, fire, heat, gas, dust, vibration, water and power outages. Security perimeters are taken into account in the security classification.	**LoA Annex, section 2.4.5: Facilities and staff** 3. Facilities used for providing the service are continuously monitored for, and protected against, damage caused by environmental events, unauthorised access and other factors that may impact the security of the service. 4. Facilities used for providing the service shall ensure access to areas holding or processing	A.11.1.2 Physical entry controls A.11.1.3 Securing offices, rooms and facilities	

		All facilities have appropriate **access controls** in place that ensure that entry is possible only for relevant persons. Security systems and equipment for the physical protection of information meet universally applied technical standards or minimum requirements.	personal, cryptographic or other sensitive information is limited to authorised staff or subcontractors.	A.11.1.4 Protecting against external and environmental threats A.11.2.1 Equipment siting and protection A.11.2.3 Cabling security	
66.	S, H	Security perimeters are used to ensure that no **unauthorised** equipment or connections are used.	**LoA Annex, section 2.4.5: Facilities and staff** 3. Facilities used for providing the service are continuously monitored for, and protected against, damage caused by environmental events, unauthorised access and other factors that may impact the security of the service. 4. Facilities used for providing the service shall ensure access to areas holding or processing personal, cryptographic or other sensitive information is limited to authorised staff or subcontractors.	A.11 Physical and environmental security	

B 7 Sufficiency and competence of human resources

KEY PROVISIONS

M72B, section 15.1: Identification scheme and identification means features to be assessed
The identification service assessment required in section 29 of the Identification and Trust Services Act must cover all of the requirements specified in the Act and in this regulation, which pertain to:
1) certain properties of the functions affecting the provision of the identification service (the identification scheme), namely:
c) […] and staff

NO.	LEVEL OF ASSURANCE	REQUIREMENT PERTAINING TO THE IDENTIFICATION SERVICE (SUMMARY)	PROVISIONS	STANDARD REFERENCE	NOTES

67.	S, H	**Availability and competence of staff** The production organisation of the identification service must have sufficient expertise and human resources available to ensure information security and privacy.	**ITSA, section 13: General obligations of an identification service provider** […] the personnel and subcontracted services used by an identification service provider in association with identification shall, at a minimum, meet the requirements laid down for assurance level substantial in sections … 2.4.5 of the Annex to the Act on Level of Assurance in Electronic Identification. **LoA Annex, section 2.4.5: Facilities and staff** Requirements concerning the facilities, personnel and (if applicable) subcontractors who carry out tasks related to the scope of application of this regulation. The requirements must be commensurate with the risk related to the level of assurance that is provided. 1. The existence of procedures that ensure that staff and subcontractors are sufficiently trained, qualified and experienced in the skills needed to execute the roles they fulfil. 2. The existence of sufficient staff and subcontractors to adequately operate and resource the service according to its policies and procedures.	A.7.2.2 Human resource security / During employment: Information security awareness, education and training	Assessment - sufficiency of human resources considering the nature of the operations (24/7/365) - assessment of technical controls; no precise requirements for the number of employees or on-call availability - expertise in the required competence areas such as technical and legal competence (due to the processing of personal information).
68.	S, H	Subcontracted services used in the identification scheme are identified and documented. The competence and availability of the subcontractors' personnel resources is ensured.	**See previous row.**	See previous row. A.15.1.1 Information security policy for supplier relationships A.15.2.1 Monitoring and review of supplier services	Information on subcontractors of the identification scheme (office systems, operator services, software applications, infrastructure...) and assessment of their human resources at least on a general level.

B 8 Information security management

KEY PROVISIONS

M72B, section 15.1: Identification scheme and identification means features to be assessed
The identification service assessment required in section 29 of the Identification and Trust Services Act must cover all of the requirements specified in the Act and in this regulation, which pertain to:

1) certain properties of the functions affecting the provision of the identification service (the identification scheme), namely:
    a) information security management

M72B, section 4: Information security management system of the identification service provider
4.1 Information security management standard
The identification service provider must comply with the ISO/IEC 27001 standard or another corresponding, well-known information security management standard in the management of the information security of its identification scheme. Information security management may also be based on the combination of several standards.

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

1) overall context of the identification service provider;
2) governance, organisation and maintenance of information security management;
3) management of information security risks related to the provision of the identification service;
4) resources allocated to information security, competences, staff awareness of information security, communication, documentation and the management of documented information;
5) planning and steering of the provision of the identification service for the purpose of meeting information security requirements; and
6) evaluation of the efficiency and functionality of information security management.

ITSA, section 8: Requirements posed on the electronic identification scheme
An electronic identification scheme must fulfil the following requirements:

5) Information security management is ensured so that, at a minimum, the conditions for assurance level substantial laid down in the introduction to section 2.4 and in sections 2.4.3 and 2.4.7 of the Annex to the Act on Level of Assurance in Electronic Identification are met.

LoA Annex, section 2.4: Management and organisation
All participants providing a service related to electronic identification in a cross-border context ("providers") shall have in place documented information security management practices, policies, approaches to risk management, and other recognised controls so as to provide assurance to the appropriate governance bodies for the electronic identification schemes in the respective Member States that effective practices are in place. Throughout section 2.4, all requirements/elements shall be understood as commensurate to the risks at the given level.

LoA Annex, section 1: Applicable definitions

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

LoA Annex, section 2.4.7: Compliance and audit Substantial: The existence of periodical independent internal or external audits scoped to include all parts relevant to the supply of the provided services to ensure compliance with relevant policy.					
NO.	**LEVEL OF ASSURANCE**	**REQUIREMENT PERTAINING TO THE IDENTIFICATION SERVICE (SUMMARY)**	**PROVISIONS**	**STANDARD REFERENCE**	**NOTES**
69.	S, H	The provider of the identification service has an efficient **information security management system** (including organisational and technical measures) in place for the management and monitoring of information security risks related to the operation of the identification service.	**LoA Annex, section 2.4.3: Information security management** There is an effective information security management system for the management and control of information security risks. Substantial: The information security management system adheres to proven standards or principles for the management and control of information security risks.	5 Leadership A.5 Policies for information security	ISO 27001 compliance without substantial deviations is considered proof of meeting the information security management requirements.
70.	S, H	The information security management system is based on a universally applied standard or set of standards.	**M72B, section 4: Information security management system of the identification service provider** **4.1 Information security management standard** The identification service provider must comply with the ISO/IEC 27001 standard or another corresponding, well-known information security management standard in the management of the information security of its identification scheme. Information security management may also be based on the combination of several standards. **LoA Annex, section 2.4.3: Information security management** Substantial: The information security management system adheres to proven standards or principles for the management and control of information security risks.		

71.	S, H	The information security management system covers all substantial internal and external technical, legal and administrative requirements and needs with impacts on the identification scheme.	**M72B, section 4.2: Information security management scope** Information security management shall cover the following aspects concerning the provision of identification service: 1) overall context of the identification service provider; 2) governance, organisation and maintenance of information security management; […]	4 Context of the organisation	The identification service must follow current legislation and regulations, such as the Identification and Trust Services Act, Regulation 72 and the General Data Protection Regulation.
72.	S, H	The information security management system covers the management, organisation and maintenance of the management procedures. An up to date **information security policy** approved by the management of the organisation is in place. Security principles and policies are sufficiently extensive and appropriate for the organisation and the items to be protected. Information security responsibilities of the staff and the subcontractors are defined.	**M72B, section 4.2: Information security management scope** Information security management shall cover the following aspects concerning the provision of identification service: […] 2) governance, organisation and maintenance of information security management; […] 4) resources allocated to information security, competences, staff awareness of information security, communication, documentation and the management of documented information; […]	5 Leadership 9.2 Internal audit 9.3 Management review 10 Improvement A.5.1.1 Policies for information security A.6.1.1 Information security roles and responsibilities A.15.1.1 Information security policy for supplier relationships	
73.	S, H	The information security management system covers the management of information security risks related to the offering of the identification service.	**M72B, section 4.2: Information security management scope** Information security management shall cover the following aspects concerning the provision of identification service: […]	6 Planning 8 Operation	

		Risk management is a regular, continuous and documented process. The risks that are identified are classified and prioritised. The risk management process is able to detect risks to the confidentiality, integrity and availability of information. The risk management process and its results are employed in designing the security measures of the identification service/identification scheme.	3) management of information security risks related to the provision of the identification service; […]		
74.	S, H	The information security management system covers the resources allocated to information security, competence requirements, staff awareness of information security, communication, documentation and the management of documented information. Up to date information security guidelines and policies are available to everyone working with tasks related to electronic identification. Information security training given to the staff is regular and documented. Efficiency of the training is monitored.	**M72B, section 4.2: Information security management scope** Information security management shall cover the following aspects concerning the provision of identification service: […] 4) resources allocated to information security, competences, staff awareness of information security, communication, documentation and the management of documented information; […]	7 Support	
75.	S, H	The information security management system ensures that the offering of the	**M72B, section 4.2: Information security management scope**	8 Operation	Regulatory requirements for identification services

		identification service is planned and managed in such a way that the information security requirements set for identification services are met.	Information security management shall cover the following aspects concerning the provision of identification service: […] 5) planning and steering of the provision of the identification service for the purpose of meeting information security requirements; and […]	A.18.1.1 Compliance / Compliance with legal and contractual requirements: Identification of applicable legislation and contractual requirements	Data protection regulation (as applicable) Contractual trust network provisions (as applicable)
76.	S, H	The information security management system features regular assessment of information security efficiency and functionality.	**M72B, section 4.2: Information security management scope** Information security management shall cover the following aspects concerning the provision of identification service: […] 6) evaluation of the efficiency and functionality of information security management.	9.1 Monitoring, measurement, analysis and evaluation	How effective the information security management is concerning the factors, processes and problems that affect the information security of the identification scheme.

