**Assessment guideline for electronic identification services**

**211/2023 O**

Traficom Guideline

[Draft for chapters 1–4]

1 June 2023

Contents

1 Introduction 4

1.1 Purpose of the Guideline 4

1.2 Entry into force of the Guideline 4

1.3 References to regulations and standards; abbreviations 5

1.4 Definitions of identification service 6

1.5 Overall reliability of the service provider (not part of the criteria) 8

2 Identification service assessment and the assessment report 9

2.1 Submission of the assessment report as an attachment to a notification 9

2.1.1 Commencement notification 9

2.1.2 Change notification 10

2.1.3 Periodic assessment 10

2.2 Areas of identification services subject to assessment 11

2.3 Identification means, identification scheme and subcontractors 12

2.3.1 Definitions 12

2.3.2 Assessment and subcontractors 13

2.3.3 Assessment report: A description that specifies the part of the identification means and/or the identification scheme covered by the assessment. 14

2.3.4 Assessment report: Name(s) of the identification service to be assessed 15

2.3.5 Assessment report: Description of identification means 15

2.3.6 Assessment report: Description of the identification scheme (system architecture) 15

2.4 Information on assessment body 16

2.4.1 Assessment report: Identifying information and contact information of assessment body 16

2.4.2 Assessment report or notification: Competence and independence of the assessment body 17

2.5 Assessment implementation 18

2.5.1 Assessment report: Assessment time and duration of assessment in person work time 18

2.5.2 Assessment report: Assessment methods 18

2.5.3 Details of the documentation used in the conformity assessment 19

2.5.4 Identification means risk assessment 19

2.6 Commensurability between assessment, assurance levels and risks 19

2.7 Accuracy of the assessment report 21

2.8 Reporting of irregularities in the assessment report 21

2.9 Correcting irregularities and reporting corrections 22

3 Areas of assessment 22

3.1 Characteristics of the identification means; authentication mechanism 22

3.2 Interoperability 23

3.3 Technical information security requirements 23

3.4 Security incident observation capacity; management of security incidents; disturbance notifications 24

3.5 Storage and handling of data 25

3.6 Security of physical premises 25

3.7 Sufficiency and competence of human resources 25

3.8 Information security management 26

3.9 Identity proofing and verification of the applicant of identification means (initial identification) 26

3.10 About initial identification based on an identity document using a remote connection 27

3.11 Lifecycle of identification means 32

3.12 Testing 33

ANNEX A: Assessment report checklist (guideline) 34

# Introduction

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

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

The document also features a checklist for assessment report contents.

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

## Purpose of the Guideline

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

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

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

Under section 42 of the Act on Strong Electronic Identification and Electronic Trust Services (617/2009), it is Traficom's duty to monitor compliance with the Act and the EU's eIDAS Regulation[[1]](#footnote-2). This Guideline has been issued pursuant to the general guidance and monitoring authorisation referred to in section 42 of the Act.

A separate guideline has been published on the notifications to be submitted to Traficom (214/2023 O). The eIDAS Regulation and the Electronic Identification Assurance Level Regulation (LOA) provide for the conformity assessment of an electronic identification means to be notified to the EU.[[2]](#footnote-3).

## Entry into force of the Guideline

Guideline 211/2023 O will enter into force on Day Month 2023.

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

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 |
| 211/2023 O | Day Month 2023 |  | Finnish Transport and Communications Agency (Traficom)  NCSC-FI |
| 211/2019 O | 9 Oct 2019 | 2nd published combined version   * Amended the general criteria by reducing the number of items and by listing them based on regulatory requirements. * Added a new set of special criteria for mobile apps used for electronic identification. * Incorporated updated guidelines on assessment reports of identification services from document 215/2016 O. | Finnish Transport and Communications Agency (Traficom), NCSC-FI |
| 211/2016 O Model criteria for identification service provider audits  215/2016 O Identification and trust service assessment reports | 2 Nov 2016 | First published versions | Finnish Communications Regulatory Authority (FICORA), NCSC-FI |

## References to regulations and standards; abbreviations

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

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

The assessment report guidelines are based on regulatory requirements.

