**Assessment guideline for electronic identification services**

Traficom Guideline

211/2023 O Annex B

**DRAFT 26 May 2023**

Contents

[1. Characteristics of the identification means; authentication mechanism 3](#_Toc138170208)

[2. Interoperability 20](#_Toc138170209)

[3. Technical information security requirements 25](#_Toc138170210)

[3.1 Communications security 27](#_Toc138170211)

[3.2 Information system security 34](#_Toc138170212)

[3.3 Operator security 40](#_Toc138170213)

[4. Security incident observation capacity; management of security incidents; disturbance notifications 44](#_Toc138170214)

[5. Storage and handling of data 52](#_Toc138170215)

[6. Security of physical premises 59](#_Toc138170216)

[7. Sufficiency and competence of human resources 61](#_Toc138170217)

[8. Information security management 62](#_Toc138170218)

[9. Identity proofing and verification of the applicant of identification means (initial identification) 67](#_Toc138170219)

[10. Lifecycle of identification means 84](#_Toc138170220)

ANNEX B: General assessment criteria for identification services

# Characteristics of the identification means; authentication mechanism

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **M72B, section 15.1: Identification scheme and identification means features to be assessed**  The identification service assessment required in section 29 of the Identification and Trust Services Act must cover all of the requirements specified in the Act and in this regulation, which pertain to:  […]  2) the identification means, meaning certain properties of the identification means, namely:  […]  c) identification means characteristics and design;  […]  g) authentication mechanisms.  M72B, section 6: Information security requirements of the identification means  6.1 Identification means characteristics and its resistance  6.1.1  The authentication factors, authentication mechanism and security measures of the identification means must be planned, executed and maintained so that they protect the integrity and confidentiality of the identification means. The identification means must be able to resist at least moderate or high-level threats and attack potential specified in section 2.3 of the appendix to the regulation on *Level of Assurance in Electronic Identification* in accordance with the assurance level of the identification service.  The resistance must be based on a risk assessment including specific assessments of threats directed at an authentication mechanism and authentication factors based on possession, knowledge and inherence as well as assessment of security measures in place to protect against these threats.  6.1.2  The features and security measures of the identification means must prevent the possibility that the compromise of one authentication factor would compromise the reliability of other authentication factors. The security measures protecting the identification means must separate and protect the authentication factors especially if they are used on the same terminal device.  6.1.3  The identification means and authentication must employ internationally or nationally recommended encryption methods. The communications connection between the identification means and the identification scheme must employ encryption methods specified in section 7 of the regulation, where technically applicable, unless resistance of the system assessed as a whole is otherwise realised by other security means.  6.2 Specific security measures  6.2.1  The identification service must present the user with information during the identification event, based on which the user may ensure that the identification request received in the identification means by the user is connected to the user’s event. This information must be presented in identification means that have the technical ability to do so.  6.2.2  The identification service must present the identification means user with information concerning the relying party, for whom the identification is carried out, during the identification event. This information must be presented in identification means that have the technical ability to do so.  6.2.3  In this regulation, single sign-on refers to the identification service offering authentication to more than one relying party based on a single authentication of the holder using strong electronic identification means.  In planning, executing and maintaining single sign-on, the identification service must take care of the security measures based on the management of the length, transfer and ending of the session related to single sign-on. [...]  6.3 Connecting identification means to a person  6.3.1  The authentication factors of the identification means must be bound to the identification means holder in the identification scheme.  6.3.2  An identification means shall not be bound to an applicant before the applicant has passed initial identification or it has been otherwise ensured in the process of granting an identification means that the identification means is not functional before the initial identification referred to in section 17 of the Identification and Trust Services Act has been performed.  6.4 Processing identification means holder-specific data  6.4.1  The identification service provider shall ensure that secret data related to an identification means is not revealed to its staff under any circumstances.  6.4.2  The identification service provider shall not make copies of any secret data related to an identification means. | | | | | |
| **NO.** | **LEVEL OF ASSURANCE** | **REQUIREMENT PERTAINING TO THE IDENTIFICATION SERVICE (SUMMARY)** | **PROVISIONS** | **STANDARD REFERENCE** | **NOTES** |
|  |  | A risk assessment is available for the identification means (calculation of attack potential). | **ITSA, section 8: Requirements posed on the electronic identification scheme**  Section 8.1, paragraph 3: The identification means can be used to verify that only the holder of the identification means can use the means in a way that, at a minimum, meets the conditions for assurance level substantial laid down in sections 2.2.1 and 2.3 of the Annex to the Act on Level of Assurance in Electronic Identification.  **LOA Annex, section 2.3.1: Authentication mechanism**  The authentication mechanism implements security controls for the verification of the electronic identification means, so that it is highly unlikely that activities such as guessing, eavesdropping, replay or manipulation of communication by an attacker with moderate attack potential can subvert the authentication mechanisms.  M72B, section 6.1.1  The authentication factors, authentication mechanism and security measures of the identification means must be planned, executed and maintained so that they protect the integrity and confidentiality of the identification means. The identification means must be able to resist at least moderate or high-level threats and attack potential specified in section 2.3 of the appendix to the regulation on *Level of Assurance in Electronic Identification* in accordance with the assurance level of the identification service.  The resistance must be based on a **risk assessment** including specific assessments of threats directed at an authentication mechanism and authentication factors based on possession, knowledge and inherence as well as assessment of security measures in place to protect against these threats. | ISO 29115  ISO/IEC 15408-1  ISO/IEC 18045, Annex B  Common Criteria CCDB 2009 03, part 3  ETSI TS 102 165-1, clauses 6.6 and 6.7 | E.g. Common Criteria CCDB 2009 03, part 3, or ETSI TS 102 165-1, clauses 6.6 and 6.7 calculation of the likelihood of the attack. The appropriate implementation of risk assessment is the basic premise for the calculation of attack potential. |
| 1. 1 | S, H | The identification means uses at least two authentication factors from different authentication factor categories. | ITSA, section 8 a: Authentication factors used in the identification means.  […]  1) a knowledge-based authentication factor that the subject is required to demonstrate knowledge of;  2) a possession-based authentication factor that the subject is required to demonstrate possession of;  3) an inherent authentication factor that is based on a physical attribute of a natural person.  […]  LOA Annex, section 2.2.1: Electronic identification means characteristics and design  The electronic identification means uses at least two authentication factors from different categories. |  |  |
