Assessment guideline for electronic identification services

TRAFICOM Guideline

211/2019 O

DRAFT VERSION – 20 June 2019

Finnish Transport and Communications Agency Traficom

Erik Palménin aukio 1
P.O. Box 313
FI-00059 TRAFICOM
Tel. +358 295 390 100
www.traficom.fi

Contents

Finnish Transport and Communications Agency Traficom

Erik Palménin aukio 1
P.O. Box 313
FI-00059 TRAFICOM
Tel. +358 295 390 100
www.traficom.fi

Finnish Transport and Communications Agency Traficom

Erik Palménin aukio 1
P.O. Box 313
FI-00059 TRAFICOM
Tel. +358 295 390 100
www.traficom.fi

Finnish Transport and Communications Agency Traficom

Erik Palménin aukio 1
P.O. Box 313
FI-00059 TRAFICOM
Tel. +358 295 390 100
www.traficom.fi

Finnish Transport and Communications Agency Traficom

Erik Palménin aukio 1
P.O. Box 313
FI-00059 TRAFICOM
Tel. +358 295 390 100
www.traficom.fi

1 Introduction

This document applies to conformity assessments for electronic identification services and the audit 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 audit 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.

Finnish Transport and Communications Agency Traficom

Erik Palménin aukio 1
P.O. Box 313
FI-00059 TRAFICOM
Tel. +358 295 390 100
www.traficom.fi

As a result of the audit, an identification service audit 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 audit 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 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 (214/2016 O). The eIDAS Regulation and the Electronic Identification Assurance Level Regulation (LOA)[2] provide for the conformity assessment of an electronic identification means to be notified to the EU.

1.2 Entry into force of the Guideline

Guideline 211/2019 O will enter into force on x x 2019.

[1] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing of Directive 1999/93/EC.
[2] Commission Implementing Regulation (EU) 2015/1502 of 8 September 2015 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 (Text with EEA relevance).

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.

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

Version	Date	Description/change	Author
211/2019 O	x x 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	2 Nov 2016	First published versions	Finnish Communications Regulatory Authority (FICORA), NCSC-FI

service provider audits 215/2016 O Identification and trust service assessment reports			

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 audit 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 or Identification and Trust Services Act*)
- Commission Implementing Regulation (EU) 2015/1502[3] (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)[4]
- FICORA Regulation 72A/2018 M (hereinafter referred to as *M72*)
    - This Regulation complements certain requirements set out in the Identification Act.

References to standards:[5]

- ISO/IEC 27001:2013 Information security management

[3] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ%3AJOL_2015_235_R_0002 The Commission Implementation Regulation is based on eIDAS Regulation (EU) No 910/2014 of the European Council and of Parliament on electronic identification and trust services for electronic transactions in the single market and repealing Directive 1999/93/EC.
[4] https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/LOA_Guidance.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

- 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.1.1.3[6]

Assurance level abbreviations used in tables:

- S=substantial (corresponds to eIDAS2, *substantial*)
- H=high (corresponds to eIDAS3, *high*)

1.4 Definitions of identification service

In both the relevant regulations and this document, an *identification service* is a combined term for identification means providers and identification broker services.

Identification means providers offer electronic identification means to end users.

Identification broker services provide identification transactions for providers of eServices, in other words, for parties relying on electronic identification.

[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 method and an identification scheme.

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 72.

The information to be submitted to Traficom with notifications on commencing, terminating or changing of operations is described in further detail in **Guideline 214/2016 O Electronic identification and trust service notifications**.

PROVISIONS

M72, Section 16: Declaration of compliance with other requirements

Finnish Transport and Communications Agency Traficom

Erik Palménin aukio 1
P.O. Box 313
FI-00059 TRAFICOM
Tel. +358 295 390 100
www.traficom.fi

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

1) published notices and user information, such as identification principles, price lists and terms and conditions
2) established organisation
3) preparedness to bear risks of damage
4) sufficient financial resources
5) responsibility for subcontractors
6) planning for the termination of operations.

2 Identification service assessment and the audit report

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

PROVISIONS

Identification Act (617/2009, amendment 23.11.2018/1009, unofficial translation), 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 an association of identification service providers, if such services provided can be deemed as such by an identification service.

The notification shall contain:

[…]

5) an audit report on the independent audit drawn up by 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.

Identification Act (617/2009, unofficial translation) 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.

Identification Act (617/2009, unofficial translation) section 31: Assessment report

The identification service provider and the Population Register Centre 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.

Finnish Transport and Communications Agency Traficom

Erik Palménin aukio 1
P.O. Box 313
FI-00059 TRAFICOM
Tel. +358 295 390 100
www.traficom.fi

2.1.1 Commencement notification

When a new identification service provider notifies Traficom that it will commence operations, an audit 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 audit 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 audit report must be submitted before the change is transferred to production.

Examples of material changes include:

- Changes of the identification method, 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.

2.1.3 Periodic assessment

An audit report must be submitted to Traficom as an attachment to the change notification when two years have passed since the approval of the previous audit report.

Finnish Transport and Communications Agency Traficom

Erik Palménin aukio 1
P.O. Box 313
FI-00059 TRAFICOM
Tel. +358 295 390 100
www.traficom.fi

According to law, the identification service assessment report must be valid for the period defined in the standard that is applied, but no more than for two years. The validity period of the audit report, i.e. up to two years, must be calculated from the date when Traficom approved the audit report. The identification service provider must submit a new audit report to Traficom within two years of the approval of the previous audit 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 audit report referred to in this Guideline must be submitted within two years of the approval of the previous report.

Regulations on the assessment requirement entered into force as part of the Identification Act on 1 July 2016, and according to the period of transition specified in the act, the report was to be submitted to FICORA by 31 January 2017. FICORA has published an advisory memorandum for the 2019 reassessment (reg. no. 1003/620/2018, Interpretation memorandum 12/2018, *Advice on assessing of compliance of identification services in 2019*).

The minimum contents of the notification of commencing operations and change notifications are described in FICORA Guideline 214/2016 O.

Finnish Transport and Communications Agency Traficom

Erik Palménin aukio 1
P.O. Box 313
FI-00059 TRAFICOM
Tel. +358 295 390 100
www.traficom.fi

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 FICORA's Regulation 72.

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 audit 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 method and the identification scheme.

Annex C provides assessment criteria for mobile apps intended to complement the overall criteria in cases where the identification method 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 methods** (identification means).

Sections from 1a) to 1d) and section 2g) apply to **identification broker services**.

PROVISIONS

Finnish Transport and Communications Agency Traficom

Erik Palménin aukio 1
P.O. Box 313
FI-00059 TRAFICOM
Tel. +358 295 390 100
www.traficom.fi

Identification Act (617/2009, amendment 1009/2018, unofficial translation) section 29: Compliance assessments of electronic identification services

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

[…]

Identification Act (617/2009, amendment 1009/2018, unofficial translation) section 42: General guidance and regulations by the Finnish Transport and Communications Agency

[…]

The Finnish Transport and Communications Agency may issue further regulations on the following:

[…]

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

[…]

M72, section 15: Assessment criteria

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

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

Finnish Transport and Communications Agency Traficom

Erik Palménin aukio 1
P.O. Box 313
FI-00059 TRAFICOM
Tel. +358 295 390 100
www.traficom.fi

a) information security management
b) record keeping
c) facilities and staff
d) technical measures

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

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

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

2.3 Identification method, identification scheme and subcontractors

2.3.1 Definitions

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

An identification method 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

Identification Act (617/2009, amendment 1009(2018, unofficial translation) section 2 Definitions

2) identification means means the electronic identification means referred to in Article 3(2) of the EU regulation on electronic identification and trust services;

Cf. Identification Act section 8: Requirements posed on the electronic identification scheme

Cf. Identification Act 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;

Finnish Transport and Communications Agency Traficom

Erik Palménin aukio 1
P.O. Box 313
FI-00059 TRAFICOM
Tel. +358 295 390 100
www.traficom.fi

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

Identification Act (617/2009, unofficial translation) 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 people working for it.

2.3.2 Assessment

As the offering 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 offering 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, in other words, 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.

Requirements set for **identification methods** with relevance to **identification broker services** include authentication mechanisms as far as the broker service relays identification transactions between the party offering 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 transactions.

The assessment criteria presented in the table do not include separate ISO/IEC 27001:2013 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 authentication method 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 is 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 method 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 identification relying on mobile phone only 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 (virtualization 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.
-

Finnish Transport and Communications Agency Traficom

Erik Palménin aukio 1
P.O. Box 313
FI-00059 TRAFICOM
Tel. +358 295 390 100
www.traficom.fi

2.3.3 Assessment report: A description that specifies the part of the identification method 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 audit report is unambiguous in detailing whether the audit 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 audit 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 report or in the documentation of the identification service.

2.3.5 Assessment report: Description of identification method (identification means)

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

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

- What are the authentication factors used in the identification method (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 transactions are implemented).

The specification documents 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 description 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 productized 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

Identification Act (617/2009, unofficial translation, amendment 2016/533), 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 audit 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 audit reports can be provided. Full details of all assessment bodies need to be provided.

The identification service audit 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 M72, sections 18 and 19).

Identification Act (617/2009, unofficial translation, amendment 2018/1009), 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 72, section 18: Requirements concerning an external assessment body of the identification service

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

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

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

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

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

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

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

Regulation 72, section 19: Requirements concerning an internal notified body of the identification service

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

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

Finnish Transport and Communications Agency Traficom

Erik Palménin aukio 1
P.O. Box 313
FI-00059 TRAFICOM
Tel. +358 295 390 100
www.traficom.fi

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

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

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

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

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

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

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.

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 audit report must establish which concrete matters the conformity assessment is based on, in other words 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 tasks from anyone whose rights and obligations are provided for in the 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.

2.6 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 method 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 method. 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.

[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.

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

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 prevent all attacks completely, they can only offer resistance to attacks on a certain level of security/assurance. A standard way to quantify the resistance of different mechanisms is to rank them according their resistance against attacks with a certain attack potential (i.e. strength of an attacker).

The Level of Assurance use the terms "enhanced-basic", "moderate" and "high" to denote the different attack potentials. This terminology is borrowed from ISO/IEC 15408 "Information technology – Security techniques – Evaluation criteria for IT security" and ISO/IEC 18045 "Information technology – Security techniques – Methodology for IT security evaluation". The text of the standards is

Finnish Transport and Communications Agency Traficom
Erik Palménin aukio 1
P.O. Box 313
FI-00059 TRAFICOM
Tel. +358 295 390 100
www.traficom.fi

also freely available at www.commoncriteriaportal.org/cc (CCPART1-3 being equivalent to ISO/IEC 15408 and CEM equivalent to ISO/IEC 18045).

ISO/IEC 15408-1 defines "attack potential – measure of the effort to be expended in attacking a [mechanism], expressed in terms of an attacker's expertise, resources and motivation".

Annex B.4 of ISO/IEC 18045 / CEM contains Guidance on how to calculate the attack potential necessary to exploit a given weakness of an authentication mechanism.

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

The assessment should take relevant threats into accounts. For example, ISO 29115 mentions: online guessing, offline guessing, credential duplication, phishing, eavesdropping, replay attack, session hijacking, man-in-the-middle, credential theft, spoofing and masquerading.

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

…

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.

…

Finnish Transport and Communications Agency Traficom

Erik Palménin aukio 1
P.O. Box 313
FI-00059 TRAFICOM
Tel. +358 295 390 100
www.traficom.fi

> ***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***
>
> …
>
> As 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 competence in the maintenance and management of information security, it is recommended that the audit 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.

Normally, any irregularities that are found should be corrected before the assessment report is submitted to Traficom. However, if any irregularities remain, they must be clearly identified in the assessment report. In

this case, the report must contain details of any minor or other irregularities still remaining in the system and indicate how and when they will be corrected.