B 9 Identity proofing and verification of the applicant of identification means (initial identification)

KEY PROVISIONS

M72B, section 15.1: Identification scheme and identification means features to be assessed
The identification service assessment required in section 29 of the Identification and Trust Services Act must cover all of the requirements specified in the Act and in this regulation, which pertain to:
[…]
2) the identification method, meaning certain properties of the identification means, namely:
b) identity proofing and verification of the applicant

ITSA, section 8: Requirements posed on the electronic identification scheme
An electronic identification scheme must fulfil the following requirements:
1) The identification means shall be based on initial identification according to section 17 and section 17 a, where the relevant data can be verified afterwards as set out in section 24;
2) The identification means can be used for unambiguously identifying the holder of the identification means in a way that, at a minimum, fulfils the requirements on assurance level substantial laid down in sections 2.1.2, 2.1.3 and 2.1.4 of the Annex to the 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, hereinafter the Act on Level of Assurance in Electronic Identification.

[…]

ITSA, section 17: Identifying a natural person applying for an identification means
The initial identification of a natural person shall be made personally or electronically in a way that fulfils the requirements for assurance level substantial or high laid down in section 2.1.2 of the Annex of the Act on Level of Assurance in Electronic Identification. The proofing of a person's identity may be based on a document issued by an authority showing the person's identity or a strong electronic identification means referred to in this Act. In addition, the proofing of an identity may be based on a procedure used at an earlier date by a public or private entity for a purpose other than the issuing of a strong electronic identification means, which the Finnish Transport and Communications Agency approves pursuant to regulations and regulatory control on the procedure, or pursuant to a confirmation by a conformity assessment body referred to in section 28, subsection 1.

In initial identification that is solely based on a document issued by an authority showing the person's identity, the only acceptable documents are a valid passport or a personal identity card issued by an authority of a member state of the European Economic Area, Switzerland or San Marino. If the identification means provider so desires, they may also verify the identity from a valid passport granted by an authority of another state.

If the identity of an applicant cannot be reliably established, the police will perform the initial identification for the application. […]

LoA Annex, section 2.1.2: Identity proofing and verification (natural person)
LoA Annex, section 2.1.3: Identity proofing and verification (legal person)
LoA Annex, section 2.1.4: Binding between the electronic identification means and legal persons

LEGAL PERSON
Requirements for granting of identification means to legal persons are not discussed in more detail in these criteria. In cases of an identification service provider offering strong identification means to legal persons, the assessment must take the applicable provisions into account.

ITSA, section 17 a: Identifying a legal person applying for an identification means
The reported identity of a legal person must be verified from the Business Information Register or by means that, at a minimum, meet the requirements laid down for the identity proofing and verifying of a legal person at assurance level substantial laid down in section 2.1.3 of the Annex to the Act on Level of Assurance in Electronic Identification.

ITSA, section 7 a: Using the data in the Business Information System
The provider of an identification means and a certification service provider offering a trust service must use the Business Information System to obtain and update the data they need in order to be able to offer a service for identifying a legal person. The identification service provider shall also ensure that the data it needs for the pur-pose of offering identification services are up-to-date with the data in the Business Information System.

DEFINITIONS

ITSA, section 2: Definitions
7) initial identification means the verification of the identity of the applicant for an identification means in connection with the issuing of the means;

LoA Annex, section 1: Applicable definitions
1) 'authoritative source' means any source irrespective of its form that can be relied upon to provide accurate data, information and/or evidence that can be used to prove identity.

Standard: ETSI TS 119 461

NO.	LEVEL OF ASSURANCE	REQUIREMENT PERTAINING TO THE IDENTIFICATION SERVICE (SUMMARY)	PROVISIONS	STANDARD REFERENCE	NOTES
Method 1: Initial identification is based on the presentation of an identity document approved in Finland					
77.	S, H	Identify proofing is based on approved identity documents defined in the Identification Act. The acceptance of identity documents issued by countries other than those listed in the Act is clearly defined.	**ITSA, section 17: Identifying a natural person applying for an identification means** […] In initial identification that is solely based on a document issued by an authority showing the person's identity, the only acceptable documents are a valid passport or a personal identity card issued by an authority of a member state of the European Economic Area, Switzerland or San Marino. If the identification means provider so desires, they may also verify the identity from a valid passport granted by an authority of another state. […]		If the initial identification is based on identity documents.
78.	S, H	The identity document is presented, and its validity is ensured **on the spot**. The staff are familiar with the authenticity factors of the identification documents and have the ability to verify them.	**ITSA, section 17: Identifying a natural person applying for an identification means** The initial identification of a natural person shall be made personally or electronically in a way that fulfils the requirements for assurance level substantial or high laid down in section 2.1.2 of the Annex of the Act on Level of Assurance in Electronic Identification. The proofing of a person's identity may be based on a document issued by an authority showing the person's identity or a strong		In case a remote identification solution is used, see the criteria in section Method 5.

		It is ensured that the identity document belongs to the person presenting the document.	electronic identification means referred to in this Act. […] **LoA Annex, section 2.1.2: Identity proofing and verification (natural person)** Substantial: 1. The person has been verified to be in possession of evidence recognised by the Member State in which the application for the electronic identity means is being made and representing the claimed identity and the evidence is checked to determine that it is genuine; or, according to an authoritative source, it is known to exist and relates to a real person and steps have been taken to minimise the risk that the person's identity is not the claimed identity, taking into account for instance the risk of lost, stolen, suspended, revoked or expired evidence; or 2. An identity document is presented during a registration process in the Member State where the document was issued and the document appears to relate to the person presenting it and steps have been taken to minimise the risk that the person's identity is not the claimed identity, taking into account for instance the risk of lost, stolen, suspended, revoked or expired evidence;		
79.	S	The identity document is presented, and its validity is ensured **using a remote connection.** The staff are familiar with the authenticity factors of the	**ITSA, section 17: Identifying a natural person applying for an identification means** The initial identification of a natural person shall be made personally or electronically in a way that fulfils the requirements for assurance level substantial or high laid down in section 2.1.2 of the Annex of the Act on Level of Assurance in Electronic Identification. The proofing of a person's identity		See section 3.9 of this document.

		identification documents and have the ability to verify them. It is ensured that the identity document belongs to the person presenting the document. Reliability requirements for the remote connection take substantial-level attack potentials into account.	may be based on a document issued by an authority showing the person's identity or a strong electronic identification means referred to in this Act. […] **LoA Annex, section 2.1.2: Identity proofing and verification (natural person)** Substantial: 1. The person has been verified to be in possession of evidence recognised by the Member State in which the application for the electronic identity means is being made and representing the claimed identity and the evidence is checked to determine that it is genuine; or, according to an authoritative source, it is known to exist and relates to a real person and steps have been taken to minimise the risk that the person's identity is not the claimed identity, taking into account for instance the risk of lost, stolen, suspended, revoked or expired evidence; or 2. An identity document is presented during a registration process in the Member State where the document was issued and the document appears to relate to the person presenting it and steps have been taken to minimise the risk that the person's identity is not the claimed identity, taking into account for instance the risk of lost, stolen, suspended, revoked or expired evidence;		
80.	H	The identity document is presented, and its validity is ensured using a remote connection.	**LoA Annex, section 2.1.2: Identity proofing and verification (natural person)** High: 1.a) Where the person has been verified to be in possession of photo or biometric identification evidence recognised by the Member State in which		See section 3.9 of this document.

		The authenticity of the identification document is verified based on an electronic signature read from a chip on the identification document. It is ensured that the identity document belongs to the person presenting the document by comparing the physical properties of the person to the electronically signed comparison data read from the identity document. Reliability requirements for the remote connection take high-level attack potentials into account.	the application for the electronic identity means is being made and that evidence represents the claimed identity, the evidence is checked to determine that it is valid according to an authoritative source; and the applicant is identified as the claimed identity through comparison of one or more physical characteristics of the person with an authoritative source;		
81.	S, H	The validity of the passport or the identity card is verified using the available police information systems or reliable international authorities.	**LoA Annex, section 2.1.2: Identity proofing and verification (natural person)** *Procedures 1 and 2, partial requirements:* steps have been taken to minimise the risk that the person's identity is not the claimed identity, taking into account for instance the risk of lost, stolen, suspended, revoked or expired evidence; **ITSA, section 7 b: Information on the validity of a passport or a personal identity card** An identification service provider has the right to obtain via an interface or other electronic means and without prejudice to secrecy provisions information from the information system of the police about the validity of a passport or a personal identity card used for initial identification.		Not a requirement but has an impact on risk assessment and may have an impact on liabilities. On the high level of assurance this requirement is mandatory.
82.	S, H	The existence of the person is verified from the population information system.	**ITSA, section 7: Use of data stored in the Population Information System** The provider of an identification means and a certification service provider offering a trust service		Applies to all initial identification procedures.

			must use the Population Information System to obtain and update the data they need in order to be able to offer a service for identifying a natural person. The identification service provider shall also ensure that the data it needs for the purpose of offering identification services are up-to-date with the data in the Population Information System. […]		
Method 2: Initial identification using an electronic identification means					
83.	S	Identity proofing is based on strong electronic identification means approved in the Identification Act.	**ITSA, section 17: Identifying a natural person applying for an identification means** The initial identification of a natural person shall be made personally or electronically in a way that fulfils the requirements for assurance level substantial or high laid down in section 2.1.2 of the Annex of the Act on Level of Assurance in Electronic Identification. The proofing of a person's identity may be based on a document issued by an authority showing the person's identity or a strong electronic identification means referred to in this Act. […] **LoA Annex, section 2.1.2: Identity proofing and verification (natural person)** Substantial: 4. Where electronic identification means are issued on the basis of a valid notified electronic identification means having the assurance level substantial or high, and taking into account the risks of a change in the person identification data, it is not required to repeat the identity proofing and verification processes. Where the electronic identification means serving as the basis has not been notified, the assurance level substantial or high must be confirmed by a conformity assessment body referred to in Article 2(13) of Regulation (EC) No 765/2008 or by an equivalent body.		If initial identification based on strong electronic identification is used. Identification means used for the substantial level of assurance are registered in Traficom's register as required by the Identification Act.