| 1. 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.  M72B, section 6.1.2  The features and security measures of the identification means must prevent the possibility that the compromise of one authentication factor would compromise the reliability of other authentication factors. The security measures protecting the identification means must separate and protect the authentication factors especially if they are used on the same terminal device. |  | Mutual independence of authentication factors requires special attention especially in identification means used on mobile devices. |
|  | S, H | Different threat types that target different authentication factors are taken into account in the planning of the identification means. | LOA Annex, section 2.2.1: Electronic identification means characteristics and design  The electronic identification means is designed so that it can be assumed to be used only if under the control or possession of the person to whom it belongs.  M72B, section 6.1.2  The features and security measures of the identification means must prevent the possibility that the compromise of one authentication factor would compromise the reliability of other authentication factors. The security measures protecting the identification means must separate and protect the authentication factors especially if they are used on the same terminal device. |  |  |
|  | S, H | Secret information related to the identification means is not accessible to the personnel or the subcontractors of the identification service provider. | M72B, section 6.4: Processing identification means holder-specific data  6.4.1  The identification service provider shall ensure that secret data related to an identification means is not revealed to its staff under any circumstances.  6.4.2  The identification service provider shall not make copies of any secret data related to an identification means. |  | Secret information typically includes PIN codes and other information-based authentication factors.  This requirement is intended to address the risk of dishonest personnel. |
|  | S, H | Authentication factors are confirmed as being bound to a person. | LOA Annex, section 1: Applicable definitions  2) ‘authentication factor’ means a factor confirmed as being bound to a person, which falls into any of the following categories […]  LOA Annex, section 2.2.1: Electronic identification means characteristics and design  The electronic identification means is designed so that it can be assumed to be used only if under the control or possession of the person to whom it belongs.  M72B, section 6.3: Connecting identification means to a person  6.3.1  The authentication factors of the identification means must be bound to the identification means holder in the identification scheme.  6.3.2  An identification means shall not be bound to an applicant before the applicant has passed initial identification or it has been otherwise ensured in the process of granting an identification means that the identification means is not functional before the initial identification referred to in section 17 of the Identification and Trust Services Act has been performed. |  | Examples include binding of identification application to a person, chip personalisation or the linking of a pass code list or device to a person. |
|  | S, H | The authentication mechanism is designed so that each identification event has unique electronic proof. | ITSA, section 8 a  […] Every identification means must use a dynamic authentication referred to in section 2.3.1 of the Annex to Act on Level of Assurance in Electronic Identification that changes in every new authentication event between the person and the system certifying their identity.  **LOA Annex, section 1: Applicable definitions**  (3) 'dynamic authentication' means an electronic process using cryptography or other techniques to provide a means of creating on demand an electronic proof that the subject is in control or in possession of the identification data and which changes with each authentication between the subject and the system verifying the subject’s identity.  LOA Annex, section 2.3.1: Authentication mechanism  The release of person identification data is preceded by reliable verification of the electronic identification means and its validity through a dynamic authentication process. |  | Also applies to identification broker services.  LOA Guidance (extracts)  The primary purpose of dynamic authentication is to mitigate against attacks such as ‘man-in-the-middle’ or misusing verification data from a previously recorded authentication replay to the verifier.  …  It is important to understand that multi-factor and dynamic authentication are not the same; multi-factor authentication does not require that the authentication is dynamic (e.g. PIN and fingerprint) and can therefore be more exposed to replay attack than a dynamic authentication.  …  If the subject’s private key is stored remotely (centrally stored, e.g. in an HSM operated by the identity provider), the authentication used to access the private key should also be dynamic. |
|  | S, H | The electronic proof of each identification event is based on authentication factors bound to a person. | **LOA Annex, section 1: Applicable definitions**  (3) 'dynamic authentication' means an electronic process using cryptography or other techniques to provide a means of creating on demand an electronic proof that the subject is in control or in possession of the identification data and which changes with each authentication between the subject and the system verifying the subject’s identity.    **M72B, section 6.3: Connecting identification means to a person**  6.3.1  The authentication factors of the identification means must be bound to the identification means holder in the identification scheme.  **LOA Annex, section 2.3.1: Authentication mechanism**  Substantial:  1. The release of person identification data is preceded by reliable verification of the electronic identification means and its validity through a dynamic authentication process.  2. The authentication mechanism implements security controls for the verification of the electronic identification means, so that it is highly unlikely that activities such as guessing, eavesdropping, replay or manipulation of communication by an attacker with moderate attack potential can subvert the authentication mechanisms. |  | The authentication factors cannot be copyable. |
|  | H | The user is able to protect the identification means and their authentication factors reliably against use by others. | **LOA Annex, section 2.2.1: Electronic identification means characteristics and design**  The electronic identification means is designed so that it can be reliably protected by the person to whom it belongs against use by others.  Also **LOA Annex, section 2.2.2: Issuance, delivery and activation**  The activation process verifies that the electronic identification means was delivered only into the possession of the person to whom it belongs.  **M72B, section 6.1: Identification means characteristics and its resistance**  6.1.1  The authentication factors, authentication mechanism and security measures of the identification means must be planned, executed and maintained so that they protect the integrity and confidentiality of the identification means. The identification means must be able to resist at least moderate or high-level threats and attack potential specified in section 2.3 of the appendix to the regulation on Level of Assurance in Electronic Identification in accordance with the assurance level of the identification service. […]  6.1.2  The features and security measures of the identification means must prevent the possibility that the compromise of one authentication factor would compromise the reliability of other authentication factors. The security measures protecting the identification means must separate and protect the authentication factors especially if they are used on the same terminal device.  **M72B, section 6.4: Processing identification means holder-specific data**  6.4.1  The identification service provider shall ensure that secret data related to an identification means is not revealed to its staff under any circumstances.  6.4.2  The identification service provider shall not make copies of any secret data related to an identification means. |  | 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.   LOA Guidance, section 2.2.2, high  For level High the activation process shall ensure that only the legitimate owner can activate the electronic identification means and that the activation process is protected from accidental loss and insider threats such as collusion.  NOTE! The user must be able to ensure that the security factors, or e.g. a resetting code connected to the identification means, cannot be available to others. Any activation or resetting codes can only be used once. |