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 decision 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.

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 overall assessment criteria can be found in Annex B.

3.1 Characteristics of the identification method; authentication mechanism

The requirements are set out in the following provisions:

- Identification Act, section 8 a: Authentication factors used in the identification method.
- LOA Annex, section 2.2.1: Electronic identification means characteristics and design
- Identification Act, section 8: Requirements posed on the electronic identification system (subsection 1, paragraph 3)

- LOA Annex, section 2.3.1: Authentication mechanism
- LOA Annex, section 2.4.6: Technical controls (point 2)
- M72, section 6: Information security requirements of the identification method
- M72, section 7: Encryption requirements of the identification scheme and interfaces
- M72, section 8: Information security requirements concerning the interface between an identification means provider and an identification broker service provider
- M72, section 9: Information security requirements at the eService interface

- 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 method and the authentication mechanism as well as the identification method's capacity for protecting against data security threats and violations on the level required by the level of assurance have been assessed.

The compliance of the characteristics of the identification method is the responsibility of the party that offers the identification means.

The compliance of the authentication mechanism is also the responsibility of the identification broker service, as the broker system is involved in the relaying of identification transactions.

In addition to the assessment report, a scanning report of the assessment (specified in M72, 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:

- Identification Act (amendment 2019/412), 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)
- M72, section 12: Minimum set of data to be relayed in a trust network
- M72, 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 method are assessed. The 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 method.

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:

- Identification Act section 8: Requirements posed on the electronic identification system (subsection 1, paragraph 4)
- LOA 2.3.1: Authentication mechanism
- LOA Annex, section 2.4.6 Technical controls, points 1, 2 and 3
- M72, section 5: Technical information security measures of the 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 of 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 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:

- Identification Act, 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
- Identification Act, section 16: The identification service provider's duty of notification about threats and risks related to data security and protection
- M72, section 5: Technical information security measures of the identification scheme
- M72, section 11: Disturbance notifications by the identification service provider to FICORA [Traficom]

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

- incident observation capacity
- collecting of transaction 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:

- Identification Act, section 13: General obligations of an identification service provider
- LOA Annex, section 2.4.4: Record keeping, points 1 and 2

- Identification Act, 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
- M72, section 5: Technical information security measures of the identification scheme
- M72, section 7: Encryption requirements of the identification scheme and interfaces
- Identification Act, 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:

- Identification Act, section 8: Requirements posed for 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 audit report should pay attention to the following matters (as applicable):
- protection from environmental hazards (fire, heat, gas, dust, vibration, water)
- prevention of authorised 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:

- Identification Act, 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 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:

- Identification Act, section 8: Requirements posed for 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
- M72, section 4: Information security management requirements of an 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 (Identification Act, the eIDAS LOA Regulation and FICORA Regulation 72) 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:

- Identification Act, section 8: Requirements posed for the electronic identification scheme (subsection 1, paragraphs 1 and 2)
- Identification Act, section 17: Initial identification of an applicant for an identification device
- LOA Annex, section 2.1.2: Identity proofing and verification (natural person)
- Identification Act, section 7 b: Information of validity of passport or identity card
- M72, section 6: Information security requirements of the identification method

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

- Identification Act, section 7 a: Use of information from the business information system
- Identification Act, section 17 a: Initial identification of an applicant for an identification means (legal person)

- LOA Annex, section 2.1.3: Identity proofing and verification (legal person)
- LOA Annex, section 2.1.4

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

Initial identification procedures available:
- initial identification is based on the presentation of an identity document approved in Finland
- initial identification using an electronic identification means
- initial identification based on identification made for other purpose
- initial identification by the police.

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.

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.

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, for example: 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 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.

- The question of how the authenticity of an identity document without a chip can be confirmed remains open. 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.

Finnish Transport and Communications Agency Traficom

Erik Palménin aukio 1
P.O. Box 313
FI-00059 TRAFICOM
Tel. +358 295 390 100
www.traficom.fi

- 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) is freely readable.

- Almost all passports 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. This feature will be introduced for EU identity cards at some point in the future. However, US passports do not have this additional authentication feature.

- 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 transaction.

- 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.

- 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.

- Assessment of the lifelike appearance of the person who presents the identity document in the remote identification transaction can help confirm that the presenter of the identity document is present and that no forged recording is used. The person could be requested, for example, to perform certain random gestures in real time.

- 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.

- 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.

3.10 Lifecycle of identification means (identification method)

The requirements are set out in the following provisions:

- Application and registration: Identification Act, sections 7 and 20; M72, section 6
- Issuance, delivery and activation: Identification Act, sections 20 and 21; LOA, section 2.2.2
- Suspension, revocation and reactivation: Identification Act, sections 25 and 26; LOA, section 2.2.3
- Renewal and replacement: Identification Act, section 22; LOA, section 2.2.4

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

- The personal information 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 March 2019, Traficom published an advisory memorandum[8] on the verification of identity in maintenance situations.

[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.

4 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 organisation and a unique registration number or identifier.

    2) If the company or the 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. The competence and independence of the assessment body (2.4.2)

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

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

4. Assessment methods (2.5.2)

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

6. A description of which part of the identification method and/or the identification scheme the assessment covers (2.3.3)
7. Name(s) of the identification service to be assessed (2.3.4)
8. Description of identification method (identification means) (2.3.5)
9. Description of the identification scheme (system architecture) (2.3.6)
10. Irregularities (2.8)
11. Results of assessment specific to individual areas (3.1–3.10 as applicable)

Finnish Transport and Communications Agency Traficom

Erik Palménin aukio 1
P.O. Box 313
FI-00059 TRAFICOM
Tel. +358 295 390 100
www.traficom.fi

5 ANNEX B: General assessment criteria for identification services

5.1 Characteristics of the identification method; authentication mechanism

1 Characteristics of the identification method; authentication mechanism

M72, section 15: Assessment criteria

The identification service assessment shall cover the requirements concerning the following:
2) the identification method, meaning certain properties of the identification means, namely:
c) identification means characteristics and design
g) authentication mechanisms

NO.	LEVEL OF ASSURANCE	REQUIREMENT PERTAINING TO THE IDENTIFICATION SERVICE (SUMMARY)	PROVISIONS	STANDARD REFERENCE	NOTES
1.	S, H	The identification method uses at least two authentication factors from different authentication factor categories.	**Identification Act, section 8 a: Authentication factors used in the identification method.** 1) knowledge-based authentication factor, the possession of which the individual needs to prove; 2) possession-based authentication factor, the possession of which the individual needs to prove; 3) inherent authentication factor 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 utilises at least two authentication factors from different categories.		
2.	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.		Mutual independence of authentication factors requires special attention especially in identification methods used on mobile devices.
3.	S, H	Different threat types that target different authentication factors are taken into account in the planning of the identification method.	**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.		
4.	S, H	Secret information related to the identification method is not accessible to the personnel or the subcontractors of the identification service provider.	**M72A, section 6: Information security requirements of the identification method** […] The service provider shall ensure that secret information related to the identification means are not revealed to its staff under any circumstances. The service provider shall not make copies of any secret information related to the identification means.		Secret information typically includes PIN codes and other information-based authentication factors. This requirement is intended to address the risk of dishonest personnel.

5.	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.		Examples include binding of identification application to a person, chip personalisation or the linking of a pass code list or device to a person.
6.	S, H	The authentication mechanism is designed so that each identification transaction has unique electronic proof.	**Identification Act, section 8** […]Every identification means must use a dynamic authentication referred to in section 2.3.1 of the Annex to the Regulation on Level of Assurance in Electronic Identification that changes in every new identification event between the person and the system certifying his or her identity.		Also applies to identification broker services.
7.	S, H	The electronic proof of each identification transaction 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;		LOA Guidance (excerpts) 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.	H	The user is able to protect the identification method (means) and his or her 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.		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 • 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.

Finnish Transport and Communications Agency Traficom

Erik Palménin aukio 1
P.O. Box 313
FI-00059 TRAFICOM
Tel. +358 295 390 100
www.traficom.fi

9.	S, H	No identification data is released to the relying party (no identification transaction is performed) before the identification means/method is verified using dynamic authentication.	**LOA Annex, section 2.3.1: Authentication mechanism** The release of person identification data shall be 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 application services transactions	Also applies to identification broker services.
10.	S, H	The identification data stored in the identification transaction 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		Also applies to identification broker services.

			order to protect against loss and against compromise, including analysis offline. Cf. M72, sections 7–9: Message-level encryption requirements (below).		Applies to all technical environments that participate in the identification transaction in which identification data is stored.
11.	S	The security measures used in the identification method provide protection against attacks of a moderate severity rating.	**Identification Act, section 8**: **Requirements posed on the electronic identification scheme** Section 8.1, paragraph 3: Section 8.1, paragraph 3: The identification means can be used 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 Level of Assurance Regulation on 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.	The assessment should take relevant threats into accounts. For example, ISO 29115 mentions: online guessing, offline guessing, credential duplication, phishing, eavesdropping, replay attack, session hijacking, man-in-the-middle,	Also applies to identification broker services. 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 LOA Guidance, Point 2.3.1 (description, pages 24–26) https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/LOA_Guidance.pdf

Finnish Transport and Communications Agency Traficom

Erik Palménin aukio 1
P.O. Box 313
FI-00059 TRAFICOM
Tel. +358 295 390 100
www.traficom.fi

				credential theft, spoofing and masqueradin g. 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.	
12.	H	The security measures used in the identification method provide protection against attacks of high severity rating.	**Identification Act, section 8: Requirements posed on the electronic identification scheme.** Section 8.1, paragraph 3: The identification means can be used 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 Level of Assurance Regulation on Electronic Identification **LOA Annex, section 2.2.1: Electronic identification means characteristics and design**	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.

			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 potential can subvert the authentication mechanisms.		
13.	S, H	The authentication mechanism follows the mandatory encryption requirements **between the identification means provider and the identification broker~~ing~~**.	**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. **M72, section 7: Encryption requirements of the identification scheme and interfaces** Interfaces between identification service providers and interfaces between an identification service provider and an eService shall be encrypted. The following methods shall be used in the encryption, key exchange and signcryption: 1) Key exchange: In key exchange, DHE methods or ECDHE methods with elliptic curves shall be used. The size	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.

Finnish Transport and Communications Agency Traficom
Erik Palménin aukio 1
P.O. Box 313
FI-00059 TRAFICOM
Tel. +358 295 390 100
www.traficom.fi

			of the finite field to be used in calculations shall be at least 2048 bits in DHE and at least 224 bits in ECDHE. 2) Signature: When using the RSA for electronic signatures, the key length shall be at least 2048 bits. When using the elliptic curve method ECDSA, the underlying field size shall be at least 224 bits. 3) Symmetrical encryption: The encryption algorithm shall be AES or Serpent. The key length shall be at least 128 bits. The encryption mode shall be CBC, GCM, XTS or CTR. 4) Hash functions: The hash function shall be SHA-2, SHA-3 or Whirlpool. SHA-2 refers to functions SHA224, SHA256, SHA384 and SHA512. Encryption settings shall be technically forced to the minimum levels listed above to avoid a situation where settings weaker than the minimum levels are adopted following connection handshakes. If the TLS protocol is used, version 1.2 of TLS or newer shall be used. Version 1.1 of TLS may only be used if the user's terminal does not support newer versions. The integrity and confidentiality of messages containing personal data shall be protected by encryption referred to		

Finnish Transport and Communications Agency Traficom

Erik Palménin aukio 1
P.O. Box 313
FI-00059 TRAFICOM
Tel. +358 295 390 100
www.traficom.fi

			paragraph 1 above and also at a message level in accordance with paragraph 1. **M72 Section 8: Information security requirements concerning the interface between an identification means provider and an identification broker service provider** Encryption methods shall meet the requirements of section 7(1)–(4) above. In identifying the parties and in relaying the data necessary for identification, metadata or similar procedures that ensure a corresponding level of information security shall be used. All personal data shall be encrypted and signed at the message level.		
14.	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. **M72, section 7 (see above)** **M72, section 9: Information security requirements at the eService interface**	A.10.1.1 Policy on the use of cryptographic controls A.13.2.3 Communications security	Note: also applies to identification broker services.