84.	H	Identity proofing is based on strong electronic identification means approved in the Identification Act. Issuing identification means used for a high level of assurance on the basis of electronic identification is only possible for identification means with a high assurance level.	**LoA Annex, section 2.1.2: Identity proofing and verification (natural person)** High: 3. Where electronic identification means are issued on the basis of a valid notified electronic identification means having the assurance level high, it is not required to repeat the identity proofing and verification processes. Where the electronic identification means serving as the basis has not been notified, the assurance level high must be confirmed by a conformity assessment body referred to in Article 2(13) of Regulation (EC) No 765/2008 or by an equivalent body. and steps are taken that the results of this previous issuance procedure of a notified electronic identification means remain valid.		If initial identification based on strong electronic identification is used. Identification means used for the high level of assurance are registered in Traficom's register as required by the Identification Act.
Method 3: Initial identification based on identification made for other purpose ("prior customer relationship")					
85.	S, H	Identify proofing relies on a procedure where an identity has been proven and verified earlier for purposes other than issuing an electronic identification means. The procedure can be based on regulations other than the Identification Act or eIDAS regulation and is supervised by an authority. The procedure offers assurance similar to the procedure based on the presentation of an identity document or identification using electronic means of identification.	**ITSA, section 17: Identifying a natural person applying for an identification means** The initial identification of a natural person shall be made personally or electronically in a way that fulfils the requirements for assurance level substantial or high laid down in section 2.1.2 of the Annex of the Act on Level of Assurance in Electronic Identification. The proofing of a person's identity may be based on a document issued by an authority showing the person's identity or a strong electronic identification means referred to in this Act. In addition, the proofing of an identity may be based on a procedure used at an earlier date by a public or private entity for a purpose other than the issuing of a strong electronic identification means, which the Finnish Transport and Communications Agency approves pursuant to regulations and regulatory control on the procedure, or pursuant to a confirmation by a conformity assessment body referred to in section 28, subsection 1. […]		The use of such an initial identification procedure is subject to express approval from the Finnish Transport and Communications Agency. Notification of such a procedure must be accompanied by a conformity assessment. For example, the use of a qualified electronic signature or an advanced electronic signature accompanied by a qualified certificate issued for the electronic signature, may come into question as a part of the initial identification process.

			LoA Annex, section 2.1.2: Identity proofing and verification (natural person) Substantial: 3. Where procedures used previously by a public or private entity in the same Member State for a purpose other than the issuance of electronic identification means provide for an equivalent assurance to those set out in section 2.1.2 for the assurance level substantial, then the entity responsible for registration need not to repeat those earlier procedures, provided that such equivalent assurance is confirmed by a conformity assessment body referred to in Article 2(13) of Regulation (EC) No 765/2008 of the European Parliament and of the Council or by an equivalent body;		When handing over the new identification means, it must be ensured by other means that the identification means is handed over to the right person.
Method 4: Initial identification by the police					
86.	S, H	If required, an initial identification should be performed by police.	**ITSA, section 17: Identifying a natural person applying for an identification means** […] If the identity of an applicant cannot be reliably established, the police will perform the initial identification for the application. […] **LoA Annex, section 2.1.2: Identity proofing and verification (natural person)** High: 2. Where the applicant does not present any recognised photo or biometric identification evidence, the very same procedures used at the national level of the Member State of the entity responsible for the registration to obtain such recognised photo or biometric identification evidence are applied.		
Method 5: Remote initial identification					

87.	S	The remote initial identification solution must be based on a risk assessment (Level of Identity Proofing, LoIP).	**ITSA, section 8: Requirements posed on the electronic identification scheme** […] 4) The identification scheme is reliable and safe so that, at a minimum, it meets the conditions for assurance level substantial laid down in sections 2.2.1, 2.3.1 and 2.4.6 of the Annex to the Act on Level of Assurance in Electronic Identification and takes into account the threats to the information security of the technology available at the time, and that the premises used for providing an identification service are safe in compliance with the provisions laid down in section 2.4.5 of the Annex to the Act on Level of Assurance in Electronic Identification. 5) Information security management is ensured so that, at a minimum, the conditions for assurance level substantial laid down in the introduction to section 2.4 and in sections 2.4.3 and 2.4.7 of the Annex to the Act on Level of Assurance in Electronic Identification are met. […] **M72B, section 6.1: Identification means characteristics and its resistance** 6.1.1 The authentication factors, authentication mechanism and security measures of the identification means must be planned, executed and maintained so that they protect the integrity and confidentiality of the identification means. The identification means must be able to resist at least moderate or high-level threats and attack potential specified in section 2.3 of the appendix to the *regulation on Level of Assurance in Electronic Identification* in accordance with the assurance level of the identification service. The resistance must be based on a risk assessment including specific assessments of threats directed at an authentication mechanism and authentication	ETSI TS 119 461 ISO/IEC TS 29003:2018	Attack potential (substantial/high) and its calculation, defined criteria that must be met to complete the issuing process, supply chain security if a service provider is used, is it based on the examination of a photo (selfie) or video material, criteria for moving from an automatic process to a manual process.

			factors based on possession, knowledge and inherence as well as assessment of security measures in place to protect against these threats. **LoA Annex, section 2.4.3: Information security management** Low: There is an effective information security management system for the management and control of information security risks. Substantial: The information security management system adheres to proven standards or principles for the management and control of information security risks.		
88.	S	Informing the customer of terms and conditions	**ITSA, section 20: Issuing an identification means** The issuance of an identification means is based on the agreement between the applicant for the identification means and the identification service provider. The agreement must be in writing. The agreement can be in electronic format, provided that its content cannot be changed unilaterally and that it remains available to the parties. The identification service provider shall treat its customers in a non-discriminatory way and the identification means applicants fairly when entering into the agreement. […] **ITSA, section 23: Obligations of the identification means holder** The identification means holder shall use the means according to the terms and conditions of the agreement. The holder shall store the identification means with care. The holder's duty of care for the identification means starts with its acceptance. The identification means holder shall not make the use of the means available to any other person.		

			LoA 2.1.1. Application and registration 1. Ensure the applicant is aware of the terms and conditions related to the use of the electronic identification means. 2. Ensure the applicant is aware of recommended security precautions related to the electronic identification means. […]		
89.	S	Approved initial identification documents and checking their validity.	**ITSA, section 17: Identifying a natural person applying for an identification means** […] In initial identification that is solely based on a document issued by an authority showing the person's identity, the only acceptable documents are a valid passport or a personal identity card issued by an authority of a member state of the European Economic Area, Switzerland or San Marino. If the identification means provider so desires, they may also verify the identity from a valid passport granted by an authority of another state. […] **ITSA, section 7 b: Information on the validity of a passport or a personal identity card** An identification service provider has the right to obtain via an interface or other electronic means and without prejudice to secrecy provisions information from the information system of the police about the validity of a passport or a personal identity card used for initial identification. **LoA section 2.1.2: Identity proofing and verification (natural person)** Low: 1. The person can reasonably be assumed to be in possession of evidence recognised by the Member State in which the application for the electronic identity means is being made and representing the claimed identity.		In practice, this currently applies to passports, possibly also to identity cards. The validity of the initial identification document must be checked against the interface of the Police or other internationally trusted interface (Interpol).

			2. The evidence can be assumed to be genuine, or to exist according to an authoritative source, and the evidence appears to be valid. 3. It is known by an authoritative source that the claimed identity exists and it may be assumed that the person claiming the identity is one and the same. Substantial: Level Low, plus one of the alternatives listed under level Substantial, e.g. 1. The person has been verified to be in possession of evidence recognised by the Member State in which the application for the electronic identity means is being made and representing the claimed identity and the evidence is checked to determine that it is genuine; or, according to an authoritative source, it is known to exist and relates to a real person and steps have been taken to minimise the risk that the person's identity is not the claimed identity, taking into account for instance the risk of lost, stolen, suspended, revoked or expired evidence;		
90.	S	The existence of the person is verified from the population information system.	**ITSA, section 7: Use of data stored in the Population Information System** The provider of an identification means and a certification service provider offering a trust service must use the Population Information System to obtain and update the data they need in order to be able to offer a service for identifying a natural person. The identification service provider shall also ensure that the data it needs for the purpose of offering identification services are up-to-date with the data in the Population Information System. […]		Applies to all initial identification procedures.