|  | S, H | No identification data is released to the relying party (no identification event is performed) before the identification means is verified using dynamic authentication. | **LOA Annex, section 2.3.1: Authentication mechanism**  The release of person identification data is preceded by reliable verification of the electronic identification means and its validity through a dynamic authentication process. | A.14.1  System acquisition, development and maintenance / Security requirements of information systems  A.14.1.2 Securing application services on public networks    A.14.1.3 Protecting application services transactions | Also applies to identification broker services. |
|  | S, H | The identification data (personal data) stored in the identification event is protected. | **LOA Annex, section 2.3.1: Authentication mechanism**Where person identification data is stored as part of the authentication mechanism, that information is secured in order to protect against loss and against compromise, including analysis offline.  **M72B, section 7.1: Communications encryption methods**  7.1.1  Interfaces between identification service providers and interfaces between an identification service provider and relying parties shall be encrypted. [see methods later in the regulation]  **M72B, section 9.1: Protecting messages between identification services and relying parties**  9.1.1  The **integrity and confidentiality of authentication messages containing personal data must be protected** in communications between identification services and between identification services and relying parties in one of the following ways:  a) by ensuring the integrity and confidentiality of the communications connection by binding the parties’ communications to digital certificates or keys provided in compliance with section 8, or  b) by encrypting and signing the messages with a key provided in compliance with the procedure in section 8. |  | Also applies to identification broker services.  All technical environments of the participants of the identification event where identification data is stored must be taken into account. |
|  | S | The security measures used in the identification means provide protection against attacks of a moderate severity rating. | **ITSA, section 8: Requirements posed on the electronic identification scheme**  Section 8.1, paragraph 3: The identification means can be used to verify that only the holder of the identification means can use the means in a way that, at a minimum, meets the conditions for assurance level substantial laid down in sections 2.2.1 and 2.3 of the Annex to the Act on Level of Assurance in Electronic Identification.  **LOA Annex, section 2.3.1: Authentication mechanism**  The authentication mechanism implements security controls for the verification of the electronic identification means, so that it is highly unlikely that activities such as guessing, eavesdropping, replay or manipulation of communication by an attacker with moderate attack potential can subvert the authentication mechanisms. | ISO 29115  ISO/IEC 15408-1  ISO/IEC 18045, Annex B  Common Criteria CCDB 2009 03, part 3  ETSI TS 102 165-1, clauses 6.6 and 6.7 | Cf. criteria 1 risk assessment and calculation of attack potential  The assessment should take relevant threats into account. For example, ISO 29115 mentions: online guessing, offline guessing, credential duplication, phishing, eavesdropping, replay attack, session hijacking, man-in-the-middle, credential theft, spoofing and masquerading.  ISO/IEC 15408-1 defines “attack potential – measure of the effort to be expended in attacking a [mechanism], expressed in terms of an attacker's expertise, resources and motivation”.  Annex B.4 of ISO/IEC 18045 / CEM contains Guidance on how to calculate the attack potential necessary to exploit a given weakness of an authentication mechanism.  Common Criteria and ETSI 102 165-1 contain instructions for the calculation of attack potential.  The authentication mechanism needs to take the threat of identification requests initiated by incorrect eServices or the hijacking of an identification session (phishing) into account.  see description in LOA Guidance, section 2.3.1  Also applies to identification broker services. |
|  | H | The security measures used in the identification means provide protection against attacks of high severity rating. | **ITSA, section 8: Requirements posed on the electronic identification scheme**  Section 8.1, paragraph 3: The identification means can be used to verify that only the holder of the identification means can use the means in a way that, at a minimum, meets the conditions for assurance level substantial laid down in sections 2.2.1 and 2.3 of the Annex to the Act on Level of Assurance in Electronic Identification.  **LOA Annex, section 2.2.1: Electronic identification means characteristics and design**  The electronic identification means protects against duplication and tampering against attackers with high attack potential.  **LOA Annex, section 2.3.1: Authentication mechanism**  The authentication mechanism implements security controls for the verification of the electronic identification means, so that it is highly unlikely that activities such as guessing, eavesdropping, replay or manipulation of communication by an attacker with high attack potential can subvert the authentication mechanisms. | 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. |
|  | S, H | The authentication mechanism displays the name of the eService in the means and identification process stages where possible. | **M72B, section 6.2.2** The identification service must present the identification means user with information concerning the relying party, for whom the identification is carried out, during the identification event. This information must be presented in identification means that have the technical ability to do so.  **M72B, section 12.1: Mandatory set of data**  The following minimum set of data shall be relayed at the interface between the identification means provider and the provider of an identification broker service:  [...] 4) name of the relying party authenticated by the identification broker service. |  | Also applies to identification broker services. |
|  | S, H | The authentication mechanism displays the session identifier in the means and identification process stages where possible. | **M72B, section 6.2.1** The identification service must present the user with information during the identification event, based on which the user may ensure that the identification request received in the identification means by the user is connected to the user’s event. This information must be presented in identification means that have the technical ability to do so. |  | Also applies to identification broker services. |