Finnish Transport and Communications Agency Traficom

Erik Palménin aukio 1
P.O. Box 313
FI-00059 TRAFICOM
Tel. +358 295 390 100
www.traficom.fi

			The interface between an identification broker service provider and an eService shall meet the requirements of section 7(1)–(4) above. An identification means provider and identification broker service shall ensure the confidentiality and integrity of personal data at the eService and user interface.	/ Information transfer: Electronic messaging	
15.	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. **M72, section 7 (see above)** **M72, section 9: Information security requirements at the eService interface** The interface between an identification broker service provider and an eService shall meet the requirements of section 7(1)–(4) above. An identification means provider and identification broker service shall ensure the confidentiality and integrity of personal data at the eService and user interface.	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.
16.	H	The authentication method follows the **recommended** tightened/high level encryption requirements between the	**MPS72, section B 7.2 (14.5.2018, recommendation)**	A.10.1.1 Policy on the use of	Note: also applies to identification broker services.

Finnish Transport and Communications Agency Traficom
Erik Palménin aukio 1
P.O. Box 313
FI-00059 TRAFICOM
Tel. +358 295 390 100
www.traficom.fi

		identification broker service and identification brokering, between the identification service and the eServices and in the user interface (browser, mobile device).	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 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 2048 (3072 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 *15 to 21* at high level of assurance) of IANA's IKEv2 specifications meet the above requirements. 2) Signature: When using the RSA for electronic signatures, the key length shall be at least 2048 (3072 at high level of assurance) bits. When using the elliptic curve method ECDSA, the underlying field size shall be at least 224 (256 at high level of assurance) bits. 3) Symmetrical encryption: The encryption algorithm shall be AES or Serpent *(*AES or Serpent *at high level of assurance)*. The key length shall be at least 128 (128 at	cryptographic controls A.13.2.3 Communications security / Information transfer: Electronic messaging	

			high level of assurance) bits. The encryption mode shall be CBC, GCM, XTS or CTR. 4) Hash functions: The hash function shall be SHA-2, SHA-3 or Whirlpool. SHA-2 refers to functions SHA224, SHA256, SHA384 and SHA512 (*SHA256, SHA384, SHA512 and SHA-3* at high level of assurance).		

5.2 Interoperability

2 Interoperability

KEY PROVISIONS

Identification Act, 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 assess whether the identification service meets the requirements on interoperability, information security, data protection and other reliability laid down in this Act.

…

M72, section 15: Assessment criteria
The identification service assessment shall cover the requirements concerning the following:
1) certain properties of the functions affecting the provision of the identification service (the identification scheme), namely:

Finnish Transport and Communications Agency Traficom
Erik Palménin aukio 1
P.O. Box 313
FI-00059 TRAFICOM
Tel. +358 295 390 100
www.traficom.fi

d) technical measures

Identification Act, section 12 a
...
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.
...

M72, section 12: Minimum set of data to be relayed in a trust network

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

1) in identification events concerning natural persons: at least the first name, family name, date of birth and the unique identifier of the person;
2) in identification events concerning legal persons: at least the first name, family name and the unique identifier of the natural person representing the legal person as well as the unique identifier of the organisation; and
3) an indication of whether the level of assurance is substantial or high.

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

1) an indication of whether the identification event concerns a public administration eService or a private eService;
2) in identification events concerning natural persons: forename(-s) and surname(s) at the time of birth, place of birth, current address and gender;
3) in identification events concerning legal persons:
a) current address;
b) VAT registration number;
c) tax reference number;

Finnish Transport and Communications Agency Traficom

Erik Palménin aukio 1
P.O. Box 313
FI-00059 TRAFICOM
Tel. +358 295 390 100
www.traficom.fi

d) the identifier related to Article 3(1) of Directive 2009/101/EC of the European Parliament and of the Council[9];
e) Legal Entity Identifier (LEI) referred to in Commission Implementing Regulation (EU) No 1247/2012[10];
f) The Economic Operator Registration and Identification (EORI) referred to in Commission Implementing Regulation (EU) No 1352/2013[11]; and
g) excise number provided in Article 2(12) of Council Regulation (EC) No 389/2012[12].

M72, section 14: Data transfer protocol and other requirements

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

M72, section 25: Transitional provisions and entry into force

[…]

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

[9] Directive 2009/101/EC of the European Parliament and of the Council of 16 September 2009 on coordination of safeguards which, for the protection of the interests of members and third parties, are required by Member States of companies within the meaning of the second paragraph of Article 48 of the Treaty, with a view to making such safeguards equivalent (OJ L 258, 1.10.2009, p. 11).
[10] Commission Implementing Regulation (EU) No 1247/2012 of 19 December 2012 laying down implementing technical standards with regard to the format and frequency of trade reports to trade repositories according to Regulation (EU) No 648/2012 of the European Parliament and of the Council on OTC derivatives, central counterparties and trade repositories (OJ L 352, 21.12.2012, p. 20).
[11] Commission Implementing Regulation (EU) No 1352/2013 of 4 December 2013 establishing the forms provided for in Regulation (EU) No 608/2013 of the European Parliament and of the Council concerning customs enforcement of intellectual property rights (OJ L 341, 18.12.2013, p. 10).
[12] Council Regulation (EU) No 389/2012 of 2 May 2012 on administrative cooperation in the field of excise duties and repealing Regulation (EC) No 2073/2004 (OJ L 121, 8.5.2012, p. 1).

Finnish Transport and Communications Agency Traficom
Erik Palménin aukio 1
P.O. Box 313
FI-00059 TRAFICOM
Tel. +358 295 390 100
www.traficom.fi

NO.	LEVEL OF ASSURANCE	REQUIREMENT PERTAINING TO THE IDENTIFICATION SERVICE (SUMMARY)	PROVISIONS	STANDARD REFERENCE	NOTES
17.	S, H	The identification service provider offers at least one interface in the trust network that complies with a widely accepted 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; 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,		**Application:** The Finnish Transport and Communications Agency has provided recommended profiles for the SAML and Open IDConnect protocols taking into account recommendations given by the trust network collaboration group. 212/2018 S Finnish Trust Network SAML 2.0 Protocol Profile version 1.0 213/2018 S Finnish Trust Network OpenID Connect 1.0 Protocol Profile version 1.0 The recommendations are available online at https://www.kyberturvallisuuskeskus.fi/en/electronic-identification

			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.		
18.	S, H	The identification means provider offers the required information (attributes) for the identification of **natural persons**.	**M72, section 12: Minimum set of data to be relayed in a trust network** The following minimum set of data shall be relayed at the interface between the identification means provider and the provider of an identification broker service: 1) in identification events concerning natural persons: at least the first name, family name, date of birth and the unique identifier of the person; … 3) an indication of whether the level of assurance is substantial or high.		
19.	S, H	The identification means provider has the required **planned capacity** to provide the optional data for the identification of **natural persons**.	**M72, section 12: Minimum set of data to be relayed in a trust network** Subsection 2:		MPS72, justification of section 12.1, page 59: Being prepared to relay non-mandatory attributes means that

Finnish Transport and Communications Agency Traficom

Erik Palménin aukio 1
P.O. Box 313
FI-00059 TRAFICOM
Tel. +358 295 390 100
www.traficom.fi

			The interface between the identification means provider and the provider of an identification broker service must enable the relay of the following information: 1) an indication of whether the identification event concerns a public administration eService or a private eService; 2) in identification events concerning natural persons: forename(s) and surname(s) at the time of birth, place of birth, current address and gender; …		the processing of non-mandatory attributes in the interface and identification systems 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 non-mandatory attributes in systems is not required. However, in the technical configurations, it should be ensured that the non-mandatory 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.
20.	S, H	The identification means provider offers the required information (attributes) for the identification of **legal persons**.	**M72, section 12: Minimum set of data to be relayed in a trust network** The following minimum set of data shall be relayed at the interface between the identification means provider and the provider of an identification broker service:		Only if strong electronic identification of legal persons is offered.

Finnish Transport and Communications Agency Traficom

Erik Palménin aukio 1
P.O. Box 313
FI-00059 TRAFICOM
Tel. +358 295 390 100
www.traficom.fi

			… 2) in identification events concerning legal persons: at least the first name, family name and the unique identifier of the natural person representing the legal person as well as the unique identifier of the organisation; and 3) an indication of whether the level of assurance is substantial or high.		
21.	S, H	The identification means provider has the required planned capacity to provide the optional data for the identification of **legal persons**.	**M72, section 12: Minimum set of data to be relayed in a trust network** The interface between the identification means provider and the provider of an identification broker service must enable the relay of the following information: 1) an indication of whether the identification event concerns a public administration eService or a private eService; … 3) in identification events concerning legal persons: a) current address; b) VAT registration number; c) tax reference number;		

Finnish Transport and Communications Agency Traficom

Erik Palménin aukio 1
P.O. Box 313
FI-00059 TRAFICOM
Tel. +358 295 390 100
www.traficom.fi

			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.		

5.3 Technical information security requirements

3 Technical information security requirements

KEY PROVISIONS

M72A, section 15: Assessment criteria
The identification service assessment shall cover the requirements concerning the following:
1) certain properties of the functions affecting the provision of the identification service (the identification scheme), namely:
d) technical measures

Identification Act, section 8: Requirements posed on the electronic identification scheme

4) the identification system is secure and reliable so that the requirements set down for (at minimum) substantial level of assurance in sections... 2.4.6 of the LOA Regulation for electronic identification are fulfilled taking into consideration taking into consideration the relevant technical threats to data security.

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.

M72, section 5: Technical information security measures of the identification scheme

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

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

Finnish Transport and Communications Agency Traficom
Erik Palménin aukio 1
P.O. Box 313
FI-00059 TRAFICOM
Tel. +358 295 390 100
www.traficom.fi

d) management of software vulnerabilities
e) backup copies

Production network together with its control connections referred to subsection 1(1)(e) and remote access and remote management referred to in subsection (1)(3)(c) above must be implemented in such a way that the information security threats caused by other services of the organisation such as e-mail or web browsing, or information security threats caused by other functions than those essential to management in a terminal used for the management, are

a) at substantial assurance level specifically assessed and minimised, and
b) at high level of assurance prevented when assessed as a whole.