			LoA section 2.1.2: Identity proofing and verification (natural person) Low: 3. It is known by an authoritative source that the claimed identity exists and it may be assumed that the person claiming the identity is one and the same.		
91.	S	The application and external solutions or components carrying out remote initial identification must be assessed.	**ITSA, section 29: Conformity assessment of an electronic identification service** An identification service provider must regularly subject their service to an assessment by an assessment body referred to in section 28 to determine whether the identification service meets the requirements on interoperability, information security, data protection and other reliability laid down in this Act. […] **M72B, section 4.2: Information security management scope** Information security management shall cover the following aspects concerning the provision of identification service: 1) overall context of the identification service provider; 2) governance, organisation and maintenance of information security management; 3) management of information security risks related to the provision of the identification service; 4) resources allocated to information security, competences, staff awareness of information security, communication, documentation and the management of documented information; 5) planning and steering of the provision of the identification service for the purpose of meeting information security requirements; and	ETSI TS 119 461 ISO/IEC TS 29003:2018 ISO/IEC 30107	Assessment by an assessment body, FAR value, on which data the FAR is based, correspondence to attack potential (substantial/high). PAD ability (Presentation Attack Detection). FRR not essential. The application must also be assessed or its security otherwise verified with a procedure in accordance with Annex C or similar

			6) evaluation of the efficiency and functionality of information security management. **M72B, section 15: Conformity assessment criteria** **15.1 Identification scheme and identification means features to be assessed** The identification service assessment required in section 29 of the Identification and Trust Services Act must cover all of the requirements specified in the Act and in this regulation, which pertain to: 1) certain properties of the functions affecting the provision of the identification service (the identification scheme), namely: a) information security management; b) record keeping and data processing; c) facilities and staff; d) technical measures (controls); and […] 2) the identification means, meaning certain properties of the identification means, namely: a) application and registration; b) identity proofing and verification of the applicant; c) […] d) issuance, delivery and activation; e) suspension, revocation and reactivation; f) renewal and replacement; and g) authentication mechanisms. **LoA section 2.1.2: Identity proofing and verification (natural person)** Substantial: 1. The person has been verified to be in possession of evidence recognised by the Member State in which the application for the electronic identity		

			means is being made and representing the claimed identity and the evidence is checked to determine that it is genuine; or, according to an authoritative source, it is known to exist and relates to a real person and steps have been taken to minimise the risk that the person's identity is not the claimed identity, taking into account for instance the risk of lost, stolen, suspended, revoked or expired evidence;		
92.	S	The authenticity of the presented document and the unaltered nature of the data is verified. Active and passive authentication of the document used for initial identification, document examination across video link (MRZ, visual security features)	**LoA Annex, section 2.1.2: Identity proofing and verification (natural person)** Low: 2. The evidence can be assumed to be genuine, or to exist according to an authoritative source, and the evidence appears to be valid. Substantial: 1. […] the evidence is checked to determine that it is genuine; or, according to an authoritative source, it is known to exist and relates to a real person […]		The authenticity of the initial identification document (passport, identity card) and of the data stored on the chip must be verified.
93.	S	The remote identification event and person verification via video link is carried out in conditions for which minimum requirements are defined.	**LoA Annex, section 2.1.2: Identity proofing and verification (natural person)** Substantial: 1. The person has been verified to be in possession of evidence recognised by the Member State in which the application for the electronic identity means is being made and representing the claimed identity and the evidence is checked to determine that it is genuine; or, according to an authoritative source, it is known to exist and relates to a real person and steps have been taken to minimise the risk that the person's identity is not the claimed identity, taking		The remote initial identification event is carried out in a situation or conditions where the realisation of automatic security controls can be maximised.

			into account for instance the risk of lost, stolen, suspended, revoked or expired evidence;		
94.	S	The automatic security controls analysing the biometrics in remote initial identification are random or are based on methods that can be used to demonstrate compliance with the requirements of the regulation on Level of Assurance in Electronic Identification	**LoA Annex, section 2.1.2: Identity proofing and verification (natural person)** Low: 3. It is known by an authoritative source that the claimed identity exists and it may be assumed that the person claiming the identity is one and the same. Substantial: 1. The person has been verified to be in possession of evidence recognised by the Member State in which the application for the electronic identity means is being made and representing the claimed identity and the evidence is checked to determine that it is genuine; or, according to an authoritative source, it is known to exist and relates to a real person and steps have been taken to minimise the risk that the person's identity is not the claimed identity, taking into account for instance the risk of lost, stolen, suspended, revoked or expired evidence;		The aim is to prevent e.g. the creation of prepared video feeds. The detection of vitality by different automated means, for example, from either video material or the detection of bio-signals from a facial image.
95.	S	Technical minimum requirements are defined for a remote initial identification event; unless they are met, the remote initial identification cannot be carried out	**LoA Annex, section 2.1.2: Identity proofing and verification (natural person)** Low: 3. It is known by an authoritative source that the claimed identity exists and it may be assumed that the person claiming the identity is one and the same. Substantial: […] and the evidence is checked to determine that it is genuine; or, according to an authoritative source, it is known to exist and relates to a real person and		E.g. minimum requirements for hardware levels, smoothness and speed of data communication connections, resolution, camera abilities, appearance of artefacts, Annex C resilience criteria.

			steps have been taken to minimise the risk that the person's identity is not the claimed identity, taking into account for instance the risk of lost, stolen, suspended, revoked or expired evidence;		
96.	S	Data transfer, storage	**LoA Annex, section 2.4.4: Record keeping** 1. Record and maintain relevant information using an effective record-management system, taking into account the applicable legislation and good practice in relation to data protection and data retention. 2. Retain, as far as it is permitted by national law or other national administrative arrangement, and protect records for as long as they are required for the purpose of auditing and investigation of security breaches, and retention, after which the records shall be securely destroyed. **also M72B, section 7: Identification scheme interface encryption requirements**		Data protection, especially if data is transferred outside the EU. Saving for later examination e.g. in case of detected misuse.
97.	S	The software component carrying out remote initial identification must be authenticated.	**ITSA, section 13: General obligations of an identification service provider** […] The identification service provider is responsible for the reliability and functionality of services and products provided by persons contributing to the identification service process. **LoA Annex, section 2.4.6: Technical controls** 1. The existence of proportionate technical controls to manage the risks posed to the security of the services, protecting the confidentiality, integrity and availability of the information processed. 2. Electronic communication channels used to exchange personal or sensitive information are protected against eavesdropping, manipulation and replay. […] **M72B, section 15: Conformity assessment criteria**		In practice, a mobile application and the application attestation to the back-end system.

			15.1 Identification scheme and identification means features to be assessed The identification service assessment required in section 29 of the Identification and Trust Services Act must cover all of the requirements specified in the Act and in this regulation, which pertain to: 1) certain properties of the functions affecting the provision of the identification service (the identification scheme), namely: a) information security management;		
98.	S	Remote identification must be based at least in part on automated processes.	**LoA Annex, section 2.4.6: Technical controls** 4. Procedures exist to ensure that security is maintained over time and that there is an ability to respond to changes in risk levels, incidents and security breaches.		Using only an official for remote initial identification is not sufficient, but the process must be based at least in part on computerised comparison of the above-mentioned criteria.
99.	S	Staff participating in the remote identification process must be trained.	**LoA Annex, section 2.4.5: Facilities and staff** 1. The existence of procedures that ensure that staff and subcontractors are sufficiently trained, qualified and experienced in the skills needed to execute the roles they fulfil. 2. The existence of sufficient staff and subcontractors to adequately operate and resource the service according to its policies and procedures.		If an employee takes part in the decision-making of a remote initial identification process, they must be adequately trained in assessing the authenticity of any video material and initial identification document authenticity factors.

B 10 Lifecycle of identification means

KEY PROVISIONS

M72B, section 15.1: Identification scheme and identification means features to be assessed
The identification service assessment required in section 29 of the Identification and Trust Services Act must cover all of the requirements specified in the Act and in this regulation, which pertain to:
[…]
2) the identification means, meaning certain properties of the identification means, namely:

	a) application and registration; b) […] c) […] d) issuance, delivery and activation; e) suspension, revocation and reactivation; f) renewal and replacement; and g) […].				
NO.	**LEVEL OF ASSURANCE**	**REQUIREMENT PERTAINING TO THE IDENTIFICATION SERVICE (SUMMARY)**	**PROVISIONS**	**STANDARD REFERENCE**	**NOTES**
100.	S, H	The identification is not connected to the person (personalised) before initial identification. The identification means factors are connected to the identification means holder.	**M72B, section 6.3: Connecting identification means to a person** 6.3.1 The authentication factors of the identification means must be bound to the identification means holder in the identification scheme. 6.3.2 An identification means shall not be bound to an applicant before the applicant has passed initial identification or it has been otherwise ensured in the process of granting an identification means that the identification means is not functional before the initial identification referred to in section 17 of the Identification and Trust Services Act has been performed.		
101.	S, H	The personal data of a natural person is checked from the population information system when issuing an identification means and regularly during the validity of the identification means.	**ITSA, section 7: Use of data stored in the Population Information System** The provider of an identification means and a certification service provider offering a trust service must use the Population Information System to obtain and update the data they need in order to be able to offer a service for identifying a natural person. The identification service provider shall also ensure that the data it needs for the purpose of offering identification services are up-to-date with the data in the Population Information System.		The frequency of regular verification has not been defined. Weekly verification is a good established practice. Cf. (no reference in the Identification Act; applied formally only if the procedure is notified) **LoA 2.1.1: Application and registration**

			[…] **See M72B, section 12: Minimum set of data to be relayed in a trust network** **LoA Annex, section 2.1.2: Identity proofing and verification (natural person)** Substantial: 1. The person has been verified to be in possession of evidence recognised by the Member State in which the application for the electronic identity means is being made and representing the claimed identity and the evidence is checked to determine that it is genuine; or, according to an authoritative source, it is known to exist and relates to a real person and steps have been taken to minimise the risk that the person's identity is not the claimed identity, taking into account for instance the risk of lost, stolen, suspended, revoked or expired evidence;		3. Appropriate identification data required for identity proofing is collected.
102.	S, H	**Issuance, delivery and activation of an identification means** An issuance procedure is used to ensure that the identification means does not unlawfully end up in the possession of a third party when the identification means is being released.	**ITSA, section 20: Issuing an identification means** The issuance of an identification means is based on the agreement between the applicant for the identification means and the identification service provider. The agreement must be in writing. The agreement can be in electronic format, provided that its content cannot be changed unilaterally and that it remains available to the parties. […] Cf. (there is no reference to LoA 2.1.1 in the Identification Act; it is therefore applied formally only in case the procedure is notified) **LoA 2.1.1: Application and registration** 1. Ensure the applicant is aware of the terms and conditions related to the use of the electronic identification means.		Contract terms (such as those mentioned in section 15 of the Identification Act) are to be arranged by the service providers and are not within the scope of the audit. The verification requirement specified in section 8 of the ITSA and section 2.2.1 of the LoA that only the holder of a means of identification may use that means is also related to the separate requirement on release in section 21,

			2. Ensure the applicant is aware of recommended security precautions related to the electronic identification means. **ITSA, section 21: Delivering the identification means to the applicant** The identification service provider shall deliver the identification means to the applicant as stated in the agreement. The identification service provider must ensure that when the identification means is handed over, it does not become subject to unauthorised possession. The method for ensuring this must meet, at a minimum, the requirements laid down for assurance level substantial in section 2.2.2 of the Annex of the Act on Level of Assurance in Electronic Identification. **LoA Annex, section 2.2.2: Issuance, delivery and activation** After issuance, the electronic identification means is delivered via a mechanism by which it can be assumed that it is delivered only into the possession of the person to whom it belongs.		according to which the identification service provider must ensure that the identification means does not become subject to unauthorised possession when it is handed over. See LoA Guidance: Possible mechanisms include: - delivery in person - delivery by registered mail - using some activation process, where it can be reasonably assumed that only the subject has the necessary information to activate the means (e.g. a transport-PIN delivered separately from the identification means). For Substantial, multiple authentication factors shall be used. Activation codes are not necessarily required. Several issuance, delivery and activation combinations are possible that meet Substantial: - The delivery of the electronic identification means can be done via regular mail, its activation by sending a code to the bank account of the subject.