|  | S, H | The authentication mechanism follows the mandatory encryption requirements between the **identification means provider and the identification broker services.** | **LOA Annex, section 2.4.6: Technical controls**  2. Electronic communication channels used to exchange personal or sensitive information are protected against eavesdropping, manipulation and replay.  **M72B, section 7.1: Identification scheme interface encryption requirements**  7.1.1  Interfaces between identification service providers and interfaces between an identification service provider and relying parties shall be encrypted. The following methods shall be used in the encryption, key exchange, digital certificates and signing:  1) Key exchange: In key exchange, DHE methods or ECDHE methods with elliptic curves shall be used. The size of the finite field to be used in calculations shall be at least 2,048 bits in DHE and at least 224 bits in ECDHE.  2) Signature or asymmetric encryption: When using the RSA for electronic signatures or encryption, the key length shall be at least 2,048 bits. When using the ECDSA or EdDSA methods with elliptic curves, the size of the finite field must be at least 224 bits.  3) Symmetrical encryption: The encryption algorithm must be AES, Serpent or ChaCha20. The key length shall be at least 128 bits. The encryption mode must be CBC, CCM, GCM or CTR.  4) Hash functions: The hash function or authentication code must be SHA-2, SHA-3, Whirlpool or Poly1305.  7.1.2  In addition to methods and values mentioned in section 7.1.1, methods and values that have been assessed as secure in use specified in subsections 1–4 in the current versions of the following documents may also be complied with:  a) Kryptografiset vahvuusvaatimukset luottamuksellisuuden suojaamiseen - kansalliset turvallisuusluokat (Dnro 190/651/2015) instruction (in Finnish) issued by the Crypto Approval Authority operating within the Finnish Transport and Communications Agency, or  b) SOG-IS Crypto Evaluation Scheme Agreed Cryptographic Mechanisms of the SOGIS-MRA (Senior Officers Group for Information Systems, Mutual Recognition Agreement), an agreement between certain certification bodies of EU or EEA Member States.  7.1.3  Encryption settings shall be technically forced to the minimum levels listed above to avoid a situation where settings weaker than the minimum levels are adopted following connection handshakes.  7.2 Communications encryption protocol  If the TLS protocol is used, version 1.2 of TLS or newer shall be used.  The integrity and confidentiality of messages containing personal data shall be protected by encryption referred to paragraph 1 above and also at a message level in accordance with paragraph 1.  **M72B, section 8: Authenticating parties to the communications**  8.1 Verification of the parties to the communications connection  The authenticity and integrity of the digital certificates or keys used to encrypt the communications or messages as well as their holders must be verified in establishing communications connections between identification services and identification services and relying parties.  The authentication must be based on a qualified electronic signature or a qualified electronic seal in compliance with the eIDAS Regulation or a direct bilateral procedure. Authentication may not only be based on a generally trusted digital certificate.  8.2 Certificate and key renewal  The digital certificates and keys referred to in section 8.1 above must be regularly renewed.  In order to ensure the authenticity and integrity of new digital certificates and keys, the renewal must be carried out in one of the following ways:   1. in accordance with the procedure in section 8.1; 2. by providing new keys via a communications connection, whose integrity and confidentiality has been ensured by binding the parties’ communications to digital certificates or keys provided in accordance with section 8.1; or 3. by signing a new key using a key provided in accordance with section 8.1 or a key chained from such a key.   **M72B, section 9: Integrity and confidentiality of authentication messages**  9.1: Protecting messages between identification services and relying parties  9.1.1  The integrity and confidentiality of authentication messages containing personal data must be protected in communications between identification services and between identification services and relying parties in one of the following ways:   1. by ensuring the integrity and confidentiality of the communications connection by binding the parties’ communications to digital certificates or keys provided in compliance with section 8; or 2. by encrypting and signing the messages with a key provided in compliance with the procedure in section 8.   9.1.2  Authentication messages between identification broker services and relying parties must be authenticated with signatures.  9.2 Protecting messages in the user interface  If the authentication messages are relayed via the user’s browser or terminal device, the messages must be encrypted and signed in accordance with subsection 9.1.1.b).  9.3 Encryption algorithms and procedures  The encryption and signing of messages must employ the procedures specified in section 7.1, where applicable. | 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. |
|  | S, H | The authentication mechanism follows the mandatory encryption requirements **between the identification service and the eService.** | **LOA Annex, section 2.4.6: Technical controls**  2. Electronic communication channels used to exchange personal or sensitive information are protected against eavesdropping, manipulation and replay.  **M72B, sections 7–9 (above)**  **M72B, section 9: Integrity and confidentiality of authentication messages**  **9.1: Protecting messages between identification services and relying parties**  9.1.1  The integrity and confidentiality of authentication messages containing personal data must be protected in communications between identification services and between identification services and relying parties in one of the following ways:  a) by ensuring the integrity and confidentiality of the communications connection by binding the parties’ communications to digital certificates or keys provided in compliance with section 8, or  b) by encrypting and signing the messages with a key provided in compliance with the procedure in section 8.  […]  **9.2 Protecting messages in the user interface**  If the authentication messages are relayed via the user’s browser or terminal device, the messages must be encrypted and signed in accordance with subsection 9.1.1.b).  **9.3 Encryption algorithms and procedures**  The encryption and signing of messages must employ the procedures specified in section 7.1, where applicable. | 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. |
|  | S, H | The authentication mechanism follows the mandatory encryption requirements **on the user interface (browser, mobile device).** | **LOA Annex, section 2.4.6: Technical controls**  2. Electronic communication channels used to exchange personal or sensitive information are protected against eavesdropping, manipulation and replay.  **M72B, section 7 (above)**  **M72B, section 9.2: Protecting messages in the user interface**  If the authentication messages are relayed via the user’s browser or terminal device, the messages must be encrypted and signed in accordance with subsection 9.1.1.b).  **M72B, section 9.3: Encryption algorithms and procedures**  The encryption and signing of messages must employ the procedures specified in section 7.1, where applicable. | A.10.1.1 Policy on the use of cryptographic controls  A.13.2.3 Communications security / Information transfer: Electronic messaging | Note! Also applies to identification broker services. |
|  | H | The authentication method follows the **recommended** tightened/high level encryption requirements between the identification broker service and identification brokering, between the identification service and the eServices and in the user interface (browser, mobile device). | **MPS72B, section 4.7.1.3 (20 May 2022) recommendation**  At the high level of assurance, instead of using the requirements for substantial level of assurance provided in section 7.1 of the Regulation, it is recommended to apply the following values in parentheses, **which will meet the minimum assurance level of 128 bits**, to the identification scheme:  1) **Key exchange**: In key exchange, DHE methods or ECDHE methods with elliptic curves shall be used. The size of the finite field to be used in calculations shall be at least 2,048 (**4,096 at high level of assurance**) bits in DHE and at least 224 (**256 at high level of assurance**) bits in ECDHE.  The DH groups 14 to **21**, 23, 24 and 26 (**from 16 to 21** at high level of assurance) of IANA’s IKEv2 specifications meet the above requirements.  2) Signature or asymmetric encryption: When using the RSA for electronic signatures or encryption, the key length shall be at least 2,048 (**3,072 at high level of assurance**) bits. When using the elliptic curve method ECDSA or EdDSA, the underlying field size shall be at least 224 (**256 at high level of assurance**) bits.  3) Symmetrical encryption: The encryption algorithm must be AES, Serpent or ChaCha20 (***AES or Serpent* at high level of assurance**). The key length shall be at least 128 (**128 at high level of assurance**) bits. The encryption mode must be CBC, CCM, GCM or CTR.  4) Hash functions: The hash function or authentication code must be SHA-2, SHA-3, Whirlpool or Poly1305. SHA-2 refers to functions SHA224, SHA256, SHA384 and SHA512 (**SHA-3-256, SHA-3-384, SHA-3-512 at high level of assurance**). | A.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. |