5.3.1 Security of data communication

3.1 Security of data communication

No.	Level of assurance	REQUIREMENT PERTAINING TO THE IDENTIFICATION SERVICE (SUMMARY)	Provisions	Standard reference	Notes
22.	S, H	Security of data communication: The **data communication connections, control connections and processes** (data	**M72A, section 5: Technical information security measures of the identification scheme**	A.8.1.1 Inventory of assets	The overall architecture of the identification scheme must ensure

		communications of subprocesses related to the production of identification services, including the administration of the service) and their **security policies** are **identified and documented**. 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.	The identification scheme shall be designed, implemented and maintained to take into account the following aspects of the scheme: 4) telecommunication security a) structural network security b) Segmenting of the communication network **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.13.1 Communications security / Network security management: A.13.1.1 Network controls A.13.1.3 Segregation in networks	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/**audit 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.
23.	S, H	Security of data communication: **The data communication equipment** and **systems** of the identification scheme	**M72A, section 5: Technical information security measures of the identification scheme**	A.8.1.1 Inventory of assets	

Finnish Transport and Communications Agency Traficom
Erik Palménin aukio 1
P.O. Box 313
FI-00059 TRAFICOM
Tel. +358 295 390 100
www.traficom.fi

		(*existing assets* in the old criteria) are identified and documented.	The identification scheme shall be designed, implemented and maintained to take into account the following aspects of the scheme: 1) telecommunication security a) structural network security		
24.	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.	**M72A, section 5: Technical information security measures of the identification scheme** The identification scheme shall be designed, implemented and maintained to take into account the following aspects of the scheme: 1) telecommunication security a) structural network security b) Segmenting of the communication network	A.12.1.4 Operations security: Separation of development, testing and production environments	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.
25.	S, H	Security of data communication: The data communication connections of the identification scheme are **filtered** based on the least privilege principle.	**M72A, section 5: Technical information security measures of the identification scheme** The identification scheme shall be designed, implemented and maintained to take into account the following aspects of the scheme: 1) telecommunication security c) filtering rules according to the principle of least privilege	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*.	
26.	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.	**M72A, section 5: Technical information security measures of the identification scheme** The identification scheme shall be designed, implemented and maintained to take into account the following aspects of the scheme: 1) telecommunication security a) structural network security c) filtering rules according to the principle of least privilege	See previous row.	Any other links except those necessary for operations are expressly prohibited or must be closed.

27.	S, H	Security of data communication: **Cryptographic key materials** and **metadata** is exchanged safely between the identification services and the relying parties.	**M72A, section 8: Information security requirements concerning the interface between an identification means provider and an identification broker service provider** In identifying the parties and in relaying the data necessary for identification, metadata or similar procedures that ensure a corresponding level of information security shall be used. Cf. **M72A, sections 7–9 on message-level encryption requirements.** Cf. **LOA, 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. Cf. **LOA, 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	A.10.1.2 Cryptography / Key management	Cf. PSD2/RTS eIDAS art45 or eSeal certificate requirements for the identification of the parties. Should the key management policies of each level of assurance be defined separately? For practical reasons, the first key exchange and repeated key exchanges (especially with the relying parties) may need to be planned differently; however, both must be secure. Guideline 211/2016 contained the following informative observations: The policy takes into account the protection of encryption keys throughout their lifecycle. The processes and practices of private key management are documented and appropriately implemented.

Finnish Transport and Communications Agency Traficom

Erik Palménin aukio 1
P.O. Box 313
FI-00059 TRAFICOM
Tel. +358 295 390 100
www.traficom.fi

			communication by an attacker with enhanced-basic attack potential can subvert the authentication mechanisms.		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)
28.	H	Security of data communication: Cryptographic key materials and metadata are exchanged safely between the identification services and the relying parties.	Cf. above and **LOA 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 potential can subvert the authentication mechanisms.	A.10.1.2 Cryptography / Key management	Should the key management policies of each level of assurance be defined separately? For practical reasons, the first key exchange and repeated key exchanges (especially with the relying parties) may need to be planned differently; however, both must be secure.
29.	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.	The identification scheme shall be designed, implemented and maintained to take into account the following aspects of the scheme: 1) telecommunication security d) administration of the entire life cycle of the filtering and control systems	A.13.1 Communications security / Network security management:	

Finnish Transport and Communications Agency Traficom

Erik Palménin aukio 1
P.O. Box 313
FI-00059 TRAFICOM
Tel. +358 295 390 100
www.traficom.fi

				A.13.1.1 Network controls	
30.	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 in a terminal used for the management are **assessed and minimised** in the remote operation and administration of the identification scheme.	**M72A, section 5: Technical information security measures of the identification scheme** The identification scheme shall be designed, implemented and maintained to take into account the following aspects of the scheme: 1) telecommunication security e) control connections 3) operator security c) remote access and remote management Production network together with its control connections referred to subsection 1(1)(e) and remote access and remote management referred to in subsection (1)(3)(c) above must be implemented in such a way that the information security threats caused by other services of the organisation such as e-mail or web browsing, or information security threats caused by other functions than those essential to management in a terminal used for the management, are a) at substantial assurance level specifically assessed and minimised, and	A.9.4. System and application access control: A.9.4.1 Information access restriction A.9.4.4 Use of privileged utility programmes A.13.1.3 Network controls: Segregatio	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 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.

				n in networks	
31.	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 administration of the identification scheme (production network).	**M72A, section 5: Technical information security measures of the identification scheme** The identification scheme shall be designed, implemented and maintained to take into account the following aspects of the scheme: 1) telecommunication security e) control connections 3) operator security c) remote access and remote management **M72A, section 5: Technical information security measures of the identification scheme** Production network together with its control connections referred to paragraph 1(1)(e) and remote access and remote management referred to in paragraph (1)(3)(c) above must be implemented in such a way that the information security threats caused by other services of the organisation such as e-mail or web browsing, or information security threats caused by other functions than those essential to management in a terminal used for the management, are …	See previous row.	

Finnish Transport and Communications Agency Traficom

Erik Palménin aukio 1
P.O. Box 313
FI-00059 TRAFICOM
Tel. +358 295 390 100
www.traficom.fi

			b) at high level of assurance prevented when assessed as a whole. **MPS72 Explanatory Notes:** At the high level of assurance, the requirements in section 5(2) 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.		

5.3.2 Information system security

3.2 Information system security					
NO.	**LEVEL OF ASSURANCE**	**REQUIREMENT PERTAINING TO THE IDENTIFICATION SERVICE (SUMMARY)**	**PROVISIONS**	**STANDARD REFERENCE**	**NOTES**
32.	S, H	Information system security: The **information systems and processes** of the identification scheme (including processes related to the production and the administration of the identification service that use these information systems) are **identified and documented.** The information systems of the identification scheme are **classified** based on the 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	**M72A, section 5: Technical information security measures of the identification scheme** The identification scheme shall be designed, implemented and maintained to take into account the following aspects of the scheme: 2) computer security a) access rights control b) identification of the users of the scheme	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.

33.	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.	**M72A, section 5: Technical information security measures of the identification scheme** The identification scheme shall be designed, implemented and maintained to take into account the following aspects of the scheme: 2) computer security a) access rights control b) identification of the users of the scheme	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.

Finnish Transport and Communications Agency Traficom

Erik Palménin aukio 1
P.O. Box 313
FI-00059 TRAFICOM
Tel. +358 295 390 100
www.traficom.fi

34.	S, H	Information system security: The users (admins) of the information systems of the identification schemes **are identified** using a technique or method that is known and considered safe.	**M72A, section 5: Technical information security measures of the identification scheme** The identification scheme shall be designed, implemented and maintained to take into account the following aspects of the scheme: 2) computer security a) access rights control b) identification of the users of the scheme	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 accounts are a requirement.
35.	S, H	Information system security: Access privileges are controlled and **maintained so they are up to date**.	**M72A, section 5: Technical information security measures of the identification scheme** The identification scheme shall be designed, implemented and maintained to take into account the following aspects of the scheme: 2) computer security a) access rights control b) identification of the users of the scheme	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	
36.	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).	**M72A, section 5: Technical information security measures of the identification scheme** The identification scheme shall be designed, implemented and maintained to take into account the following aspects of the scheme: 2) computer security a) access rights control b) identification of the users of the scheme		For example, the possibility of a dishonest or negligent employee granting an identification method 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 method.

37.	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.	**M72A, section 5: Technical information security measures of the identification scheme** The identification scheme shall be designed, implemented and maintained to take into account the following aspects of the scheme: 2) computer security c) hardening of the scheme	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.
38.	S, H	Information system security: Identification, prevention and correction of adverse impact and threats caused by **malware** is ensured.	**M72A, section 5: Technical information security measures of the identification scheme** The identification scheme shall be designed, implemented and maintained to take into account the following aspects of the scheme: 2) computer security d) malware protection	A.12.2 Protection from malware A.12.6 Technical vulnerability management	See also incident observation capacity.

Finnish Transport and Communications Agency Traficom

Erik Palménin aukio 1
P.O. Box 313
FI-00059 TRAFICOM
Tel. +358 295 390 100
www.traficom.fi

39.	S, H	Information system security: The identification scheme uses up to date and secure **encryption solutions**.	**M72A, section 5: Technical information security measures of the identification scheme** The identification scheme shall be designed, implemented and maintained to take into account the following aspects of the scheme: 2) computer security g) internationally or nationally recommended encryption solutions in other respects than those laid down in section 7	A.10.1 Cryptographic controls A.18.1.5 Regulation of cryptographic controls	The MPS72 mentions the following sources: SOGIS-MRA NCSA-FI NIST Enisa SANS 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)
40.	S, H	Information system security: Cryptographic materials are protected over their entire lifecycle.	**LOA, 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	A.8.2.1 Classification of information	Guideline 211/2016 included the following observations, which are included here for reference:

Finnish Transport and Communications Agency Traficom

Erik Palménin aukio 1
P.O. Box 313
FI-00059 TRAFICOM
Tel. +358 295 390 100
www.traficom.fi

			access. It shall be ensured that such material is never persistently stored in plain text. Sensitive cryptographic material, if used for issuing electronic identification means and authentication, is protected from tampering. **M72A, section 5: Technical information security measures of the identification scheme** The identification scheme shall be designed, implemented and maintained to take into account the following aspects of the scheme: 2) computer security a) access rights control b) identification of the users of the scheme g) internationally or nationally recommended encryption solutions in other respects than those laid down in section 7 3) operator security b) processing environment for confidential materials	A.10.1.1 Policy on the use of cryptographic controls A.10.1.2 Key management	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 old or revealed keys and the prevention of unauthorised key exchanges. KATAKRI 2015 (I12)

5.3.3 Operator security

3.3 Operator security

NO.	LEVEL OF ASSURANCE	REQUIREMENT PERTAINING TO THE IDENTIFICATION SERVICE (SUMMARY)	PROVISIONS	STANDARD REFERENCE	NOTES
41.	**S, H**	Operator security: management of changes in the identification scheme is planned and careful.	**M72A, section 5: Technical information security measures of the identification scheme** The identification scheme shall be designed, implemented and maintained to take into account the following aspects of the scheme: 3) operator security 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 processes: System change	Clear processes have been defined for change management.

Finnish Transport and Communications Agency Traficom

Erik Palménin aukio 1
P.O. Box 313
FI-00059 TRAFICOM
Tel. +358 295 390 100
www.traficom.fi

				control procedures A.14.2.3 Technical review of applications after operating platform changes A.14.2.4 Restrictions on changes to software packages	
42.	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.	**M72A, section 5: Technical information security measures of the identification scheme** The identification scheme shall be designed, implemented and maintained to take into account the following aspects of the scheme: 3) operator security c) management of software vulnerabilities	A.12.5.1 Operations security: Installation of software on operational systems	Guideline 211/2016 included the following observations, which are included here for reference: The organisation shall have a method for monitoring general vulnerabilities. Software used in the identification scheme shall comply with the

Finnish Transport and Communications Agency Traficom

Erik Palménin aukio 1
P.O. Box 313
FI-00059 TRAFICOM
Tel. +358 295 390 100
www.traficom.fi

				A.12.6.1 Operations security: Management of technical vulnerabilities A.14.2 System acquisition, development and maintenance / Security in development and support processes A.14.2.1 Secure development policy A.14.2.2 System change	principles of secure programming.

Finnish Transport and Communications Agency Traficom

Erik Palménin aukio 1
P.O. Box 313
FI-00059 TRAFICOM
Tel. +358 295 390 100
www.traficom.fi

				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	

Finnish Transport and Communications Agency Traficom

Erik Palménin aukio 1
P.O. Box 313
FI-00059 TRAFICOM
Tel. +358 295 390 100
www.traficom.fi

				development environment A.14.2.7 Outsourced development A.14.2.8 System security testing A.14.2.9 System acceptance testing	
43.	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.	**M72A, section 5: Technical information security measures of the identification scheme** The identification scheme shall be designed, implemented and maintained to take into account the following aspects of the scheme: 3) operator security d) backup copies	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.