					The applicant enters the code to activate the electronic identification means. The assumption here is that bank authentication is of at least level Substantial. - Separate delivery of the electronic identification means and the activation code via regular mail to the verified address of the subject. - Delivery of the electronic identification means via regular mail to the address of the applicant. - The electronic identification means is handed over after having verified the identity of the applicant.
103.	H	**Issuance, delivery and activation of an identification means** An issuance procedure is used to ensure that the identification means does not unlawfully end up in the possession of a third party when the identification means is being released.	**LoA Annex, section 2.2.2: Issuance, delivery and activation** High: The activation process verifies that the electronic identification means was delivered only into the possession of the person to whom it belongs.		The activation process primarily requires the use of an activation code. In particular, it must be ensured that the activation code cannot become available to third parties in the delivery process, and that the activation code is single-use and cannot be used e.g. for reactivation or creating a new PIN code. If the activation is not performed within a certain time, the activation code expires.

					The purpose is to ensure that an unused or a reusable activation code cannot be used to invalidate, i.e. overwrite, the knowledge-based authentication factor (PIN) or activate the identification means without the user's knowledge. There is no reference in the Identification Act to section 2.2.3 of the LoA ("The existence of measures taken to prevent unauthorised suspension, revocation and/or reactivation." However, the one-time use of the code is a good practice, if unauthorized reactivation of the identification means cannot be protected in other ways.
104.	S, H	**Suspension, revocation and reactivation of the identification means** The identification means provider has a revocation service with 24/7 availability available to the users, a revocation list available to the relying parties and the capacity to technically prevent the use of any identification means reported as lost or stolen by the user.	**ITSA, section 25: Cancellation and prevention of use of identification means** The identification means holder shall notify the identification service provider or a designated party if the identification means has been lost, is in the unauthorised possession of another person or of any unauthorised use immediately upon detection of this fact. The identification means provider shall provide an opportunity to submit a notification as set out in subsection 1 at any time. Upon receipt of the notification, the identification service provider		Cf. (there is no reference to LoA 2.2.3 in the Identification Act; it is therefore applied only in case the procedure is notified) **LoA Annex, section 2.2.3: Suspension, revocation and reactivation** 1. It is possible to suspend and/or revoke an electronic identification

			shall immediately cancel the identification means or prevent its use. The identification means provider shall properly and without delay enter in its system the information about the time of cancellation or prevention of use. The holder of the identification means has the right to request proof of submitting a notification mentioned in subsection 1. Such request must be made within 18 months from the notification. The system shall be designed to allow a service provider using an identification service to easily verify the information entered at any time. However, such obligation to create an opportunity to verify information does not exist if the use of the identification means can be prevented or blocked by technical means. […] **Section 26: Identification service provider's right to suspend or revoke the use of an identification means** In addition to the provisions of section 25, the identification service provider may suspend or revoke the use of an identification means if: 1) the identification service provider has reason to believe that someone other than the person to whom the means was issued is using it; 2) the identification means is obviously defective; 3) the identification service provider has reason to believe that the safe use of the means is at risk; 4) the identification means holder is using the identification means contrary to the agreed terms of use; or 5) the identification means holder has died.		means in a timely and efficient manner. 2. The existence of measures taken to prevent unauthorised suspension, revocation and/or reactivation. 3. Reactivation shall take place only if the same assurance requirements as established before the suspension or revocation continue to be met.

			The identification service provider shall notify the holder as soon as possible about the revocation or suspension of use of the identification means, as well as the time of and reasons for such action. The identification service provider shall renew, reactivate or replace the ability to use the identification means or give the identification means holder a new means immediately after removal of reasons referred to in subsection 1(2 and 3). **LoA Annex, section 2.2.3: Suspension, revocation and reactivation** 1. It is possible to suspend and/or revoke an electronic identification means in a timely and efficient manner. 2. The existence of measures taken to prevent unauthorised suspension, revocation and/or reactivation. 3. Reactivation shall take place only if the same assurance requirements as established before the suspension or revocation continue to be met.		
105.	S, H	**Renewal and replacement of an identification means**	**ITSA, section 22: Renewal of the identification means** The identification service provider may provide a new identification means without explicit request to the holder only if a previously delivered identification means needs to be replaced. The renewal of the identification means must follow, at a minimum, the requirements laid down for assurance level substantial in section 2.2.4. **LoA Annex, section 2.2.4: Renewal and replacement** Taking into account the risks of a change in the person identification data, renewal or replacement needs to meet the same assurance requirements as initial identity proofing and verification or be		The verification requirement set out in section 8 of the ITSA and sections 2.2.1 and 2.2.2 of the LoA (the identification means is used only under the control or possession of the person to whom it belongs) must be fulfilled in all situations where some or all authentication factor or activation codes are issued in connection with renewal, replacement or reactivation.

			based on a valid electronic identification means of the same, or higher, assurance level. **LoA Annex, section 2.2.1: Electronic identification means characteristics and design** Substantial: 2. The electronic identification means is designed so that it can be assumed to be used only if under the control or possession of the person to whom it belongs. **LoA Annex, section 2.2.2: Issuance, delivery and activation** Substantial: After issuance, the electronic identification means is delivered via a mechanism by which it can be assumed that it is delivered only into the possession of the person to whom it belongs.		See interpretative comment *Reg. no: Traficom/106/09.02.00/2019 (25.3.2019) Interpretation memorandum of the Finnish Transport and Communications Agency (Traficom) on using a driving licence to verify one's identity when an identification means has been locked or when an identification means or authentication factor is being renewed.* The memorandum is available online at https://www.kyberturvallisuuskeskus.fi/en/electronic-identification
106.	H	**Renewal and replacement of an identification means**	**LoA Annex, section 2.2.4: Renewal and replacement** Low/substantial: Taking into account the risks of a change in the person identification data, renewal or replacement needs to meet the same assurance requirements as initial identity proofing and verification or be based on a valid electronic identification means of the same, or higher, assurance level. High: Where renewal or replacement is based on a valid electronic identification means, the identity data is verified by an authoritative source. **LoA Annex, section 2.2.1: Electronic identification means characteristics and design** High:		The verification requirement set out in section 8 of the ITSA and sections 2.2.1 and 2.2.2 of the LoA (the identification means is used only under the control or possession of the person to whom it belongs) must be fulfilled in all situations where some or all authentication factor or activation codes are issued in connection with renewal, replacement or reactivation.

			2. The electronic identification means is designed so that it can be reliably protected by the person to whom it belongs against use by others. **LoA Annex, section 2.2.2: Issuance, delivery and activation** High: The activation process verifies that the electronic identification means was delivered only into the possession of the person to whom it belongs.		

Assessment guideline for electronic identification services

Traficom Guideline

211/2023 O Annex C Special criteria for mobile identification applications

Annex C: Special criteria for mobile identification applications

General

The mobile application criteria is intended to **complement the general criteria** in case the identification means or identification scheme includes a mobile app.

The criteria is created **primarily for the level of assurance substantial**. References to LoA (Level of Assurance regulation, (EU) 2015/1502) are to the level of assurance substantial, unless otherwise stated. The criteria may be updated in the future to provide more detail on the high level of assurance when experience of its application in Finland is available and when standardised interpretation practices concerning the eIDAS Regulation have been established in Europe.

This document is a guideline. The assessment body must evaluate how well the app corresponds to the criteria provided in this guideline. Risks related to irregularities are assessed as a whole. Operating system and identification app versioning must be monitored and the overall impact of changes to conformity must be assessed. Identification service providers must ensure that the application suppliers provide them adequate and up-to-date information on any changes in hardware and software.

In this context, sensitive data (as referred to in the OWASP criteria) means, for example, personal data, cryptographic materials or confidential/secret information related to identification or registration events.

The guideline is targeted for security evaluation of mobile authentication applications. These applications typically have a strong link to the issuer back-end services. Wallet type of applications with a minimized connections to the back-end can also be evaluated using this guideline.

The App/Wallet label refers to an identification method, i.e. an application running on a terminal device or to a part of an application that performs strong electronic identification.

The criteria is based on the English-language OWASP Mobile AppSec Verification document (OWASP Mobile Application Security Verification Standard, MASVS version 1.4.2), which has been extended and modified for identification purposes.

The testing guide for the original OWASP criteria is available on the OWASP website. The guide contains specific and exhaustive instructions for testing the original OWASP criteria.