# Interoperability

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| KEY PROVISIONS  ITSA, section 29: Conformity assessment of an electronic identification service  An identification service provider must regularly subject their service to an assessment by an assessment body referred to in section 28 to determine whether the identification service meets the requirements on interoperability, information security, data protection and other reliability laid down in this Act.  …  M72B, section 15: Conformity assessment criteria  The identification service assessment shall cover the requirements concerning the following:  1) certain properties of the functions affecting the provision of the identification service (the identification scheme), namely:  d) technical measures (controls)  e) interoperability in the trust network  ITSA, section 12  …  Identification service providers must collaborate to ensure that the technical interfaces of the members of a trust network are interoperable and that they enable the provision of interfaces that implement commonly known standards to the relying parties.  …  M72B, section 12: Minimum set of data to be relayed in a trust network  12.1 Mandatory set of data  The following minimum set of data shall be relayed at the interface between the identification means provider and the provider of an identification broker service:   1. in identification events concerning natural persons: at least the first name, family name, date of birth and the unique identifier of the person authenticated by the identification means provider; 2. in identification events concerning legal persons: at least the first name, family name and the unique identifier of the natural person representing the legal person as well as the unique identifier of the organisation authenticated by the identification means provider; 3. an indication of whether the level of assurance is substantial or high; as well as 4. name of the relying party authenticated by the identification broker service.   12.2 Optional information  The interface between the identification means provider and the provider of an identification broker service must have the technically planned possibility to relay the following information:   1. indication of whether the identification event concerns a public administration eService or a private eService; 2. in identification events concerning natural persons: forename(s) and surname(s) at the time of birth, place of birth, current address and gender; and 3. in identification events concerning legal persons: 4. current address; 5. VAT registration number; 6. tax reference number; 7. the identifier related to Article 3(1) of Directive 2009/101/EC of the European Parliament and of the Council; 8. Legal Entity Identifier (LEI) referred to in Commission Implementing Regulation (EU) No 1247/20122; 9. Economic Operator Registration and Identification (EORI) referred to in Commission Implementing Regulation (EU) No 1352/20133; and 10. excise number provided in Article 2(12) of Council Regulation (EC) No 389/20124.   12.3 Pseudonymisation of identification  The duties specified in sections 12.1 and 12.2 above pertain to the interface between the identification means and the identification broker service in authenticating the user even when the identification broker service only discloses the pseudonym of the identification means user or a limited amount of personal data on the user to the relying party in accordance with section 8, subsection 2 of the Identification and Trust Services Act.  14 Data transfer protocol and other requirements  14.1 Data transfer protocol  The identification service provider must enable the chaining of initial identification in accordance with section 17 of the Identification and Trust Services Act and relaying identification events within the trust network in accordance with section 12 a of the Identification and Trust Services Act using an interface conforming to at least either the Open IDConnect or SAML protocol.  14.2 Other features of the interface  The identification means provider, the provider of the identification broker service, the relying party and the national node operator shall negotiate the properties of their mutual interfaces (other than those laid down in this Regulation) and the respective protocol to be employed. | | | | | |
| **NO.** | **LEVEL OF ASSURANCE** | **REQUIREMENT PERTAINING TO THE IDENTIFICATION SERVICE (SUMMARY)** | **PROVISIONS** | **STANDARD REFERENCE** | **NOTES** |
|  | S, H | The identification service provider offers at least one interface in the trust network that complies with a universally applied standard. | **Government Decree 169/2016 on the trust network of strong electronic identification services providers**  **Section 1: Technical interfaces of a trust network**  Technical interfaces referred to in section 12 a, paragraph 2 of the Act on Strong Electronic Identification and Electronic Signatures (617/2009), hereinafter referred to as the Identification Act, are:  1) interface between identification means providers;  2) interface between an identification means provider and an identification broker service provider;  3) interface between an identification broker service provider and an identification service relying party.  The identification service providers in a trust network may agree on an interface required for the transmission of a charge for identification data referred to in section 12 a, paragraph 3 of the Identification Act or other interface necessary for the operation of the trust network.  An identification service provider belonging to a trust network shall, in both the interfaces referred to in subsection 1, paragraphs 1 and 2, provide at least one technical interface that meets a universally applied standard.  **M72B, section 14: Data transfer protocol and other requirements**  **14.1 Data transfer protocol**  The identification service provider must enable the chaining of initial identification in accordance with section 17 of the Identification and Trust Services Act and relaying identification events within the trust network in accordance with section 12 a of the Identification and Trust Services Act using an interface conforming to at least either the Open IDConnect or SAML protocol. |  | **Application: M72B, section 14.1: stricter requirement of “an interface conforming to at least either the OpenID Connect or SAML protocol"** The Finnish Transport and Communications Agency has provided recommended profiles for the SAML and Open IDConnect protocols taking into account recommendations given by the trust network collaboration group.  212/2023 S Finnish Trust Network SAML 2.0 Protocol Profile version 2.1  213/2023 S Finnish Trust Network OpenID Connect 1.0 Protocol Profile version 2.1  The recommendations are available online at <https://www.kyberturvallisuuskeskus.fi/en/electronic-identification> |
|  | S, H | The identification means provider offers the required information (attributes) for the identification of **natural persons**. | **M72B, section 12: Minimum set of data to be relayed in a trust network**  **12.1 Mandatory set of data**  The following minimum set of data shall be relayed at the interface between the identification means provider and the provider of an identification broker service:  1) in identification events concerning natural persons: at least the first name, family name, date of birth and the unique identifier of the person authenticated by the identification means provider;  3) an indication of whether the level of assurance is substantial or high; […] |  | The broker service can enrich or filter the data received from the identification means provider as needed (see M72B, section 12.3). In any case, the identification means provider must relay data in accordance with M72B, section 12.1. |
|  | S, H | The identification means provider has the required **planned capacity** to provide the optional data for the identification of **natural persons**. | **M72B, section 12: Minimum set of data to be relayed in a trust network**  **12.2 Optional information**  The interface between the identification means provider and the provider of an identification broker service must have the technically planned possibility to relay the following information:  1) an indication of whether the identification event concerns a public administration eService or a private eService;  2) in identification events concerning natural persons: forename(s) and surname(s) at the time of birth, place of birth, current address and gender; […] |  | MPS72, section 12.1: explanation, p. 56:  Being prepared to relay optional attributes means that the processing of optional attributes in the interface and identification schemes must be designed in a way where the identification service provider knows which technical measures are needed for the introduction of the attributes. Technical implementation of optional attributes in systems is not required. However, in the technical configurations, it should be ensured that the optional attributes will not impede identification events, even in those cases where their use has not been agreed upon. A documented plan must, however, be made for supervisory purposes. |
|  | S, H | The identification means provider offers the required information (attributes) for the identification of **legal persons**. | **M72B, section 12: Minimum set of data to be relayed in a trust network**  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:  […]  2) in identification events concerning legal persons: at least the first name, family name and the unique identifier of the natural person representing the legal person as well as the unique identifier of the organisation authenticated by the identification means provider; and  3) an indication of whether the level of assurance is substantial or high; […] |  | Only if strong electronic identification of legal persons is offered. |
|  | S, H | The identification means provider has the required planned capacity to provide the optional data for the identification of **legal persons**. | **M72B, section 12: Minimum set of data to be relayed in a trust network**  **12.2 Optional information**  The interface between the identification means provider and the provider of an identification broker service must have the technically planned possibility to relay the following information:  1) an indication of whether the identification event concerns a public administration eService or a private eService;  […]  3) in identification events concerning legal persons:  a) current address;  b) VAT registration number;  c) tax reference number;  d) the identifier related to Article 3(1) of Directive 2009/101/EC of the European Parliament and of the Council;  e) Legal Entity Identifier (LEI) referred to in Commission Implementing Regulation (EU) No 1247/2012;  f) Economic Operator Registration and Identification (EORI) referred to in Commission Implementing Regulation (EU) No 1352/2013; and  g) excise number provided in Article 2(12) of Council Regulation (EC) No 389/2012. |  |  |