Finnish Transport and Communications Agency Traficom

Erik Palménin aukio 1
P.O. Box 313
FI-00059 TRAFICOM
Tel. +358 295 390 100
www.traficom.fi

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

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

KEY PROVISIONS

M72A, section 15: Assessment criteria
The identification service assessment shall cover the requirements concerning the following:
1) certain properties of the functions affecting the provision of the identification service (the identification scheme), namely:
d) technical measures

General requirements

Identification Act, section 8: Requirements posed on the electronic identification scheme

4) the identification system is secure and reliable so that the requirements set down for (at minimum) substantial level of assurance in sections... 2.4.6 of the LOA Regulation for electronic identification are fulfilled taking into consideration taking into consideration the relevant technical threats to data security.

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.

Finnish Transport and Communications Agency Traficom

Erik Palménin aukio 1
P.O. Box 313
FI-00059 TRAFICOM
Tel. +358 295 390 100
www.traficom.fi

Identification Act, 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, data 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.

…

The requirements are specified in M72, sections 5 and 11.

NO.	LEVEL OF ASSURANCE	REQUIREMENT PERTAINING TO THE IDENTIFICATION SERVICE (SUMMARY)	PROVISIONS	STANDARD REFERENCE	NOTES
44.	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-related incidents also in retrospect.	**M72, section 5: Technical information security measures of the identification scheme** The identification scheme shall be designed, implemented and maintained to take into account the following aspects of the scheme: 1) telecommunication security d) administration of the entire life cycle of the filtering and control systems 2) computer security e) tracing security events f) Security incident observation capability and recovery	A.12.4.1 Operations security: Event logging A.12.4.2 Operations security: Protection of log information	

Finnish Transport and Communications Agency Traficom

Erik Palménin aukio 1
P.O. Box 313
FI-00059 TRAFICOM
Tel. +358 295 390 100
www.traficom.fi

		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.12.4.3 Operations security: 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	

Finnish Transport and Communications Agency Traficom

Erik Palménin aukio 1
P.O. Box 313
FI-00059 TRAFICOM
Tel. +358 295 390 100
www.traficom.fi

				A.16.1.6 Learning from information security incidents	
45.	S, H	The **control logs** of the identification scheme are defined and separated from other log data. Their integrity is ensured.	**Requirements concerning the information security maintenance of the identification scheme are set out in Identification Act, section 8 and LoA, section 2.4.6.** **M72, section 5: Technical information security measures of the identification scheme** The identification scheme shall be designed, implemented and maintained to take into account the following aspects of the scheme: 1) telecommunication security d) administration of the entire life cycle of the filtering and control systems 2) computer security e) tracing security events f) Security incident observation capability and recovery	A.12.4.1 Operations security: Event logging A.12.4.2 Operations security: Protection of log information A.12.1.4 Separation of developme nt, testing and operational	Information on changes implemented in the identification scheme are saved in control logs.

Finnish Transport and Communications Agency Traficom

Erik Palménin aukio 1
P.O. Box 313
FI-00059 TRAFICOM
Tel. +358 295 390 100
www.traficom.fi

				environments	
46.	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.	**M72, section 5: Technical information security measures of the identification scheme** The identification scheme shall be designed, implemented and maintained to take into account the following aspects of the scheme: 1) telecommunication security d) administration of the entire life cycle of the filtering and control systems 2) computer security f) Security incident observation capability and recovery	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	Guideline 211/2016 included the following observations, which are included here for reference: All observations are discussed and their impact is classified according to predetermined criteria.

				weaknesses A.16.1.4 Assessment and decision on information security events	
		Corrective actions required by irregularities and malfunctions of the identification scheme are systematic and effective. Planning of the continuity of operations includes preventive and corrective actions that are used to minimise the impact of significant malfunctions or exceptional events.	**M72, section 5: Technical information security measures of the identification scheme** The identification scheme shall be designed, implemented and maintained to take into account the following aspects of the scheme: 1) telecommunication security d) administration of the entire life cycle of the filtering and control systems 2) computer security f) Security incident observation capability and recovery	A.16.1 Information security incident management / Management of information security incidents, events and weaknesses: A.16.1.5 Response to	Service level agreements (SLA) are contractual matters. Their non-discriminatory nature must be ensured.

				information security incidents	
47.	S, H	The incident management processes feature a **requirement to report to other identification services within the trust network.**	**Identification Act, 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, data 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. 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 information that is significant or processing personal data illegally.	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.

Finnish Transport and Communications Agency Traficom

Erik Palménin aukio 1
P.O. Box 313
FI-00059 TRAFICOM
Tel. +358 295 390 100
www.traficom.fi

			… **Application:** The trust network collaboration group has drafted a joint policy for malfunction situations requiring mutual notification as well as notification thresholds.		
48.	S, H	The incident management process features a **requirement to notify users and relying parties**.	**Identification Act, 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, data 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.

Finnish Transport and Communications Agency Traficom

Erik Palménin aukio 1
P.O. Box 313
FI-00059 TRAFICOM
Tel. +358 295 390 100
www.traficom.fi

49.	S, H	The incident management process features a requirement to notify the **Finnish Transport and Communications Agency**.	**Identification Act, 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, data 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. **M72, section 11: Disturbance notifications by the identification service provider to FICORA [Traficom]** Notifications of a significant threats or disturbances provided to FICORA in accordance with section 16 of the Identification and Trust Services Act shall contain at least the following information: 1) the identification means or the broker service affected by the disturbance; 2) description of the disturbance and its known reasons;	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.

Finnish Transport and Communications Agency Traficom

Erik Palménin aukio 1
P.O. Box 313
FI-00059 TRAFICOM
Tel. +358 295 390 100
www.traficom.fi

			3) description of the impact of the disturbance, including the impact on the issuance of new identification means, their users, relying parties, other parties of the trust network, and cross-border operations; 4) description of corrective measures; and 5) description of the provision of information on the disturbance to relying parties, identification means holders and the trust network as well as information on notifying other authorities. In assessing the significance of a disturbance, the disturbance is deemed more significant if it relates to incorrectness or abuse of electronic identity or to an information security threat or disturbance that compromises the integrity and reliability of identification. The disturbance is also deemed more significant if it affects a trust network. **MPS72 Explanatory Notes, justification to notification threshold to FICORA** (section 11): Section 11(2) defines, at a general level, the factors deemed relevant in judging the significance of the disturbance, 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 - disclosures of the identification means provider's certificate signature keys - serious abuse of identification means, such as incidents related to the chaining of credentials - serious internal misconduct. The threshold for deeming irregularities or abuse related to electronic identities significant is very low, and the same applies to vulnerabilities or irregularities 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.		

5.5 Storage and handling of data

5 Storage and handling of data

M72A, section 15: Assessment criteria
The identification service assessment shall cover the requirements concerning the following:
1) certain properties of the functions affecting the provision of the identification service (the identification scheme), namely:
b) record keeping
d) technical measures

General requirements

Identification Act, 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 Level of Assurance Regulation on Electronic Identification. Moreover, the identification service provider shall have in place an effective plan for terminating the identification service. (533/2016)

…
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.

Identification Act, 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 …and 2.4.6 of the Annex to the Level of Assurance Regulation on 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.

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

Finnish Transport and Communications Agency Traficom

Erik Palménin aukio 1
P.O. Box 313
FI-00059 TRAFICOM
Tel. +358 295 390 100
www.traficom.fi

NO.	LEVEL OF ASSURANCE	REQUIREMENT PERTAINING TO THE IDENTIFICATION SERVICE (SUMMARY)	PROVISIONS	STANDARD REFERENCE	NOTES
50.	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. Sensitive cryptographic material, if used for issuing electronic identification means and authentication, is protected from tampering.	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 transaction information, personal data, business secrets and information related to system security into account.

Finnish Transport and Communications Agency Traficom

Erik Palménin aukio 1
P.O. Box 313
FI-00059 TRAFICOM
Tel. +358 295 390 100
www.traficom.fi

51.	S, H	Planning of information management takes the entire **lifecycle** of the information into account. Information **retention times** are defined.	**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 security breaches, and retention, after which the records shall be securely destroyed.	A.18.1.4 Compliance / Compliance with legal and contractual requirements: Privacy and protection of personally identifiable information	Matters such as traceability of security-related events and needs arising from the *corresponding* processing principles specified in section 24 of the Identification Act need to be taken into account. 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.
52.	S, H	Compliance with the **specific data retention obligations specified in section 24 of the Identification Act** is ensured.	**Identification Act 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 identification event and an electronic signature; 2) data on potential 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	A.12.4.1 Operations security: Event logging	"*…only issues identification devices*" in the Act refers to identification services such as the Population Register Centre certificate where the provider of the identification device does not relay identification messages in an identification event.

			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 identification event. Other data referred to 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 identification event shall be destroyed after the event, unless they are required to be kept to verify an individual identification 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, as well as upon request by the service provider using identification service or the holder of the identification means. The identification service provider shall store data on processing the event, 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;		

Finnish Transport and Communications Agency Traficom

Erik Palménin aukio 1
P.O. Box 313
FI-00059 TRAFICOM
Tel. +358 295 390 100
www.traficom.fi

			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.		
53.	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 transactions and processing related to the identification service are given in section 24 of the Identification Act.** **Identification Act, 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, as well as upon request by the service provider using identification service or the holder of the identification means. The identification service provider shall store data on processing the event, the time, reason, and person processing it. …	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.
54.	S, H	**Technical measures are taken to ensure the integrity and confidentiality of the information that is processed and stored** in the identification scheme.	**Identification Act, 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 …and 2.4.6 of the Annex to the Level of Assurance Regulation on Electronic	A.9.1.1 Access control policy A.9.1.2 Access to networks	Data encryption and/or access control Separation as required (cf. especially cryptographic material) Backup copies/recoverability

Finnish Transport and Communications Agency Traficom
Erik Palménin aukio 1
P.O. Box 313
FI-00059 TRAFICOM
Tel. +358 295 390 100
www.traficom.fi

			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. Sensitive cryptographic material, if used for issuing electronic identification means and authentication, is protected from tampering. **M72, Section 5: Technical information security measures of the identification scheme** The identification scheme shall be designed, implemented and maintained to take into account the following aspects of the scheme: 3) operator security b) processing environment for confidential materials d) backup copies	and network services A.10.1.1 Policy on the use of cryptographic controls A.12.4.2 Operations security: Protection of log information	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.

Finnish Transport and Communications Agency Traficom

Erik Palménin aukio 1
P.O. Box 313
FI-00059 TRAFICOM
Tel. +358 295 390 100
www.traficom.fi

			M72, section 7: Encryption requirements of the identification scheme and interfaces […] The following methods shall be used in the encryption, key exchange and signcryption: **1) Key exchange:** In key exchange, DHE methods or ECDHE methods with elliptic curves shall be used. The size of the finite field to be used in calculations shall be at least 2048 bits in DHE and at least 224 bits in ECDHE. **2) Signature:** When using the RSA for electronic signatures, the key length shall be at least 2048 bits. When using the elliptic curve method ECDSA, the underlying field size shall be at least 224 bits. **3) Symmetrical encryption:** The encryption algorithm shall be AES or Serpent. The key length shall be at least 128 bits. The encryption mode shall be CBC, GCM, XTS or CTR. **4) Hash functions:** The hash function shall be SHA-2, SHA-3 or Whirlpool. SHA-2 refers to functions SHA224, SHA256, SHA384 and SHA512. […]		

Finnish Transport and Communications Agency Traficom

Erik Palménin aukio 1
P.O. Box 313
FI-00059 TRAFICOM
Tel. +358 295 390 100
www.traficom.fi

			The integrity and confidentiality of the identification scheme record keeping shall be ensured. If the data protection is only based on encryption, requirements laid out in paragraph 1 above concerning signatures, symmetrical encryption and hash functions shall apply. **MPS72 Explanatory Notes:** If protected information is kept in the schemes in such a manner that its confidentiality and/or integrity is only or mainly protected by cryptographic means, the methods specified in paragraph 1 shall be applied apart from key exchange requirements. They do not apply because key exchange is not typically used in disk encryption. Alternatively, careful access management, for instance, may also be used.		
55.	H	Strict/substantial-level encryption requirements as specified in the **recommendation** are followed in the processing and storage of data.	**MPS72, section B 7.2 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 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	See above.	Key exchange between the identification service and its subcontractors may be relevant here.