Alternative criteria:

- FIDO 3 & 3+ (https://fidoalliance.org/certification/authenticator-certification-levels/)

C 1 Architecture, design and threat modelling

NO.	LEVEL OF ASSURANCE	CRITERION	JUSTIFICATION	ADDITIONAL INFORMATION / COMMENT
400.		All app/wallet components are identified, classified and known to be needed.	LoA, section 2.4.6, point 1 ITSA, section 8.1.4	
401.		Security controls are never enforced only on the client side, but on the respective remote endpoints.	LoA, section 2.4.6, point 1 M72B, subsection 5.3.c	
402.		A high-level architecture for the app/wallet and all connected remote services has been defined and security has been addressed in that architecture.	LoA, section 2.4.6, point 1 ITSA, section 8.1.4	
403.		Data considered sensitive in the context of the app/wallet is clearly identified, classified and protection measures documented.	LoA, section 2.4.4, point 1 LoA, section 2.4.6, points 1 and 3	
404.		All app/wallet components are defined in terms of the business and/or security functions they provide	LoA, section 2.4.6, point 1 ITSA, section 8.1.4	
405.		A threat model for the app/wallet and the associated remote services has been produced that identifies potential threats and countermeasures.	LoA, section 2.3.1, substantial, point 2 LoA, section 2.3.1, high	Attack potentials are assessed as substantial or high.
406.		All security controls have a centralized implementation	LoA, section 2.4.6, point 1	
407.		Local security controls are implemented following industry best practises and validated against this criteria.	LoA, section 2.4.6, point 1 M72B subsection 6.1.1	
408.		There is an explicit policy for how cryptographic keys are managed, and it is based on an internationally approved, up-to-date standard.	LoA, section 2.4.6, point 3 LoA, section 2.4.6, substantial	
409.		The app/wallet reports the operating system, hardware capabilities and application version number to the (application/wallet issuer) server.	LoA, section 2.4.6, point 1 M72B, subsection 5.3.c	
410.		The solution includes a mechanism that ensures that the app is genuine and has not been tampered when presenting authentication/attribute information to a relying party.	LoA 2.3.1, substantial	
411.		The app/wallet does not support/run on mobile operating system versions that are no longer supported/receiving security updates from the operating system vendor.	ITSA section 8.1.4 M72B, subsection 5.4.d LoA, section 2.4.6, point 4	The app/wallet must go through a risk assessment process. If the risk assessment comes to the conclusion that older operating systems, which do not

				receive security updates anymore, are suitable, even unsupported operating systems can be used. This evidence must be incorporated to the audit report.
412.		A mechanism for enforcing update of the app/wallet exists.	ITSA section 8.1.4 M72B, subsection 5.4.d	
413.		An outdated app/wallet prompts the user to update the operating system and/or app/wallet to complete the transaction or when launching the app/wallet instance.	(LoA 2.1.1, point 2)	Best practice (BP). LoA 2.1.1 is not incorporated in the Identification Act.
414.		Security is addressed within all parts of the software development lifecycle.	LoA 2.4.6, sections 1 and 4 ITSA, section 8.1.4	

C 2 Data storage and privacy

In this context, sensitive data (as referred to in the OWASP criteria) means, for example, personal data, cryptographic materials or confidential/secret information related to identification or registration event.

NO.	LEVEL OF ASSURANCE	CRITERION	JUSTIFICATION	ADDITIONAL INFORMATION / COMMENT
415.		Security services and features offered by the platform are used appropriately to store sensitive data.	LoA 2.4.6, section 1, point 3	
416.		The level of authentication currently performed is communicated clearly to the user.	LoA, section 2.1.1, point 2	Recommended practice.
417.		No sensitive data should be stored outside of the app /wallet container or system credential storage facilities.	LoA, section 2.4.6, point 1 M72B, subsection 5.4.b	
418.		No sensitive data is written to application logs.	LoA, section 2.4.6, point 1 M72B, subsection 5.4.b	
419.		No sensitive data is shared with third parties unless it is a necessary part of the architecture.	LoA, section 2.4.6, point 1 M72B, subsection 5.4.b	
420.		The keyboard cache is disabled on text inputs that process sensitive data.	LoA, section 2.4.6, point 1 M72B, subsection 5.4.b	
421.		No sensitive or secret data, such as passwords or pins is exposed through the user interface.	LoA, section 2.4.6, point 1 M72B, subsection 5.4.b	
422.		The clipboard is deactivated on text fields that may contain sensitive data.	LoA, section 2.4.6, point 1 M72B, subsection 5.4.b	
423.		No sensitive data is exposed via IPC mechanisms.	LoA, section 2.4.6, point 1	

			M72B, subsection 5.4.b	
424.		No authentication secrets are stored or transferred outside of the app storage facilities.	LoA 2.4.6, low, section 3 LoA, section 2.4.6, substantial M72B, subsection 5.4.b	
425.		The app/wallet removes sensitive data from views when moved to the background.	LoA, section 2.4.6, point 1 M72B, subsection 5.4.b	
426.		The app/wallet does not hold sensitive data in memory longer than necessary, and memory is cleared explicitly after use.	LoA, section 2.4.6, point 1 M72B, subsection 5.4.b	
427.		The app/wallet recommends enabling a minimum device-access-security policy (PIN code or biometric unlocking mechanism of mobile device and similar features) to the end user.	LoA, section 2.1.1, point 2	Recommended practice.
428.		The app educates the user about best practices the user should follow in processing personally identifiable information.	LoA, section 2.1.1, point 2	Recommended practice.
429.		No sensitive data should be stored locally on the mobile device. Instead, data should be retrieved from a remote end point when needed and only be kept in memory.	LoA, section 2.4.6, point 1 M72B, subsection 5.4.b	
430.		If sensitive data is still required to be stored locally, it must be encrypted using a key derived from hardware backed storage which requires the use of an identification factor(s).	LoA, section 2.4.6, point 1 M72B, subsection 5.4.b	Principle of minimizing the need to store sensitive data. A wallet type application stores sensitive data, hence this criterion should be used for wallet type of applications.
431.		The app/wallet must be deactivated after five failed authentication attempts (of the identification factor).	M72B, subsection 6.1.2	To re-enable the app, normal issuance/activation process must be followed.
432.		If the retry count cannot be communicated to the server side, the app/wallet must have adequate protection in place for the local retry counter.	LoA, section 2.3.1, substantial point 2 M72B subsection 5.3.e-f	

C 3 Cryptography requirements

NO.	LEVEL OF ASSURANCE	CRITERION	JUSTIFICATION	ADDITIONAL INFORMATION / COMMENT

433.		The app/wallet does not rely on symmetric cryptography with hardcoded keys as a sole method of encryption.	M72B subsection 5.3.g M72B, section 7	
434.		The app/wallet uses proven cryptographic primitives that are appropriate for the particular use-case and compliant with regulation.	M72B subsection 5.3.g)	
435.		The app/wallet does not use cryptographic protocols or algorithms that have expired or are widely considered depreciated for security purposes.	M72B subsection 5.3.g) M72B, section 7	
436.		The cryptographic primitives are configured according to best practises or based on regulatory requirements (if they exist).	LoA, section 2.4.6, point 2 M72B, subsection 7.1	
437.		The app/wallet doesn't re-use the same cryptographic key for multiple purposes.	LoA, section 2.4.6, point 1 ITSA, section 8.1.4	
438.		All random values are generated using a sufficiently secure and high-quality random number generator.	LoA, section 2.4.6, point 1 ITSA, section 8.1.4	
439.		The app/wallet uses a signature counter to enable the server-side detection of app cloning attempts.	LoA, section 2.3.1, substantial, point 2 LoA, section 2.3.1, high	
440.		The app/wallet does not include or use any hardcoded usernames or passwords.	LoA, section 2.4.6, point 1 LoA, section 2.3.1, point 2 M72B section 6	Development time credentials (if any) must be cleaned from production version. No hard coded credentials/secrets to allow vendor access. Possible activation and PUK-codes are valid for only one-time use, and only for a predetermined period of time.
441.		Weaker cryptographic protocols, identifications or certificates used during development (if any) are removed from the production version.	LoA, section 2.4.6, points 1 and 3 LoA, section 2.4.6, high M72B, subsection 5.3.g M72B, section 7	

C 4 Authentication, characteristics of the authentication method; session management

This chapter employs the OWASP standard and chapter 4 where applicable. Additional criteria relating to the characteristics of the authentication method are also provided.

NO.	LEVEL OF ASSURANCE	CRITERION	JUSTIFICATION	ADDITIONAL INFORMATION / COMMENT
442.		The procedure used for the personalisation of the app/wallet at registration phase ensures that the app is linked to the holder of the identification means.	LoA, section 1 (definitions), point 2 LoA, section 2.2.1, substantial, point 2	
443.		The secret used for implementing the identification is protected against unauthorised use and can only be accessed using a predefined, secure method.	LoA, section 2.4.6, point 3 LoA, section 2.4.6, substantial M72B, subsection 6.4.2	Example: private key.
444.		Secrets/identification keys are unique.	M72B, subsection 5.3.g	
445.		Asymmetric secrets that implement the identification are created in the mobile device (key pair, other secret key/secret).	M72B, subsection 5.3.g M72B, subsection 5.4.b	Cf. RTS.
446.		If secrets used to implement the identification are created outside the device, they are provisioned to the device using a secure method.	LoA, section 2.4.6, point 2 LoA, section 2.4.6, substantial M72B, subsection 5.4.b	Cf. RTS.
447.		If secrets used to implement the identification are created outside of the device and provisioned to the device using a secure method, the link between the secret and the PID (person/holder) is done on the device and only during the registration phase.	LoA, section 2.3.1, point 2 LoA, section 2.2.1, substantial point 2 M72B, subsection 6.3	
448.		Identification may not be based on a shared secret alone.	LoA, section 2.2.1, substantial, point 2	
449.		App initialisation binds the secrets into the mobile device so that the secrets cannot be copied and used in another device or transferred to another device or a backup system so that the secrets could be used in the other device.	LoA, section 2.2.1, substantial, point 2 M72B, subsection 6.4.2	
450.		The app/wallet implements device binding using a device fingerprint derived from multiple properties unique to the device.	LoA, section 2.3.1, low point 3, substantial point 2 M72B, subsection 6.1	The app/wallet should implement methods/mechanisms for device binding or a mechanism that corresponds to device binding. This might however be problematic for both iOS and Android platforms when using device fingerprinting.