Provisions with requirements for identification services include:

* The Act on Strong Electronic Identification and Electronic Trust Services (617/2009, hereinafter referred to as the *Identification Act*, *ITSA* or *Identification and Trust Services Act*)
* Commission Implementing Regulation (EU) 2015/1502 (hereinafter referred to as *LOA* or the *Assurance Level Regulation*)
  + The sections on Assurance Level Regulation referenced in the Identification Act
  + LOA Guidance (unofficial guide for the application of the Assurance Level Regulation)[[3]](#footnote-4)
* Traficom Regulation M72B/2022 (hereinafter referred to as *M72B*)[[4]](#footnote-5)
  + This Regulation complements certain requirements set out in the Identification Act.

References to standards[[5]](#footnote-6):

* ISO/IEC 27001:2013/2017 Information security management
  + The requirements of the general criteria contain references to the relevant requirements of standard ISO 27001. The purpose of the references is to facilitate the integration of identification service conformity assessments into more general assessments of information security management.
* OWASP Mobile AppSec Verification v.1.4.2[[6]](#footnote-7)

Assurance level abbreviations used in tables:

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

## Definitions of identification service

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

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

*Identification means provider* offers electronic identification means to end users.

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

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

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

***Definitions in provisions***

***ITSA, section 2 Definitions***

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

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

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

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

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

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

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

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

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

***PROVISIONS***

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

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

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

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

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

**4) responsibility for subcontractors; as well as**

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

# Identification service assessment and the assessment report

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

***PROVISIONS***

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

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

*The notification shall contain:*

*[…]*

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

*[…]*

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

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

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

***ITSA, section 31: Assessment report***

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

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

### Commencement notification

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

### Change notification

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

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

Examples of material changes include:

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

### Periodic assessment

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

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

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

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

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

## Areas of identification services subject to assessment

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

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

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

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

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

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

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

***PROVISIONS***

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

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

*[…]*

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

*[…]*

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

*[…]*

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

*[…]*

***M72B, section 15: Conformity assessment criteria***

*15.1 Identification scheme and identification means features to be assessed*

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

1. *certain properties of the functions affecting the provision of the identification service (the identification scheme), namely:*
2. *information security management;*
3. *record keeping and data processing;*
4. *facilities and staff;*
5. *technical measures (controls); and*
6. *interoperability in the trust network; as well as*
7. *the identification means, meaning certain properties of the identification means, namely:*
8. *application and registration;*
9. *identity proofing and verification of the applicant;*
10. *identification means characteristics and design;*
11. *issuance, delivery and activation;*
12. *suspension, revocation and reactivation;*
13. *renewal and replacement; and*
14. *authentication mechanisms.*

*15.2 Assessment criteria*

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

## Identification means, identification scheme and subcontractors

### Definitions

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

An identification means includes authentication factors and the authentication mechanism.

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

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

***Definitions in provisions***

***ITSA, section 2***

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

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

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

***Article 3 of the eIDAS Regulation***

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

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

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

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

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

***PROVISIONS ON SUBCONTRACTING***

***ITSA, section 13***

***[…]***

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

### Assessment and subcontractors

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

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

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

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

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

Examples of identification means assessment:

* How does a key code application / mobile telephone work as a secondary authentication factor, and what is the first authentication factor in this case? The assessment must establish how identification is performed using the application and if there is more than one way to do it (especially from the perspective of the authentication factors). Is another information-based factor or set of factors always required in addition to the one-time password provided by the application? Are there other authentication factors bound to the mobile device in addition to the key code application or the one-time password provided by the key code application?
* If a mobile identification application is used, it must be assessed in all respects that have impact on the compliance of the identification service. The assessment must establish how the binding between the application and the correct person is implemented in the mobile device and in the back-end system. If the application includes other features, these need not be included in the assessment insofar as they cannot influence the reliability of the identification.
* If authentication to an eService can be carried out using a mobile application only, it must be ensured that the authentication factors are sufficiently separated. In other words, the assessment must establish how the identification means ensures that an authentication factor based on information or property will not fall into the wrong hands if the mobile telephone is physically in the possession of another person or because of a data security violation. For example: what measures are taken to prevent the storing of a copy or a breakable hash of the PIN code that would put mobile phone-based identification at risk?

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

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

Cloud services

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

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

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

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

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

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

### Assessment report: Description of identification means

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

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

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

The descriptions must also cover all subcontractors.