Finnish Transport and Communications Agency Traficom

Erik Palménin aukio 1
P.O. Box 313
FI-00059 TRAFICOM
Tel. +358 295 390 100
www.traficom.fi

			2048 (**3072** 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 ***15 to 21*** at high level of assurance) of IANA's IKEv2 specifications meet the above requirements. 2) **Signature**: When using the RSA for electronic signatures, the key length shall be at least 2048 (3072 at high level of assurance) bits. When using the elliptic curve method ECDSA, the underlying field size shall be at least 224 (256 at high level of assurance) bits. 3) **Symmetrical encryption**: The encryption algorithm shall be AES or Serpent *(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 shall be CBC, GCM, XTS or CTR. 4) **Hash functions**: The hash function shall be SHA-2, SHA-3 or Whirlpool. SHA-2 refers to functions SHA224, SHA256, SHA384 and SHA512 (*SHA256, SHA384, SHA512 and SHA-3* at high level of assurance).		
56.	S, H	All **media** containing personal, cryptographic or other sensitive information is stored,	**LOA Annex, section 2.4.6: Technical controls**	A.8.3 Asset management	Management, disposal and transfer.

		transported and disposed of in a safe and secure manner.	5) All media containing personal, cryptographic or other sensitive information are stored, transported and disposed of in a safe and secure manner.	/ Media handling A.11.2.6 Security of equipment and assets off-premises A.11.2.7 Secure disposal or re-use of equipment	

5.6 Security of physical premises

6. Security of physical premises
M72A, section 15: Assessment criteria The identification service assessment shall cover the requirements concerning the following: 1) certain properties of the functions affecting the provision of the identification service (the identification scheme), namely: c) facilities and […] **Identification Act, 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 Level of Assurance Regulation on Electronic Identification.

NO.	LEVEL OF ASSURANCE	REQUIREMENT PERTAINING TO THE IDENTIFICATION SERVICE (SUMMARY)	PROVISIONS	STANDARD REFERENCE	NOTES
57.	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 protect 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 the said facilities. The scope of other standards has not been established.
58.	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 protect against, damage caused by environmental events, unauthorised access and other factors that may impact the security of the service.	A.11.1.2 Physical entry controls A.11.1.3 Securing	

Finnish Transport and Communications Agency Traficom
Erik Palménin aukio 1
P.O. Box 313
FI-00059 TRAFICOM
Tel. +358 295 390 100
www.traficom.fi

		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.	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.	offices, rooms and facilities A.11.1.4 Protecting against external and environmental threats A.11.2.1 Equipment siting and protection A.11.2.3 Cabling security	
59.	S, H	Security perimeters are used to ensure that no **unauthorised** equipment or connections are used.	**LOA, section 2.4.5: Facilities and staff** 3. Facilities used for providing the service are continuously monitored for, and protect 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,	A.11 Physical and environmental security	

			cryptographic or other sensitive information is limited to authorised staff or subcontractors.		

5.7 Sufficiency and competence of human resources

7. Sufficiency and competence of human resources

M72A, section 15: Assessment criteria
The identification service assessment shall cover the requirements concerning the following:
1) certain properties of the functions affecting the provision of the identification service (the identification scheme), namely:
c) […] and staff

NO.	LEVEL OF ASSURANCE	REQUIREMENT PERTAINING TO THE IDENTIFICATION SERVICE (SUMMARY)	PROVISIONS	STANDARD REFERENCE	NOTES
60.	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.	**Identification Act, 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	A.7.2.2 Human resource security / During employment	Assessment - sufficiency of human resources considering the nature of the operations (24/7/365) - assessment of technical controls; no precise

			laid down for assurance level substantial in sections …and 2.4.5 of the Annex to the Level of Assurance Regulation on Electronic Identification. Moreover, the identification service provider shall have in place an effective plan for terminating the identification service. (533/2016) **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.	: Information security awareness, education and training	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).
61.	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	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.

				supplier relationships A.15.2.1 Monitoring and review of supplier services	

5.8 Information security management

8. Information security management

M72A, section 15: Assessment criteria
The identification service assessment shall cover the requirements concerning the following:
1) certain properties of the functions affecting the provision of the identification service (the identification scheme), namely:
a) information security management

Identification Act, 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 Assurance Level Regulation on Electronic Identification are met.
i

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
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
62.	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. The information security management system adheres to proven standards or principles for the management and control of information security risks.	A.5 Information security policies	ISO 27001 compliance without substantial deviations is considered proof of meeting the information security management requirements.

63.	S, H	The information security management system is based on a universally applied standard or set of standards.	**M72A, section 4: Information security management requirements of an identification service provider** The identification service provider shall apply the ISO/IEC 27001 standard or another corresponding, universally applied security management standard to the management of the information security of its identification scheme. Information security management may also be based on the combination of several standards.		The justifications of MPS72, section 4 are mapped to ISO 27001.
64.	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.	**M72A, section 4: Information security management requirements of an identification service provider** Information security management shall cover the following aspects concerning the provision of identification service: 1) the overall context of the identification service provider;	4 context of the organization	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.
65.	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.	**M72A, section 4: Information security management requirements of an identification service provider** Information security management shall cover the following aspects concerning the provision of identification service: 2) governance, organisation and maintenance of information security management	5 leadership 9.2 internal audit 9.3 management review	

		Information security responsibilities of the staff and the subcontractors are defined.		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	
66.	S, H	The information security management system covers the management of information security risks related to the offering of the identification service.	Information security management shall cover the following aspects concerning the provision of identification service: 3) management of information security risks related to the provision of the identification service;	Reference to MPS72: 6 planning	Mitigation is part of information security measures referred to above

Finnish Transport and Communications Agency Traficom

Erik Palménin aukio 1
P.O. Box 313
FI-00059 TRAFICOM
Tel. +358 295 390 100
www.traficom.fi

		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.			
67.	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 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;	MPS72: 7 support	

		Information security training given to the staff is regular and documented. Efficiency of the training is monitored.			
68.	S, H	The information security management system ensures that the offering of the 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 control of the provision of the identification service for the purpose of meeting information security requirements; and	MPS72: 8 operation A.18.1.1 Compliance / Compliance with legal and contractual requirements: Identification of applicable legislation and contractual requirements	Regulatory requirements for identification services Data protection regulation (as applicable) Contractual trust network provisions (as applicable)
69.	S, H	The information security management system features regular assessment of information security efficiency and functionality.	Information security management shall cover the following aspects concerning the provision of identification service: 6) evaluation of the efficiency and effectiveness of information security management.	MPS72: 9.1 Monitoring, measurement, analysis	How effective the information security management is concerning the factors, processes and problems that affect the information security of the identification scheme.

				and evaluation	

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

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

M72A, section 15: Assessment criteria
The identification service assessment shall cover the requirements concerning the following:
2) the identification method, meaning certain properties of the identification means, namely:
b) identity proofing and verification of the applicant

Identification Act, 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 *Level of Assurance Regulation on Electronic Identification*.
…

Finnish Transport and Communications Agency Traficom

Erik Palménin aukio 1
P.O. Box 313
FI-00059 TRAFICOM
Tel. +358 295 390 100
www.traficom.fi

Identification Act, 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 Assurance Level Regulation on Electronic Identification. The proofing of a person's identity may be based on a document by an authority showing the person's identity issued 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)

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.

Identification Act, section 17 a: Identifying a legal person applying for an identification means

Finnish Transport and Communications Agency Traficom

Erik Palménin aukio 1
P.O. Box 313
FI-00059 TRAFICOM
Tel. +358 295 390 100
www.traficom.fi

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 Level of Assurance Regulation on Electronic Identification

Identification Act, section 7 a: Using the data in the Business Information System

The provider of an identification device 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 purpose of offering identification services are up-to-date with the data in the Business Information System.

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

DEFINITIONS

Identification Act, section 2: Definitions

7) *initial identification* means the verification of the identity of the applicant for an identification means in connection with the acquisition 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;

Finnish Transport and Communications Agency Traficom

Erik Palménin aukio 1
P.O. Box 313
FI-00059 TRAFICOM
Tel. +358 295 390 100
www.traficom.fi

NO.	LEVEL OF ASSURANCE	REQUIREMENT PERTAINING TO THE IDENTIFICATION SERVICE (SUMMARY)	PROVISION	STANDARD	NOTES
Method 1 Initial identification is based on the presentation of an identity document approved in Finland					
70.	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.	**Identification Act, section 17** 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.
71.	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.	**Identification Act, section 17: Identifying a natural person applying for an identification means** In the case of an initial identification, a natural person shall be identified in person or in electronic format in such a manner that the requirements for a substantial or high assurance level laid down in section 2.1.2 of the Annex to the LOA Regulation are met. The verification of identity can be based on a document		

Finnish Transport and Communications Agency Traficom
Erik Palménin aukio 1
P.O. Box 313
FI-00059 TRAFICOM
Tel. +358 295 390 100
www.traficom.fi

		It is ensured that the identity document belongs to the person presenting the document.	proving the person's identity issued by an authority or a means of strong electronic identification as laid down in this Act. **LOA Annex , section 2.1.2** 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		

Finnish Transport and Communications Agency Traficom

Erik Palménin aukio 1
P.O. Box 313
FI-00059 TRAFICOM
Tel. +358 295 390 100
www.traficom.fi

			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;		
72.	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 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.	**Identification Act, 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 Assurance Level Regulation on Electronic Identification. The proofing of a person's identity may be based on a document by an authority showing the person's identity issued or a strong electronic identification means referred to in this Act. **LOA Annex, section 2.1.2** 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		See section 3.9 of this document.

Finnish Transport and Communications Agency Traficom

Erik Palménin aukio 1
P.O. Box 313
FI-00059 TRAFICOM
Tel. +358 295 390 100
www.traficom.fi

			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;		
73.	H	The identity document is presented, and its validity is ensured using a remote connection. The authenticity of the identification document is verified based on an	**LOA Annex, section 2.1.2 (High)** 1. Level substantial, plus one of the alternatives listed in points (a) to (c) has to be met: Where the person has been verified to be in possession of photo or biometric identification evidence		See section 3.9 of this document.

Finnish Transport and Communications Agency Traficom

Erik Palménin aukio 1
P.O. Box 313
FI-00059 TRAFICOM
Tel. +358 295 390 100
www.traficom.fi

		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.	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; and the applicant is identified as the claimed identity through comparison of one or more physical characteristic of the person with an authoritative source;		
74.	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 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;		Not a requirement but has an impact on risk assessment and may have impact liabilities. On the high level of assurance this requirement is mandatory.