# Technical information security requirements

|  |
| --- |
| KEY PROVISIONS  M72B, section 15: Conformity assessment criteria  The identification service assessment shall cover the requirements concerning the following:  1) certain properties of the functions affecting the provision of the identification service (the identification scheme), namely:  d) technical measures (controls)  ITSA, section 8: Requirements posed on the electronic identification scheme  4) The identification scheme is reliable and safe so that, at a minimum, it meets the conditions for assurance level substantial laid down in sections … 2.4.6 of the Annex to the Act on Level of Assurance in Electronic Identification and takes into account the threats to the information security of the technology available at the time  LOA Annex, section 2.4.6: Technical controls  1) The existence of proportionate technical controls to manage the risks posed to the security of the services, protecting the confidentiality, integrity and availability of the information processed.  M72B, section 5: Technical information security measures of the identification scheme  5.1 The resistance of the identification scheme  5.1.1  The communications and information systems of the identification scheme and their operation must be planned, executed and maintained throughout the lifecycle of the service so that the integrity and confidentiality of the identification service are protected. The identification service must be able to resist at least moderate or high-level threats and attack potential specified in section 2.3 of the appendix to the regulation on *Level of Assurance in Electronic Identification* in accordance with the assurance level of the identification service.  5.1.2  The encryption requirements concerning communications connections between identification service providers and the identification service and the relying party are specified in section 7. The encryption of other communications connections of the identification scheme and information systems and data must employ encryption methods specified in section 7 of the regulation, where technically applicable, unless the overall ability of the system to protect itself is otherwise realised by other security means.  5.2 Communications security  The identification scheme communications must be planned, executed and maintained with:   1. structural network security; 2. zoning of the communications network; 3. filtering rules according to the principle of least privilege; 4. administration of filtering and control systems; 5. secure administration connections; as well as 6. employing internationally or nationally recommended encryption methods.   5.3 Information systems security  The identification scheme information systems must be planned, executed and maintained with:   1. access control according to the principle of least privilege; 2. unique identification of the users of the systems; 3. hardening of the systems; 4. malware protection; 5. ability to trace security events and tracing procedure; 6. ability to detect security incidents and repair procedure; as well as 7. employing internationally or nationally recommended encryption methods.   5.4 Safety of operation  The identification scheme operation must be planned, executed and maintained with:   1. change management; 2. confidential data processing environment and storage based on data classification; 3. protecting remote use and administration from threats in the remote use environment; 4. software development and software vulnerability management; 5. backup procedures; and 6. employing internationally or nationally recommended encryption methods.   5.5 Administration and remote connections of the production network of the identification scheme  The production network together with its administration connections and remote access and remote administration referred to in subsections 5.2.e) and 5.4.c) above must be implemented in such a way that the information security threats caused by other services of the organisation, such as e-mail or web browsing, or information security threats caused by other functions than those essential to administration in a terminal used for the administration, are   1. specifically assessed and minimised at a substantial assurance level, and 2. prevented when assessed as a whole at a high assurance level. |