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

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

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

## Information on assessment body

***PROVISIONS***

***ITSA, section 28: Conformity assessment bodies***

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

*1) a conformity assessment body;*

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

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

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

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

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

### 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.

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

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

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

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

*[…]*

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

*[…]*

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

*[…]*

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

*18.1 Proving procedures*

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

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

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

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

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

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

*18.2 Competence*

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

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

*19.1 Independence*

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

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

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

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

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

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

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

*19.2 Competence*

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

## Assessment implementation

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

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

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

### Assessment report: Assessment methods

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

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

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

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

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

### Details of the documentation used in the conformity assessment

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

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

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

### Identification means risk assessment

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

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

## Commensurability between assessment, assurance levels and risks

Two assurance levels are defined for the reliability of strong electronic identification: substantial and high.[[7]](#footnote-8) Assessment criteria tables use the abbreviations S=substantial (corresponds to eIDAS2 substantial) and H=high (corresponds to eIDAS3 high).

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

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

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

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

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

***CF.***

***LOA 2.3: Authentication***

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

***LOA Guidance, section 2.3***

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

The Level of Assurance uses the terms “enhanced-basic”, “moderate” and “high” to denote the different attack potentials. This terminology is borrowed from ISO/IEC 15408 ”Information technology – Security techniques – Evaluation criteria for IT security” and ISO/IEC 18045 ”Information technology – Security techniques – Methodology for IT security evaluation”. The text of the standards is also freely available at www.commoncriteriaportal.org/cc (CCPART1-3 being equivalent to ISO/IEC 15408 and CEM equivalent to ISO/IEC 18045).

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

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

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

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

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

[…]

Reasonable assumptions on the level of security of components used by, but not part of, the authentication scheme (e.g. the environment of the user, browser, smart phone, etc.) should be taken into account during the risk assessment.

Components can be operated in different configurations with different security settings.

[…]

***LOA 2.4: Management and organisation***

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

***LOA Guidance, section 2.4***

[…]

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

[…]

## 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.**

## Reporting of irregularities in the assessment report

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

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

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

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

Traficom will not prepare a scale indicating the severity of irregularities, but will leave their evaluation to the discretion of the identification service provider and the assessment body. Traficom makes the final assessment on whether the irregularities are acceptable due to their limited impact or the existence of an adequate correction plan or compensating action. Traficom may also require that the irregularities that are observed are corrected.

## Correcting irregularities and reporting corrections

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

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

# Areas of assessment

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

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

## Characteristics of the identification means; authentication mechanism

The requirements are set out in the following provisions:

* ITSA, section 8 a: Authentication factors used in the identification means
* LOA Annex, section 2.2.1: Electronic identification means characteristics and design
* ITSA, section 8: Requirements posed on the electronic identification scheme. (subsection 1, paragraph 3)
* LOA Annex, section 2.3.1: Authentication mechanism
* LOA Annex, section 2.4.6: Technical controls (point 2)
* M72B, section 6: Information security requirements of the identification means
* M72B, section 7: Identification scheme interface encryption requirements
* M72B, section 8: Authenticating parties to the communications
* M72B, section 9: Integrity and confidentiality of authentication messages
* LOA Annex, section 1: Applicable definitions
* 2) ‘authentication factor’ means a factor confirmed as being bound to a person, which falls into any of the following categories […]
* (3) 'dynamic authentication' means an electronic process using cryptography or other techniques to provide a means of creating on demand an electronic proof that the subject is in control or in possession of the identification data and which changes with each authentication between the subject and the system verifying the subject’s identity.

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

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

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

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

## Interoperability

The requirements are set out in the following provisions:

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

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

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

## Technical information security requirements

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

The requirements are set out in the following provisions:

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

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

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

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

* data connections
* control connections
* zoning of data connections
* data communication equipment and systems
* separation of production, maintenance and administration networks and the development environment
* filtering
* connections to the public network
* classification of information systems
* access rights and user identification
* high-risk job combinations
* hardening
* encryption solutions
* security of cryptographic materials
* specific requirements of remote workstations
* malware
* change management
* software vulnerabilities
* backup copies.