Finnish Transport and Communications Agency Traficom

Erik Palménin aukio 1
P.O. Box 313
FI-00059 TRAFICOM
Tel. +358 295 390 100
www.traficom.fi

			Identification Act, 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.		
75.	S, H	The existence of the person is verified from the population register.	**Identification Act, 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. (533/2016) …		Applies to all initial identification procedures.
Method 2: initial identification using an electronic identification means					

Finnish Transport and Communications Agency Traficom

Erik Palménin aukio 1
P.O. Box 313
FI-00059 TRAFICOM
Tel. +358 295 390 100
www.traficom.fi

76.	S	Identity proofing is based on strong electronic identification means approved in the Identification Act.	**Identification Act, 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 Assurance Level Regulation on Electronic Identification. The proofing of a person's identity may be based on a document by an authority showing the person's identity issued or a strong electronic identification means referred to in this Act. ... **LOA Annex, section 2.1.2** 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		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.

Finnish Transport and Communications Agency Traficom

Erik Palménin aukio 1
P.O. Box 313
FI-00059 TRAFICOM
Tel. +358 295 390 100
www.traficom.fi

			body referred to in Article 2(13) of Regulation (EC) No 765/2008 or by an equivalent body.		
77.	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 (High)** 3. 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 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 a high level of assurance are registered in Traficom's register as required by the Identification Act.
Method 3: Initial identification based on identification carried out for another purpose ("existing customer")					
78.	S, H	Identify proofing relies on a procedure where an identity has been proven and verified earlier for purposes other than	**Identification Act, section 17: Identifying a natural person applying for an identification means**		The use of such an initial identification procedure is subject to express approval from the Finnish Transport and Communications

		issuing an electronic identification means. The procedure is based on regulations other than Identification Act or and 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.	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 Assurance Level Regulation on Electronic Identification. The proofing of a person's identity may be based on a document by an authority showing the person's identity issued 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 device, 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. **LOA Annex, section 2.1.2: Identity proofing and verification (natural person)** 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		Agency. Notification of such a procedure must be accompanied by a conformity assessment.

			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;		
Method 4: initial identification by the police.					
79.	S, H	If required, an initial identification should be performed by police.	**Identification Act, section 17** … 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 (High)** 3. 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.		

Finnish Transport and Communications Agency Traficom

Erik Palménin aukio 1
P.O. Box 313
FI-00059 TRAFICOM
Tel. +358 295 390 100
www.traficom.fi

5.10 Lifecycle of identification means (identification method)

10. Lifecycle of identification means (identification method)

M72A, section 15: Assessment criteria
The identification service assessment shall cover the requirements concerning the following:
2) the identification method, 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
g) […]

NO.	LEVEL OF ASSURANCE	REQUIREMENT PERTAINING TO THE IDENTIFICATION SERVICE (SUMMARY)	PROVISIONS	STANDARD	NOTES
80.	S, H	The identification is not connected to the person (personalised) before initial identification.	**M72A, section 6: Information security requirements of the identification method**		

Finnish Transport and Communications Agency Traficom
Erik Palménin aukio 1
P.O. Box 313
FI-00059 TRAFICOM
Tel. +358 295 390 100
www.traficom.fi

			An identification means shall not be connected to an applicant before the applicant has passed initial identification or it has been otherwise ensured in the process of granting an identification means that the identification means is not available before the initial identification referred to in section 17 of the Identification and Trust Services Act has been performed. […]		
81.	S, H	The personal information of a natural person is verified from a population data system upon the issuance of the identification means and then regularly during the validity of the identification means.	**Identification Act, section 7: Use of data stored in the Population Information System** The provider of an identification device 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 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, section 2.1.1: Application and registration.** 3. Appropriate identification data required for identity proofing is collected.

Finnish Transport and Communications Agency Traficom

Erik Palménin aukio 1
P.O. Box 313
FI-00059 TRAFICOM
Tel. +358 295 390 100
www.traficom.fi

			the Population Information System. (533/2016) … **See M72A, section 12: Minimum set of data to be relayed in a trust network.**		
82.	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.	**Identification Act, section 20: Issuance of an identification means** The issuance of an identification device 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, section 2.1.1: Application and registration.**		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 requirement specified in section of the Identification Act, and section 2.2.1 of the LOA requiring 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, according to which the identification service provider must ensure that the means of identification will not unlawfully end up in the possession of a third party when the means of identification is being released. See LOA Guidance: Possible mechanisms include: • delivery in person • delivery by registered mail

Finnish Transport and Communications Agency Traficom

Erik Palménin aukio 1
P.O. Box 313
FI-00059 TRAFICOM
Tel. +358 295 390 100
www.traficom.fi

			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. **Identification Act, 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 (device) is handed over, it does not become subject to unauthorized 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 Level of Assurance Regulation on Electronic Identification. **LOA Annex, section 2.2.2: Issuance, delivery and activation**		• 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.

			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.		
83.	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.	**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.		
84.	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.	**Identification Act, 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 (device) has been lost, is in the unauthorized possession of another person or of any unauthorized use immediately upon detection of this fact. (533/2016) The identification means provider shall provide an opportunity to submit a		Cf. (there is no reference to LOA 2.2.3 in the Identification Act; it is therefore applied formally only if 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 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.

			notification as set out in subsection 1 at any time. Upon receipt of the notification, the identification service provider shall immediately cancel the identification means or prevent its use. (533/2016) 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. (533/2016) The system shall be designed to allow a service provider using 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. A service provider using identification service shall check the systems and registers maintained by the identification		

			service provider for potential cancellations or restrictions to use in connection with the use of the identification means . However, no checking is needed, if the use of the identification means can be prevented or blocked by technical means. […] **Identification Act Section 26: Identification service provider's right to cancel or prevent the use of an identification means** In addition to the provisions of section 25, the identification service provider may cancel or prevent 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;		

Finnish Transport and Communications Agency Traficom

Erik Palménin aukio 1
P.O. Box 313
FI-00059 TRAFICOM
Tel. +358 295 390 100
www.traficom.fi

			3) the identification service provider has reason to believe that the safe use of the means is at risk; 4) the identification device holder is using the identification device contrary to the agreed terms of use; or 5) the identification means holder has died. The identification service provider shall notify the holder as soon as possible about the cancellation or prevention of use of the identification means, as well as the time of and reasons for such action. The identification service provider shall restore the ability to use the identification means or give the identification device holder a new device immediately after removal of reasons referred to in subsection 1 (2 and 3).		
85.	S, H	**Renewal and replacement of an identification means**	**Identification Act, section 22: Renewal of the identification means**		The verification requirement set out in section 8 of the Identification Act and section 2.2.1 of the LOA (the identification means is used only under the control or possession of the person to whom it

			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 of the Annex of the Level of Assurance Regulation on Electronic Identification. **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 based on a valid electronic identification means of the same, or higher, assurance level.		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. 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.
86.	H	**Renewal and replacement of an identification means**	**LOA Annex, section 2.2.4: Renewal and replacement** **High:**		

			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. Where renewal or replacement is based on a valid electronic identification means, the identity data is verified by an authoritative source.)		

Finnish Transport and Communications Agency Traficom

Erik Palménin aukio 1
P.O. Box 313
FI-00059 TRAFICOM
Tel. +358 295 390 100
www.traficom.fi

6 Annex C: Special criteria for mobile identification solutions

General

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

The first version of the criteria is created **primarily for the substantial level of assurance**. 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.

6.1 Architecture, design and threat modelling

Criterion	Justification	Additional information / comment
400. All app components are identified, classified and known to be needed.	LOA, section 2.4.6, point 1 Identification Act, 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 M72A, section 5.1, point 2c)	

Finnish Transport and Communications Agency Traficom

Erik Palménin aukio 1
P.O. Box 313
FI-00059 TRAFICOM
Tel. +358 295 390 100
www.traficom.fi

402. A high-level architecture for the mobile app and all connected remote services has been defined and security has been addressed in that architecture.	LOA, section 2.4.6, point 1 Identification Act, section (8)(1)(4)	
403. Data considered sensitive in the context of the mobile app is clearly identified.	LOA, section 2.4.4, point 1 LOA, section 2.4.6, points 1 and 3	
404. A threat model for the mobile app 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.
405. All security controls have a centralized implementation.	LOA, section 2.4.6, point 1	
406. 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	
407. The mobile app reports the operating system and application version number to the server, which has a mechanism for enforcing updates.	LOA, section 2.4.6, point 1 M72A, section 5.1, point 2c)	
408. An outdated mobile app prompts the user to update the operating system and/or mobile app to complete the transaction.	(LOA 2.1.1, point 2)	Best practice (BP). LOA 2.1.1 is not incorporated in the Identification Act.
409. Security is addressed within all parts of the software development lifecycle.	LOA 2.4.6, sections 1 and 4 Identification Act, section (8)(1)(4)	

Finnish Transport and Communications Agency Traficom

Erik Palménin aukio 1
P.O. Box 313
FI-00059 TRAFICOM
Tel. +358 295 390 100
www.traficom.fi

6.2 Data storage and privacy

Criterion	Justification	Additional information / comment
410. Security services and features offered by the platform are used appropriately to store sensitive data.	LOA 2.4.6, section 1, point 3	
411. The level of authentication currently performed is communicated clearly to the user [The right place for this requirement? A jointly agreed best practice on graphic elements that are used, for example.]	LOA, section 2.1.1, point 2	Recommended practice.
412. No sensitive data should be stored outside of the app container or system credential storage facilities.	LOA, section 2.4.6, point 1 M72A, section 5.1, paragraph 3b)	
413. No sensitive data is written to application logs.	LOA, section 2.4.6, point 1 M72A, section 5.1, paragraph 3b)	
414. No sensitive data is shared with third parties unless it is a necessary part of the architecture.	LOA, section 2.4.6, point 1 M72A, section 5.1, paragraph 3b)	
415. The keyboard cache is disabled on text inputs that process sensitive data.	LOA, section 2.4.6, point 1 M72A, section 5.1, paragraph 3b)	
416. No sensitive or secret data, such as passwords or pins is exposed through the user interface.	LOA, section 2.4.6, point 1	

Criterion	Justification	Additional information / comment
	M72A, section 5.1, paragraph 3b)	
417. The clipboard is deactivated on text fields that may contain sensitive data.	LOA, section 2.4.6, point 1 M72A, section 5.1, paragraph 3b)	
418. No sensitive data is exposed via IPC mechanisms.	LOA, section 2.4.6, point 1 M72A, section 5.1, paragraph 3b)	
419. 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 M72A, section 5.1, paragraph 3b)	
420. The app removes sensitive data from views when moved to the background.	LOA, section 2.4.6, point 1 M72A, section 5.1, paragraph 3b)	
421. The app does not hold sensitive data in memory longer than necessary, and memory is cleared explicitly after use.	LOA, section 2.4.6, point 1 M72A, section 5.1, paragraph 3b)	
422. The app 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.

Criterion	Justification	Additional information / comment
423. 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.

Finnish Transport and Communications Agency Traficom

Erik Palménin aukio 1
P.O. Box 313
FI-00059 TRAFICOM
Tel. +358 295 390 100
www.traficom.fi

6.3 Cryptography requirements

Criterion	Justification	Additional information / comment
424. The app does not rely on symmetric cryptography with hardcoded keys as a sole method of encryption.	M72A, section 5.1, paragraph 2g; M72A, section 7	
425. The app uses cryptographic primitives that are appropriate for the particular use-case and known to be good.	M72A, section 5.1, paragraph 2g	
426. The app does not use cryptographic protocols or algorithms that have expired or are widely considered depreciated for security purposes.	M72A, section 5.1, paragraph 2g	
427. The app doesn't re-use the same cryptographic key for multiple purposes.	LOA, section 2.4.6, point 1 Identification Act, section (8)(1)(4)	
428. All random values are generated using a sufficiently secure and high-quality random number generator.	LOA, section 2.4.6, point 1 Identification Act, section (8)(1)(4)	
429. The app 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	
430. The app does not include or use any hardcoded usernames or passwords.	LOA, section 2.4.6, point 1 M72A, sections 6.2 and 6.3	

Criterion	Justification	Additional information / comment
431. 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 M72A, section 5.1, paragraph 2g	

Finnish Transport and Communications Agency Traficom

Erik Palménin aukio 1
P.O. Box 313
FI-00059 TRAFICOM
Tel. +358 295 390 100
www.traficom.fi

6.4 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.