## Communications security

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 3.1 Communications security | | | | | |
| **NO.** | **LEVEL OF ASSURANCE** | **REQUIREMENT PERTAINING TO THE IDENTIFICATION SERVICE (SUMMARY)** | **PROVISIONS** | **STANDARD REFERENCE** | **NOTES** |
|  | S, H | Security of data communication:  The **data communication connections, control connections and processes** (data communications of subprocesses related to the production of identification services, including the administration of the service) and their **security policies** are **identified, documented and maintained**.  Zoning of the communications network and the filtering rules used in the identification scheme must follow the principles of least privilege and defence in depth. | **M72B, section 5.2: Communications security**  The identification scheme communications must be planned, executed and maintained with:   1. structural network security; 2. zoning of the communications network; 3. filtering rules according to the principle of least privilege; 4. administration of filtering and control systems; 5. secure administration connections; as well as 6. employing internationally or nationally recommended encryption methods.   **LOA Annex, section 2.4.6: Technical controls**  2. Electronic communication channels used to exchange personal or sensitive information are protected against eavesdropping, manipulation and replay. | A.8.1.1 Inventory of assets  A.13.1 Communications security / Network security management:  A.13.1.1 Network controls  A.13.1.3 Segregation in networks | The overall architecture of the identification scheme must ensure the security of data communication.  Important: The planning of the identification scheme must also take all relevant data communications with subcontractors (infrastructure, software applications, operator services, ID card production, etc.) into account.  The notification/**assessment report** must include a description of the system architecture including the data communications between different system components and their protection policies. The documentation must clearly describe the network areas of various security levels as well as the filter and control systems between them. |
|  | S, H | Security of data communication:  The **data communication equipment and systems** of the identification scheme are identified and documented. | **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  **M72B, section 5.2: Communications security**  The identification scheme communications must be planned, executed and maintained with:  a) structural network security | A.8.1.1 Inventory of assets |  |
|  | S, H | Security of data communication:  The **production network** must be **separated** from the administration and maintenance network.  The administration and maintenance network must be separated from office networks.  A development environment separate from the production environment is in place. | **M72B, section 5.2: Communications security**  The identification scheme communications must be planned, executed and maintained with:  a) structural network security  b) zoning of the communications network;  […]  **5.5 Administration and remote connections of the production network of the identification scheme**  The production network together with its administration connections and remote access and remote administration referred to in subsections 5.2.e) and 5.4.c) above must be implemented in such a way that the information security threats caused by other services of the organisation, such as e-mail or web browsing, or information security threats caused by other functions than those essential to administration in a terminal used for the administration, are  a) specifically assessed and minimised at a substantial assurance level, and  b) prevented when assessed as a whole at a high assurance level. | A.12.1.4 Operations security: Separation of development, testing and production environments | 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. |
|  | S, H | Security of data communication:  The data communication connections of the identification scheme are **filtered** based on the least privilege principle. | **M72B, section 5.2: Communications security**  The identification scheme communications must be planned, executed and maintained with:  […]  c) filtering rules according to the principle of least privilege;  d) administration of filtering and control systems;  […] | A.13.1.1–3 Communications security / Network security management:  A.13.1.1 Network controls  A.13.1.2 Security of network services  A.13.1.3 Segregation in networks  See also access control |  |
|  | S, H | Security of data communication:  **Links from the production network to the public network** must be risk-based and used only to enable the functionalities of the service. | **M72B, section 5.2: Communications security**  The identification scheme communications must be planned, executed and maintained with:  a) structural network security  […]  c) filtering rules according to the principle of least privilege;  d) administration of filtering and control systems;  e) secure administration connections; as well as  […]  **5.5 Administration and remote connections of the production network of the identification scheme**  The production network together with its administration connections and remote access and remote administration referred to in subsections 5.2.e) and 5.4.c) above must be implemented in such a way that the information security threats caused by other services of the organisation, such as e-mail or web browsing, or information security threats caused by other functions than those essential to administration in a terminal used for the administration, are  a) specifically assessed and minimised at a substantial assurance level, and  b) prevented when assessed as a whole at a high assurance level. | See previous row. | Any other links except those necessary for operations are expressly prohibited or must be closed. |
|  | S, H | Security of data communication:  **Cryptographic key materials** and **metadata** is exchanged safely between the identification services and the relying parties. | **M72B, section 8: Authenticating parties to the communications**  **8.1 Verification of the parties to the communications connection**  The authenticity and integrity of the digital certificates or keys used to encrypt the communications or messages as well as their holders must be verified in establishing communications connections between identification services and identification services and relying parties.  The authentication must be based on a qualified electronic signature or a qualified electronic seal in compliance with the eIDAS Regulation or a direct bilateral procedure. Authentication may not only be based on a generally trusted digital certificate.  **8.2 Certificate and key renewal**  The digital certificates and keys referred to in section 8.1 above must be regularly renewed.  In order to ensure the authenticity and integrity of new digital certificates and keys, the renewal must be carried out in one of the following ways:   1. in accordance with the procedure in section 8.1; 2. by providing new keys via a communications connection, whose integrity and confidentiality has been ensured by binding the parties’ communications to digital certificates or keys provided in accordance with section 8.1; or 3. by signing a new key using a key provided in accordance with section 8.1 or a key chained from such a key.   **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.  […]  5. All media containing personal, cryptographic or other sensitive information is stored, transported and disposed of in a safe and secure manner.  **LOA, section 2.4.6: Technical controls**  Substantial: Sensitive cryptographic material, if used for issuing electronic identification means and authentication, is protected from tampering.  **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 communication by an attacker with enhanced-basic attack potential can subvert the authentication mechanisms. | A.10.1.2 Cryptography / Key management | cf. PSD2/RTS eIDAS art45 or eSeal certificate requirements for the identification of the parties.  A predefined process exists between the parties for establishing safe trust, authenticating parties and exchanging permanent keys/secrets.  The processes and practices of private key management are documented and appropriately implemented.  The processes require at least the use of cryptographically strong keys, secure key distribution, secure key storage, regular key exchanges, replacement of old or revealed keys and the prevention of unauthorised key exchanges.  KATAKRI 2015 (I12) |
|  | H | Security of data communication:  Cryptographic key materials and metadata is exchanged safely between the identification services and the relying parties. | cf. above and **LOA 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. | A.10.1.2 Cryptography / Key management |  |
|  | S, H | The identification messages of the identification service (broker service or relaying own means) provider and relying party must be authenticated. | M72B, section 9.1.2  Authentication messages between identification broker services and relying parties must be authenticated with signatures. |  |  |
|  | S, H | The integrity and confidentiality of authentication messages is ensured. | **M72B, section 9.1.1**  The integrity and confidentiality of authentication messages containing personal data must be protected in communications between identification services and between identification services and relying parties in one of the following ways:  a) by ensuring the integrity and confidentiality of the communications connection by binding the parties’ communications to digital certificates or keys provided in compliance with section 8, or  b) by encrypting and signing the messages with a key provided in compliance with the procedure in section 8.  **LOA Annex, section 2.4.6: Technical controls**  1. The existence of proportionate technical controls to manage the risks posed to the security of the services, protecting the confidentiality, integrity and availability of the information processed.  2. Electronic communication channels used to exchange personal or sensitive information are protected against eavesdropping, manipulation and replay. |  | Section 8 describes different methods for implementing the required communications security. |
|  | S, H | Security of data communication:  **Administration of the filtering and control systems** of the network connections used in the identification scheme are well organised. | **M72B, section 5.2: Communications security**  The identification scheme communications must be planned, executed and maintained with:  […]  d) administration of filtering and control systems;  e) secure administration connections; as well as  […] | A.13.1 Communications security / Network security management:  A.13.1.1 Network controls |  |
|  | 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. | **M72B, section 5.2: Communications security**  The identification scheme communications must be planned, executed and maintained with:  […]  d) administration of filtering and control systems;  e) secure administration connections; as well as  […]  **5.4 Safety of operation**  The identification scheme operation must be planned, executed and maintained with:  […]  c) protecting remote use and administration from threats in the remote use environment;  […]  **5.5 Administration and remote connections of the production network of the identification scheme**  The production network together with its administration connections and remote access and remote administration referred to in subsections 5.2.e) and 5.4.c) above must be implemented in such a way that the information security threats caused by other services of the organisation, such as e-mail or web browsing, or information security threats caused by other functions than those essential to administration in a terminal used for the administration, are  a) specifically assessed and minimised at a substantial assurance level, and  […] | 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: Segregation in networks | 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. |
|  | 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). | **M72B, section 5.2: Communications security**  The identification scheme communications must be planned, executed and maintained with:  […]  d) administration of filtering and control systems;  e) secure administration connections; as well as  […]  **5.4 Safety of operation**  The identification scheme operation must be planned, executed and maintained with:  […]  c) protecting remote use and administration from threats in the remote use environment;  […]  **5.5 Administration and remote connections of the production network of the identification scheme**  The production network together with its administration connections and remote access and remote administration referred to in subsections 5.2.e) and 5.4.c) above must be implemented in such a way that the information security threats caused by other services of the organisation, such as e-mail or web browsing, or information security threats caused by other functions than those essential to administration in a terminal used for the administration, are  […]  b) prevented when assessed as a whole at a high assurance level.  **MPS72B Explanatory Notes:**  At the high level of assurance, the requirements may be met at least by disabling access of a workstation in remote use to other services of the organisation, such as e-mail, and preventing the workstation from using other functions than those essential to the operation of the management network. In practice, this means that there shall be a separate workstation for management.  The assessment as a whole required at the high level of assurance means that if other workstations than such hardened workstations described above are used, the separation of the production system and other means for managing information security threats are taken into account in the implementation. In principle, such case requires a virtual termination or a KVM solution.  The key point here is what is done on the terminal taking the virtualised connection, and therefore, a two-factor VPN connection to a virtualised workstation alone is not a sufficient solution, for example. Using antivirus and web proxy is not sufficient, either.  When transferring necessary files from one terminal to another, the risk of malware shall also be taken into account, for instance, by ensuring the use of reliable sources only and safeguarding information security (integrity) using all appropriate methods. | See previous row. |  |