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

The requirements are set out in the following provisions:

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

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

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

## Storage and handling of data

The requirements are set out in the following provisions:

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

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

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

## Security of physical premises

The requirements are set out in the following provisions:

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

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

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

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

## Sufficiency and competence of human resources

The requirements are set out in the following provisions:

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

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

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

## Information security management

The requirements are set out in the following provisions:

* ITSA, section 8: Requirements posed on the electronic identification scheme (subsection 1, paragraph 5)
* LOA Annex, section 2.4: Management and organisation (Introduction)
* LOA Annex, section 2.4.3: Information security management
* LOA Annex, section 2.4.7: Compliance and audit
* M72B, section 4: Information security management system of the identification service provider
* LOA Annex, section 1: Applicable definitions  
  4. ‘information security management system’ means a set of processes and procedures designed to manage to acceptable levels risks related to information security.

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

* That the information security management of the identification service provider is comprehensive, consistent, organised and constantly monitored.
* That the requirements of the identification service (ITSA, the eIDAS LOA Regulation and Traficom Regulation M72B) are taken into account in the administration system.
* That the information security management of the subcontractors meets the requirements.

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

The requirements are set out in the following provisions:

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

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

* ITSA, section 7 a: Using the data in the Business Information System
* ITSA, section 17 a: Identifying a legal person applying for an identification means
* LOA Annex, section 2.1.3: Identity proofing and verification (legal person)
* LOA Annex, section 2.1.4: Binding between the electronic identification means of natural and legal persons
* LOA Annex, section 1: Applicable definitions  
  1. 'authoritative source' means any source irrespective of its form that can be relied upon to provide accurate data, information and/or evidence that can be used to prove identity.

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

Initial identification procedures available:

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

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

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

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

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

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

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

**Considerations for remote initial identification**

* If the identity document can be presented using a remote connection, a thorough assessment of risks and protection methods against the threat of forged identity documents or presentation of genuine identity documents by a wrong person is required.
* Factors that need to be taken into account include observations of the authenticity factors of the identity document and verification of and observations on the authenticity of the photograph or video recording provided by the person.
* Only an identity document with a chip can be used for remote initial identification when issuing a strong electronic identification means.
* The authenticity factors of identity documents are designed to be verified on the spot using instruments such as ultraviolet light. It may very well be impossible to verify the authenticity of an identity document based on a photograph of the document alone, because the security factors in the image are not transmitted properly. An image is mostly useful for verification of correct identity document layout.
* Using a chip in the identity document changes the situation substantially. Passive authentication (verification of a signature) can be used to verify that the information is from an authentic document and has not been altered. All passports with a chip have this signature capacity.

* However, the data can be copied from the chip at any point. No specific attack potential is required for copying the chip, because the chip data is (with the exception of fingerprint data) freely readable.
* Passports and identity cards also have the possibility for active authentication or chip authentication, which can be used to ensure that the chip is authentic and that the data has not been copied – in other words that the genuine identity document is at the other end of the remote connection at that exact moment.
* Once the chip authenticity and uniqueness have been confirmed, the portrait that is read from the chip can be trusted. The portrait is high-definition and has much greater resolution than the image printed on the passport. This enables the portrait information to be trusted, and because of the greater resolution it is much more suited for facial comparison against a photograph and/or video provided in a remote identification event.
* The portrait on the document may not be stored on the chip of the electronic identity document and therefore cannot be read from the chip for authentication purposes. In biometric passports the image is stored on the chip.
* Information must be retrieved from the population information system in order to ensure that the identity document presented is authentic and valid, and that it belongs to the individual presenting the identity document.
* If there is an opportunity to use some other country’s population information system and register containing information on the validity of identity documents and passports, remote identification can also be carried out based on these systems and registers.
* The authenticity of the information about the individual presenting the identity document via the remote connection must be verified, and the actual source of the information (the individual presenting the identity document) must be ensured. Factors that need to be taken into account include the reliability of the data communication and information system, the risk of a forged transmission and alteration of the visual appearance of the person in ways that are difficult to detect using the remote connection. As a general rule, the video link must be used via a mobile application, as a video link through a computer browser can be easily hacked.
* The lighting conditions and video quality requirements must be defined. The lighting must be appropriate, and any artefacts must be visible, as these can indicate video manipulation. The resolution must be appropriate throughout the remote initial identification event. If there are disturbances in the video link, the identification event must be interrupted and started again as necessary.
* Assessment of the lifelike appearance of the person who presents the identity document in the remote identification event can help confirm that the presenter of the identity document is present and that no forged recording is used. For example, the person could be requested to perform certain random gestures in real time. Staff must be provided with adequate training and comprehensive instructions on the assessment of the lifelike appearance of individuals. Machine assessment of lifelike appearance must be based on random events or requests targeted at the customer carrying out remote initial identification.
* Reliable comparison between information read from the identity document and the physical properties of the person at the other end of the remote connection transmitted via video or still image is a requirement (FAR value).
* However, how this can be performed in a manner that is reliable is not defined. In case of a remote connection this could, in principle, mean a comparison by a human agent or automatic electronic comparison by a back-end system that has access to both photographs. The reference point for comparison when assessing the reliability is that of an employee of the identification service comparing the information of the individual and the identity document on the spot whilst also able to observe the behaviour of the individual who presents the document.
* It must be noted that observation carried out by a computer is generally much more reliable than that carried out by a human. Therefore, a remote identification carried out only by a human agent is not sufficient.