Criterion	Justification	Additional information / comment
432. The procedure used for the personalisation of the app 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, point 2	
433. 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 M72A, section 6, paragraph 3	Example: private key.
434. Secrets/identification keys are unique.	M72A, section 5.1, paragraph 2g)	
435. Asymmetric secrets that implement the identification are created in the mobile device (key pair, other secret key/secret).	M72A, section 5.1, paragraph 2g) M72A, section 5.1, paragraph 3b)	Cf. RTS.
436. 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 M72A, section 5.1, paragraph 3b)	Cf. RTS.

Criterion	Justification	Additional information / comment
437. Identification may not be based on a shared secret alone.	LOA, section 2.2.1, substantial, point 2	
438. 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 so that the secrets could be used in the other device.	LOA, section 2.2.1, substantial, point 2 M72A, section 6, paragraph 3	
439. The app 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	
440. If the app 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 M72A, section 5.1, paragraph 2g) M72A, section 7, paragraphs 1–4	

Finnish Transport and Communications Agency Traficom

Erik Palménin aukio 1
P.O. Box 313
FI-00059 TRAFICOM
Tel. +358 295 390 100
www.traficom.fi

Criterion	Justification	Additional information / comment
441. If personal information is exchanged between the app and the server, the information is protected using message-level encryption, too.	LOA, section 2.4.6, point 2 LOA, section 2.4.6, substantial M72A, section 5.1, paragraph 2g)	
442. If the app is based on or includes a method based on one-time passwords (OTP), the one-time passwords are generated using recommended, standard-based solutions.	M72A, section 5.1, paragraph 2g)	
443. The secret used for the identification is stored using services offered by the platform or hardware features, such as a device-level safe partition, or services offered by the operating system for storing sensitive information (such as keychain).	M72A, section 5.1, paragraph 2c) M72A, section 5.1, paragraph 3b)	
444. 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 must follow the same logic (PSD2, the 5-error rule).	LOA, section 2.4.6, point 1 M72A, section 5.1, paragraph 2f)	Cf. RTS and SCA. *[How about opening? Or identification saved on the operating system level, such as fingerprints?].*
445. Techniques that prevent replay attacks are used between the app 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	
446. 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	

Criterion	Justification	Additional information / comment
447. (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 M72A, section 7.1, paragraph 2	
448. Session or token validity is defined on the server side.	LOA, section 2.4.6, points 1 and 4	
449. 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	
450. 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.
451. 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.
452. If the app 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	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

Finnish Transport and Communications Agency Traficom

Erik Palménin aukio 1
P.O. Box 313
FI-00059 TRAFICOM
Tel. +358 295 390 100
www.traficom.fi

Criterion	Justification	Additional information / comment
combination would issue identification on. The combinations must be documented and assessed separately.		factor or adding a new category, which would result in authentication factors from three categories becoming available.
453. 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	
454. The implementation of a biometric authentication factor only uses interfaces offered by the platform.	LOA, section 2.4.6, point 1 M72A, section 5.1, paragraph 2c)	
455. When a biometric factor is used, the biometric record (fingerprint, facial recognition data, iris scan data) is not transferred outside the app.	LOA, section 2.2.1, substantial, point 2 LOA, section 2.3.1, substantial, point 2	
456. 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	

Finnish Transport and Communications Agency Traficom

Erik Palménin aukio 1
P.O. Box 313
FI-00059 TRAFICOM
Tel. +358 295 390 100
www.traficom.fi

Criterion	Justification	Additional information / comment
457. The user has the option to temporarily close the secret on a) one device, b) multiple devices and c) all devices at once.	LOA, section 2.2.3, substantial, point 1	
458. 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.	LOA, section 2.2.3, substantial, point 3	
459. The user must have an option to securely deactivate the identification app and secret on a) one device, b) multiple devices and c) all devices.	LOA, section 2.2.3, substantial, points 1 and 2	
460. Temporary, device-specific closing and removal of a secret must also be possible on the server side.	LOA, section 2.2.3, substantial, points 1 and 2	
461. 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.		Example: RTS, dynamic combination. EU 2018/389
462. The identification app 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	
463. If the response of the identification app 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	

Finnish Transport and Communications Agency Traficom

Erik Palménin aukio 1
P.O. Box 313
FI-00059 TRAFICOM
Tel. +358 295 390 100
www.traficom.fi

Criterion	Justification	Additional information / comment
464. The app guides the user to select strong PIN codes.	LOA, section 2.1.1, substantial, point 2 M72A, section 5.1, paragraph 2g)	LOA 2.1.1 is outside the scope of the Identification Act but is recommended practice.
465. The app 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	
466. User inputs, such as PIN codes, are validated in secure manner.	LOA, section 2.3.1, substantial, point 2 M72A, section 5.1, paragraph 3b)	
467. If the app uses hardware-level security features of the mobile device such as TEE and similar, the app indicates the hardware-level component that is used and makes other details available to the server in connection with initialisation so that the server can detect hardware-level vulnerabilities (also in the future).	LOA, section 2.4.6, point 1 M72A, section 5.1, paragraph 3d)	New, 29.4.2019: CVE-2018-11976 → Providing the server with an opportunity to react to known vulnerabilities in hardware-level components.

Finnish Transport and Communications Agency Traficom

Erik Palménin aukio 1
P.O. Box 313
FI-00059 TRAFICOM
Tel. +358 295 390 100
www.traficom.fi

6.5 Data communication

Criterion	Justification	Additional information / comment
468. The network traffic between the app and the server is protected using internationally or nationally recommended connection procedures. The secure channel is used consistently throughout the app.	LOA, section 2.4.6, point 2 M72A, section 5.1, paragraph 2g)	No encryption requirements have been set for the identification scheme's *internal* connections, but the data communication encryption policies defined in M72A, section 7 for use *between the parties* should be taken as the starting point.
469. The app checks that the TLS (or similar) settings are in line with current best practices.	LOA, section 2.4.6, point 2 M72A, section 5.1, paragraph 2g)	No encryption requirements have been set for the identification scheme's *internal* connections, but the data communication encryption policies defined in M72A, section 7 for use *between the parties* should be taken as the starting point.
470. The app uses hard-fail certificate pinning.	LOA, section 2.4.6, point 2	

Criterion	Justification	Additional information / comment
471. The app doesn't 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.
472. The app only depends on up-to-date connectivity and security libraries.	LOA 2.4.6, sections 1 and 4	

6.6 Platform interaction

Criterion	Justification	Additional information / comment
473. The app only requests the minimum set of permissions necessary.	LOA, section 2.4.6, point 1 M72A, section 5.1, paragraph 2c)	
474. All inputs form external sources are validated and sanitized.	LOA, section 2.4.6, point 4 M72A, section 5.1, paragraph 2c)	
475. The app does not export data via custom URL schemes or IPC mechanisms, unless these mechanisms are properly protected.	LOA, section 2.4.6, point 2	

Criterion	Justification	Additional information / comment
	M72A, section 5.1, paragraph 2c)	
476. WebViews are configured to allow only the minimum set of protocol handlers required. Other connection policies are blocked/confirmed as being disabled.	LOA, section 2.4.6, point 1 M72A, section 5.1, paragraph 2c)	
477. JavaScript is disabled in WebViews unless explicitly required.	LOA, section 2.4.6, point 1 M72A, section 5.1, paragraph 2c)	
478. Native methods are blocked in case the platform's software version has been found vulnerable.	LOA, section 2.4.6, point 1 M72A, section 5.1, paragraphs 2c) and 3d)	JavaScript implementations on old versions of the Android operating system, for example, may be unsecure.
479. If native methods of the app are exposed to a WebView, verify that the WebView only renders JavaScript contained within the app package.	LOA, section 2.4.6, point 1 M72A, section 5.1, paragraph 2c)	
480. WebView components cannot access / are blocked from local resources.	LOA, section 2.4.6, point 1 M72A, section 5.1, paragraph 2c)	
481. 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	

Criterion	Justification	Additional information / comment
	M72A, section 5.1, paragraph 2c)	

6.7 Code security, quality and development environment

Criterion	Justification	Additional information / comment
482. The app is signed and provisioned with a valid, trusted certificate.	LOA, section 2.4.6, point 1	
483. The app has been built in release mode (e.g. non-debuggable).	LOA, section 2.4.6, point 1 M72A, section 5.1, paragraph 2c)	
484. App development only uses tested and recommended software development/coding data security policies.	LOA, section 2.4.6, point 1 M72A, section 5.1, paragraph 2c)	All JavaScript components, for example, must be encoded and sanitised to reduce the risk of XSS attacks.
485. Debugging symbols have been removed from native binaries.	LOA, section 2.4.6, point 1 M72A, section 5.1, paragraph 2c)	

Criterion	Justification	Additional information / comment
486. Debugging code and messages has been removed.	LOA, section 2.4.6, point 1 M72A, section 5.1, paragraph 2c)	
487. All third party components used by the mobile app are identified, and checked for known vulnerabilities.	LOA, section 2.4.6, point 4 M72A, section 5.1, paragraph 3d)	
488. The app catches and handles possible exceptions.	LOA, section 2.4.6, point 4 M72A, section 5.1, paragraphs 2f) and 3d)	
489. The app or the server minimises the information contained in error messages.	LOA, section 2.4.6, point 1 M72A, section 5.1, paragraph 2c)	
490. Error handling logic in security controls denies access by default.	LOA, section 2.4.6, point 1 M72A, section 5.1, paragraph 2c)	
491. Memory is allocated, freed and used securely.	LOA, section 2.4.6, point 1 M72A, section 5.1, paragraph 2c)	
492. The data security features of the platform / development environment are activated.	LOA, section 2.4.6, point 1 M72A, section 5.1, paragraph 2c)	

6.8 Security controls and resilience

Criterion	Justification	Additional information / comment
493. The app 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.
494. The app has more than one feature that attempts to detect the presence of a rooted or jailbroken device.	LOA, section 2.4.6, point 4 M72A, section 5.1, paragraph 2f)	
495. The app 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 M72A, section 5.1, paragraph 2f)	
496. The app prevents debugging and detects, and responds to, a debugger being attached.	LOA, section 2.4.6, point 1 M72A, section 5.1, paragraph 2c)	
497. The app detects, and responds to, tampering with executable files and critical data/files within its own sandbox.	LOA, section 2.4.6, point 4 M72A, section 5.1, paragraph 2f)	
498. The app detects, and responds to, the presence of widely used reverse engineering tools on the device..	LOA, section 2.4.6, point 4	

Criterion	Justification	Additional information / comment
	M72A, section 5.1, paragraph 2f)	
499. The app detects, and responds to, being run in an emulator.	LOA, section 2.4.6, point 4 M72A, section 5.1, paragraph 2f)	
500. The app detects, and responds to, tampering the code and data in its own memory space.	LOA, section 2.4.6, point 4 M72A, section 5.1, paragraph 2f)	
501. Partitions that are important or critical to the app are encrypted where applicable on the system level. Analysis cannot be used to identify partitions that are important or critical to the app.	LOA, section 2.4.6, points 1 and 3 LOA, section 2.4.6, substantial M72A, section 5.1, paragraph 3b) M72A, section 5.1, paragraph 2c)	

Finnish Transport and Communications Agency Traficom

Erik Palménin aukio 1
P.O. Box 313
FI-00059 TRAFICOM
Tel. +358 295 390 100
www.traficom.fi