451.		The app/wallet does not store identification information/credentials (passwords, pins, usernames, etc) persistently at any point.	LoA, section 2.2.1, substantial, point 2 LoA, section 2.2.1, high, point 2 LoA, section 2.3.1, substantial, point 2 LoA, section 2.3.1, high, point 2 LoA, section 2.4.6, point 3	
452.		The app/wallet enables pseudonymous authentication	M72B, subsection 12.3 (GDPR art 32)	For wallet type of applications or for privacy preserving scenarios
453.		If the app/wallet is able to store attributes provisioned from a third party or generated by the user, the app/wallet stores them securely.	LoA, section 2.4.6, points 1-2 M72B, subsection 6.1 and 9.1.1	For wallet type of applications
454.		If the app/wallet allows for third party attributes to be added, the attributes are provisioned using a secure protocol and a secure presentation format.	LoA, section 2.4.6, points 1-2 M72B, subsection 6.1 and 9.1.1	For wallet type of applications
455.		The app/wallet that stores attributes locally and secures the confidentiality and integrity of the attributes using a secure element	LoA, section 2.4.6, points 1-2	Either in the secure element itself or using a key protected by the/in the secure element.
456.		If the app/wallet is used to present attributes directly to the relying party, the app/wallet implements both the transport and presentation using a secure protocol and a privacy preserving presentation and secure format.	LoA, section 2.4.6, points 1-2 M72B, subsection 6.1 and 9.1.1	For wallet type of applications.
457.		If the app/wallet allows the user to present attributes directly to the relying party, the app/wallet must verify from a trusted source that the relying party is authorized to receive these attributes.	[eIDAS2] LoA, 2.4.6, low point 3	For wallet type of applications.
458.		If the app/wallet detects that the relying party is asking for information that it is not entitled to, the app clearly warns the end user for sharing of the attributes that are out-of-scope for the relying party.	[eIDAS2] LoA, 2.4.6, low point 3	For wallet type of applications.
459.		If the app/wallet sends messages that are validated on the server and lead to identification, the messages must be sent securely using up-to-date and approved cryptographic protocols (such as Mutual/2-way TLS 1.2 or later).	LoA, section 2.4.6, point 2 M72B, subsection 5.3.g M72B, subsection 7.1.1, subsections 1-4	

460.		If personal information is exchanged between the app/wallet and the server, the information is protected using message-level encryption.	LoA, section 2.4.6, point 2 LoA, section 2.4.6, substantial M72B, subsection 5.3.g	
461.		If the app/wallet is based on or includes a method based on one-time passwords (OTP), the one-time passwords are generated using recommended, standard-based solutions.	M72B, subsection 5.3.g	
462.		The secret used for the identification is stored using services offered by the platform on a hardware based secure environment	M72B, subsection 5.3.c M72B, subsection 5.4.b	Secure element, Trusted execution environment etc. The app/wallet must be based on a risk assessment. If the risk assessment shows that the security element does not need to be used, other solutions can also be used to store the secret/secrets. The reasons for the deviation must be submitted in connection with the assessment report (as part of the risk assessments).
463.		Notice of invalid input is sent to the server separately after each occurrence. The server monitors the number of invalid inputs and locks automatically after X invalid attempts. If no network connection is available and the messages cannot be transmitted to the server securely, the app/wallet must follow the same logic (PSD2, the 5-error rule).	LoA, section 2.4.6, point 1 M72B, subsection 5.3.f	Cf. RTS and SCA.
464.		Techniques that prevent replay attacks are used between the app/wallet and the server. In case of a cryptographic nonce: Bounded Probability of a Birthday Collision	LoA, section 2.3.1, substantial, point 2 LoA, section 2.3.1, high	
465.		If session identifiers are used, the session identifiers are generated randomly.	LoA, section 2.3.1, substantial, point 2 LoA, section 2.3.1, high	
466.		(Software/OAuth) If token-based authentication is used, the server provides a token that has been signed using an acceptable and secure algorithm.	LoA, section 2.4.6, point 2 M72B, subsection 7.1.1, paragraph 2	
467.		Session or token validity is defined on the server side.	LoA, section 2.4.6, points 1 and 4	

468.		Authorisation policies used to grant access to the target application or service are defined on the (identification) server side.	LoA, section 2.4.6, points 1 and 4	
469.		If persons registered on the mobile device cannot be distinguished in the implementation of the authentication factor due to the platform properties, a combination that can reliably distinguish between the users is used (such as: mobile device = control, PIN code related to secret = information and fingerprint = property).	LoA, section 2.2.1, substantial, point 1	Example: Apple iOS, biometry. Strong identification means does not require all three factors. Two is enough if the independence of the authentication factors can be ensured and they have been bound to the holder of the identification means.
470.		If a biometric authentication factor is used and persons registered on a mobile device cannot be distinguished due to the platform properties, the user must be provided with clear instructions on how to remove the biometric identifications/secrets of other persons that belong to other users of the mobile device.	LoA, section 2.2.1, substantial, point 1 LoA, section 2.1.1, point 2 LoA, section 1 (definitions), point 2	LoA, section 2.1.1 Outside the scope of the Identification Act but recommended practice.
471.		If the app/wallet permits adding new, complementary authentication factors or changing the authentication factor, this information is also communicated to the server side. Changing and adding a factor always requires identification on a level at least equal to the level that the new combination would issue identification on. The combinations must be documented and assessed separately.	LoA, section 1 (definitions), point 2 LoA, section 2.2.1, substantial, point 2 LoA, section 2.2.4, substantial	The independence of the authentication factors must be ensured. This means, for example, changing the category of one authentication factor or adding a new category, which would result in authentication factors from three categories becoming available. The intention is to allow the user to choose authentication factors, but at the same time to ensure that the identification service can guarantee their security at all times.
472.		In strong multi-factor authentication, a factor based on information possessed by the user (password, pin) or a physical property of the user (fingerprint, face recognition, iris) is used to unlock the secret that is used to respond to the actual identification request.	LoA, section 1 (definitions), point 3 LoA, section 2.2.1, substantial, point 2 LoA, section 2.3.1, substantial, point 2	
473.		The implementation of a biometric authentication factor only uses interfaces offered by the platform.	LoA, section 2.4.6, point 1 M72B, subsection 5.3.c	Special use case: Reading a passport/identity card chip over NFC. In this case too, the interfaces offered by the platform should be used.
474.		When a biometric factor is used, the biometric record or the template (fingerprint, facial recognition data, iris	LoA, section 2.2.1, substantial, point 2	

		scan data, etc.) is not transferred outside the app/wallet during the identification event.	LoA, section 2.3.1, substantial, point 2	
475.		Sensitive information or personally identifiable information used at the registration phase can only be transferred to the server side using secure methods.	LoA, section 2.4.6, point 2	
476.		The user has the option to temporarily close the secret on a) one device/instance, b) multiple devices/instances and c) all devices/instances at once.	LoA, section 2.2.3, substantial, point 1	
477.		Opening a secret that is closed temporarily always requires identification on a level equal or higher to the identification that would be required for activating the app/wallet.	LoA, section 2.2.3, substantial, point 3	
478.		The user must have an option to securely deactivate the identification app and secret on a) one device/instance, b) multiple devices/instances and c) all devices/instances.	LoA, section 2.2.3, substantial, points 1 and 2	
479.		Temporary, device-specific closing and removal of a secret must also be possible on the (issuer) server side.	LoA, section 2.2.3, substantial, points 1 and 2	
480.		The identification is bound to the desired transaction or browser session; in other words, the identification app must clearly display information about the action that is being done.	LoA, section 2.3.1, substantial, point 2	E.g. RTS, dynamic linking. EU 2018/389 PSD2 regulation lays down more specific requirements for dynamic linking. These requirements must be met if the identification app is used for both general-purpose identification and identification for payment purposes.
481.		The identification app/wallet implements a binding message which enables the user to link the identification in the mobile device to a browser session, for example, in understandable terms.	LoA, section 2.3.1, substantial, point 2, M72B, section 6.2.1	Use language that can help the user to understand what a session binding message is.
482.		The identification app/wallet always displays the name of the service/application the user is authenticating to based on the attribute sp_name. This information must be visible and easy to understand by the user.	M72B, section 6.2.2	The language must be clear and not to be confused with the session binding message.
483.		If the response of the identification app/wallet is based on an asymmetrical signature, the WYSIWYS principle is followed (the information displayed to the user is the information that is being signed).	LoA, section 2.3.1, substantial, point 2	