Cf. also LOA Guidance:

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

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

**Considerations for legislation on the reading of chips**

* According to section 5a of the Passport Act 671/2006, passports feature a technical part referred to in the Council Regulation (EC) No 2252/2004 (EU Passport Regulation) on standards for security features and biometrics in passports and travel documents issued by Member States.  
    
  The passport holder’s portrait and fingerprints referred to in section 6a, along with the necessary additional information in accordance with the provisions of the EU Passport Regulation, are stored in the technical part. Information referred to in subsection 1 of section 5 can also be stored in the technical part. The EU Passport Regulation lays down provisions on the passport holder’s right to verify their personal data contained in the technical part of their passport.   
    
  The EU Passport Regulation lays down provisions on the security features and biometric identifiers on passports. A passport that contains a biometric identifier has an indication of this on the cover.
* According to section 5b of the Passport Act, the fingerprints stored in the technical part of the passport can only be read in accordance with the EU Passport Regulation. Fingerprints can only be read by the passport authority referred to in section 10 and the police or border control authority. […]  
    
  When reading fingerprints, the passport holder’s data may only be processed as defined in the EU Passport Regulation and the Passport Act.  
    
  In addition to the provisions of the Passport Act on the reading of fingerprints, the European Community’s legislation and international agreements binding upon Finland are complied with.
* The Passport Act has similarly restricted the reading of fingerprints to the named authorities, but the reading of the portrait is not restricted.
* In accordance with section 5a of the Identity Card Act (663/2016), the fingerprints and portrait stored in the technical part of the identity card can only be read as provided in the EU ID Regulation. Fingerprints can be read by the identity card authority as referred to in section 18, the Police and the Finnish Border Guard. Fingerprints can also be read by the Finnish Customs when it is acting as a pre-trial investigation authority or performing tasks of the border control authority. […]
* In other words, the reading of fingerprints is restricted only for certain authorities, but the reading of the portrait is not restricted by legislation.
* According to Article 11(6) of the EU ID Regulation (EU) 2019/1157, biometric data stored in the storage medium of identity cards shall only be used in accordance with Union and national law, by the duly authorised staff of competent national authorities and Union agencies.   
    