484.		The app/wallet guides the user to select strong PIN codes.	LoA, section 2.1.1, substantial, point 2 M72B, subsection 5.3.g	LoA 2.1.1 is outside the scope of the Identification Act but is recommended practice.
485.		The app/wallet does not accept PIN codes or other secrets based on the user's memory that are easily guessed.	LoA, section 2.3.1, substantial, point 2 LoA, section 2.4.6, point 1	For example, the app does not accept PIN codes that are known to be weak or easily guessed (e.g. 999999, 123456, 999999).
486.		User inputs, such as PIN codes, are validated in secure manner.	LoA, section 2.3.1, substantial, point 2 M72B, subsection 5.4.b	
487.		The app/wallet uses hardware-level security features of the mobile device such as TEE/SE and similar, the app indicates the hardware-level component that is used and makes other details available to the (issuer) server in connection with initialisation so that the server can detect and respond to hardware-level vulnerabilities (also in the future).	LoA, section 2.4.6, point 1 and 4 M72B, subsection 5.4.d	CVE-2018-11976 → Providing the server with an opportunity to react to known vulnerabilities in hardware-level components.
488.		If the backend or the relying party detects a non-genuine app/wallet, the identification flow must be stopped. I.e., app/wallet attestation must be implemented on the app itself and the attestation validated, when applicable, before proceeding with the identification request.	LoA, section 2.4.6, points 1 and 3 LoA, section 2.3.1, substantial point 1	NOTE:added 19.05.2023
489.		The app /wallet and/or the back-end ensures that there cannot be simultaneous active authentication requests, i.e., previous requests must be invalidated/closed before initiating a new request.	LoA, section 2.3.1, substantial point 2	

C 5 Data communication

NO.	LEVEL OF ASSURANCE	CRITERION	JUSTIFICATION	ADDITIONAL INFORMATION / COMMENT
490.		The network traffic between the app/wallet and the server is protected using internationally or nationally recommended connection procedures. The secure	LoA, section 2.4.6, point 2 M72B, subsection 5.3.g	No encryption requirements have been set for the identification scheme's *internal* connections, but the data communication encryption policies

		channel is used consistently throughout the app/wallet.		defined in M72B, section 7 for use *between the parties* should be taken as the starting point.
491.		The app/wallet checks that the TLS (or similar) settings/configuration are in line with current best practices.	LoA, section 2.4.6, point 2 M72B, subsection 5.3.g , subsection 7.1.3, and 7.2	No encryption requirements have been set for the identification scheme's *internal* connections, but the data communication encryption policies defined in M72B, section 7 for use *between the parties* should be taken as the starting point.
492.		The app/wallet pins the endpoint certificate or public key, and subsequently does not establish connections with endpoints that offer a different certificate or key, even if signed by a trusted CA.	LoA, section 2.4.6, point 2	
493.		The app/wallet does not rely on a single insecure communication channel (email or SMS) for critical operations, such as enrollments and generation of the user secret.	LoA, section 1 (definitions), point 2 LoA, section 2.2.1, substantial, point 2	In practice, the personalisation of the application must be based on a strong means of electronic identification.
494.		The app/wallet only depends on up-to-date connectivity and security libraries.	LoA 2.4.6, sections 1 and 4	

C 6 Platform interaction

NO.	LEVEL OF ASSURANCE	CRITERION	JUSTIFICATION	ADDITIONAL INFORMATION / COMMENT
495.		The app/wallet only requests the minimum set of permissions necessary.	LoA, section 2.4.6, point 1 M72B, subsection 5.3.c	
496.		All inputs form external sources are validated and sanitized.	LoA, section 2.4.6, point 4 M72B, subsection 5.3.c	
497.		The app/wallet does not export data via custom URL schemes or IPC mechanisms	LoA, section 2.4.6, point 2 M72B, subsection 5.3.c	
498.		If the app/wallet needs to display content via a browser (e.g. method selection in the identification server), the operating system's secure features (See OS vendor current best practises) should be used primarily. WebView is used only if more secure alternatives are not available. The components used	LoA, section 2.4.6, point 1 M72B, subsection 5.3.c	

		are configured to allow only the minimum set of protocol handlers required. Other connection policies are blocked/confirmed as being disabled.		
499.		JavaScript is disabled in browser components by default.	LoA, section 2.4.6, point 1 M72B, subsection 5.3.c	
500.		If browser components are used, they are configured to allow only https	LoA, section 2.4.6, point 1 M72B, subsection 7.1-2 and 9.3	
501.		Native methods are blocked in case the platform's software version has been found vulnerable.	LoA, section 2.4.6, point 1 M72B, subsection 5.3.c and 5.4.d)	JavaScript implementations on old versions of the Android operating system, for example, may be insecure.
502.		If native methods of the app/wallet are exposed to browser components, verify that the browser component only renders JavaScript contained within the app package.	LoA, section 2.4.6, point 1 M72B, subsection 5.3.c)	
503.		Browser components cannot access / are blocked from local resources.	LoA, section 2.4.6, point 1 M72B, subsection 5.3.c	
504.		Object deserialization, if any, is implemented using safe serialization APIs.	LoA, section 2.4.6, points 1 and 3 LoA, section 2.4.6, substantial M72B, subsection 5.3.c	
505.		The app/wallet protects itself against screen overlay attacks.	LoA, section 2.4.6, points 1	Risk management methods for overlay-type attacks depend on the platform used and the features it offers. For example, since Android API version 9, this risk can already be partially managed. The app/wallet makes full use of the security controls offered by the platform.
506.		The browser component cache, storage, and loaded resources must be cleared before the browser component is destroyed	LoA, section 2.4.6, points 1 and 3 M72B, subsection 5.4.b	
507.		Verify that the app/wallet prevents usage of third-party keyboards whenever sensitive data is entered.	LoA, section 2.4.6, points 1-2	As an exception, for example, those use cases where using a third-party keyboard is a prerequisite for using the identification application. These must be separately identified and documented.

C 7 Code security, quality and development environment

NO.	LEVEL OF ASSURANCE	CRITERION	JUSTIFICATION	ADDITIONAL INFORMATION / COMMENT
508.		The app/wallet is signed and provisioned with a valid, trusted certificate and the private key is properly protected	LoA, section 2.4.6, point 1	
509.		The app/wallet has been built in release mode (e.g. non-debuggable).	LoA, section 2.4.6, point 1 M72B, subsection 5.3.c	
510.		App/wallet development only uses tested and recommended software development/coding data security policies.	LoA, section 2.4.6, point 1 M72B, subsection 5.3.c	All JavaScript components, for example, must be encoded and sanitised to reduce the risk of XSS attacks.
511.		Debugging symbols have been removed from native binaries.	LoA, section 2.4.6, point 1 M72B, subsection 5.3.c	
512.		Debugging code and messages has been removed.	LoA, section 2.4.6, point 1 M72B, subsection 5.3	
513.		Testing or development time settings, verbose logging and configurations have been removed from the release version.	LoA, section 2.4.6, points 1 and 4 M72B, subsection 5.3.c and 5.4.d	
514.		All third party components used by the app/wallet are identified, and checked for known vulnerabilities regularly.	LoA, section 2.4.6, point 4 M72B, subsection 5.4.d	
515.		The app/wallet catches and handles possible exceptions.	LoA, section 2.4.6, point 4 M72B, subsections 5.3.f and 5.4.d)	
516.		The app/wallet or the server minimises the information contained in error messages.	LoA, section 2.4.6, point 1 M72B, subsection 5.3.c	
517.		Error handling logic in security controls denies access by default.	LoA, section 2.4.6, point 1 M72B, subsection 5.3.c	
518.		Memory is allocated, freed and used securely.	LoA, section 2.4.6, point 1 M72B, subsection 5.3.c	
519.		The data security features of the platform / development environment are activated.	LoA, section 2.4.6, point 1 M72B, subsection 5.3.c	

C 8 Security controls and resilience

NO.	LEVEL OF ASSURANCE	CRITERION	JUSTIFICATION	ADDITIONAL INFORMATION / COMMENT
520.		The app/wallet implements multiple defence mechanisms defined in this chapter.	LoA, section 2.4.6, point 1	The application's capacity to withstand attacks must be assessed as a whole.
521.		The app/wallet has more than one feature that attempts to detect the presence of a rooted or jailbroken device.	LoA, section 2.4.6, point 4 M72B, subsection 5.3.f	
522.		The detection mechanisms trigger responses of different types, including delayed and stealthy responses.	LoA, section 2.4.6, point 4 M72B, subsection 5.3.f and 6.1	
523.		The app/wallet sends a message to the server-side implementation upon detection of a rooted/jailbroken device platform, or the app has the ability to decide what to do upon detection of a rooted/jailbroken platform.	LoA, section 2.4.6, point 4 M72B, subsection 5.3.f	
524.		The app/wallet prevents debugging and detects, and responds to, a debugger being attached. All available debugging protocols must be covered.	LoA, section 2.4.6, point 1 M72B, subsection 5.3.c	
525.		The app/wallet detects, and responds to, tampering with executable files and critical data/files within its own sandbox.	LoA, section 2.4.6, point 4 M72B, subsection 5.3.f	
526.		The app/wallet detects, and responds to, the presence of widely used reverse engineering tools on the device.	LoA, section 2.4.6, point 4 M72B, subsection 5.3.f	
527.		The app/wallet detects, and responds to, being run in an emulator.	LoA, section 2.4.6, point 4 M72B, subsection 5.3.f	
528.		The app/wallet detects, and responds to, tampering the code and data in its own memory space.	LoA, section 2.4.6, point 4 M72B, subsection 5.3.f	
529.		Partitions that are important or critical to the app/wallet are encrypted where applicable on the system level. Analysis cannot be used to identify partitions that are important or critical to the app/wallet.	LoA, section 2.4.6, points 1 and 3 LoA, section 2.4.6, substantial M72B, subsections 5.3.c and 5.4.b	
530.		Application level payload encryption is applied	LoA, section 2.4.6, points 1-4 M72B, subsection 5.3.g	

References

The criteria used as justification for this guideline:

ITSA - Act on Strong Electronic Identification and Electronic Trust Services 617/2009

LoA - 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

M72B - Regulation on Electronic Identification and Trust Services (M72B/2022) https://www.kyberturvallisuuskeskus.fi/en/our-activities/regulation-and-supervision/electronic-identification

OWASP - OWASP Mobile Application Security Verification Standard, MASVS version 1.4.2