  According to recital 22 of the Regulation, biometric identifiers should be collected and stored in the storage medium of identity cards and residence documents for the purposes of verifying the authenticity of the document and the identity of the holder. Such a verification should only be carried out by duly authorised staff and only when the document is required to be produced by law. According to recital 19, as a general practice, Member States should, for the verification of the authenticity of the document and the identity of the holder, primarily verify the facial image and, where necessary to confirm without doubt the authenticity of the document and the identity of the holder, Member States should also verify the fingerprints. According to recital 17, security features are necessary to verify if a document is authentic and to establish the identity of a person. The establishment of minimum security standards and the integration of biometric data in identity cards […] are important steps in rendering their use in the Union more secure. **The inclusion of such biometric identifiers should allow Union citizens to fully benefit from their rights of free movement.** Furthermore, according to recital 15, “This **Regulation does not affect the use of identity cards** and residence documents with eID function **by Member States for other purposes, nor does it affect the rules laid down in Regulation (EU) No 910/2014** of the European Parliament and of the Council, which provides for Union-wide mutual recognition of electronic identifications **in access to public services** and which helps citizens who are moving to another Member State, by requiring mutual recognition of electronic identification means subject to certain conditions. **Improved identity cards should ensure easier identification and contribute to better access to services.”**
* Section 2.1.2 of the Annex of the Commission Implementing Regulation (EU) 2015/1502 (LOA or the Assurance Level Regulation) based on the eIDAS Regulation requires on the high assurance level that **where the person** has been verified to be in possession of photo or **biometric identification evidence** recognised by the Member State in which the application for the electronic identity means is being made and that evidence represents the claimed identity, **the evidence is checked** to determine that it is valid according to an authoritative source.
* Most of the data on identity cards is freely readable, but some are restricted without the correct certificate. The reading of fingerprints, in particular, is restricted by law to named authorities. Reading the portrait is generally not restricted, and there are many free applications on the market for reading portraits. (NOTE! These are not primarily usable as such as data-secure methods.)
* According to Article 9(1) of the General Data Protection Regulation, […] processing of biometric data for the purpose of uniquely identifying a natural person […] shall be prohibited. According to Article 9(2)(g), paragraph 1 shall not apply if processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.
* Generally, in situations where the portrait would be read, the customer can refuse and instead opt for authentication in person. The customer can also approve the reading of the portrait as they wish and take care of identification via a remote connection.
* The European Banking Authority (EBA) has published instructions on the remote identification of customers (<https://www.eba.europa.eu/eba-publishes-guidelines-remote-customer-onboarding>).
* Paragraph 35:  
  "In situations where the device the customers use to prove their identity allows the collection of relevant data, for example because the data is contained in the chip of a national identity card, and it is technically feasible for the credit and financial institutions to access this data, credit and financial institutions should consider using this information to verify its consistency with the information obtained through other sources, such as the submitted data or other documents submitted by the customer."
* Paragraph 39:  
  "Where the remote customer onboarding solution involves the use of biometric data to verify the customer’s identity, credit and financial institutions should make sure that the biometric data is sufficiently unique to be unequivocally linked to a single natural person. [...]"
* According to EBA’s interpretation, e.g. the portrait of a customer can and should be read in a remote identification situation.
* In its interpretation, Traficom relies on the EBA instructions and furthermore on the fact that e.g. the EU ID Regulation does not restrict the application of eIDAS, and that the Assurance Level Regulation based on eIDAS enables the reading of biometric data. Based on the above, Traficom states that reading the portrait from an identity card or passport does not appear to be prohibited by law and is even a prerequisite on assurance level high based on the Assurance Level Regulation. This makes it a good method for enabling the remote identification of a customer.

## Lifecycle of identification means

The requirements are set out in the following provisions:

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

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

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

In December 2018, Traficom published an advisory memorandum[[8]](#footnote-9) on the verification of identity in maintenance situations.

## Testing

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

# ANNEX A: Assessment report checklist (guideline)

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

1. Identifying information and contact information of assessment body (2.4.1)
   1. Name of the company or the organisation and a unique registration number or identifier.
   2. If the company or organisation is located in an EEA state other than Finland: the register in which the foreign company or organisation has been entered.
   3. Postal address and contact persons.
   4. E-mail addresses for enquiries by Traficom.
2. Competence and independence of the assessment body (2.4.2)

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

1. Assessment time and duration of assessment in person work time (2.5.1)
2. Assessment methods (2.5.2)
3. Details of the documentation used in the conformity assessment (2.5.3)
4. A description that specifies the part of the identification means and/or the identification scheme covered by the assessment (2.3.3)
5. Name(s) of the identification service to be assessed (2.3.4)
6. Description of identification means (2.3.5)
7. Description of the identification scheme (system architecture) (2.3.6)
8. Irregularities (2.8–2.9)
9. Results of assessment specific to individual areas (3.1–3.12 as applicable)

1. Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC. [↑](#footnote-ref-2)
2. Commission Implementing Regulation (EU) 2015/1502 on setting out minimum technical specifications and procedures for assurance levels for electronic identification means pursuant to Article 8(3) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market. [↑](#footnote-ref-3)
3. <https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/LOA_Guidance.pdf> [↑](#footnote-ref-4)
4. Regulation M72B/2022 on Electronic Identification and Trust Services https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/M72B\_2022\_M%C3%84%C3%84R%C3%84YS\_72B\_tunnistus-\_ja\_luottamuspalvelut\_ENG\_julkaistu.pdf [↑](#footnote-ref-5)
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> [↑](#footnote-ref-6)
6. <https://www.owasp.org/index.php/OWASP_Mobile_Security_Testing_Guide> [↑](#footnote-ref-7)
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. [↑](#footnote-ref-8)
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> [↑](#footnote-ref-9)