## Information system security

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 3.2 Information system security | | | | | |
| **NO.** | **LEVEL OF ASSURANCE** | **REQUIREMENT PERTAINING TO THE IDENTIFICATION SERVICE (SUMMARY)** | **PROVISIONS** | **STANDARD REFERENCE** | **NOTES** |
|  | S, H | Information system security:  The **information systems and processes** (processes using information systems that are related to the production of identification services, including the administration of the service) of the identification scheme are **identified, documented and maintained**.  The information systems of the identification scheme are **classified** based on the 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. | **M72B, section 5.3: Information systems security**  The identification scheme information systems must be planned, executed and maintained with:  a) access control according to the principle of least privilege;  b) unique identification of the users of the systems;  […] | A.8.1.1 Asset management / Responsibility for assets: Inventory of assets  A.8.2.1 Asset management / Information classification | Classification of information: the acceptable use of equipment, software application and other assets must be defined. |
|  | S, H | Information system security:  **Access privileges** of the identification scheme are defined and documented.    The access privileges are **based** on the classification of information systems and the tasks of each person/user.  Access must only be granted based on tasks following the principle of least privilege. | **M72B, section 5.3: Information systems security**  The identification scheme information systems must be planned, executed and maintained with:  a) access control according to the principle of least privilege;  b) unique identification of the users of the systems;  c) hardening of the systems;  […] | A.9.1.1 Business requirements of access control: Access control policy  A.9.1.2 Access to networks and network services  A.9.4.1 System and application access control: Information access restrictions | Access rights management is used to limit access to information and data processing environments in a systematic and documented manner. |
|  | S, H | Information system security:  The users of the information systems of the identification scheme **are identified** using a technique or method that is known and considered safe. | **M72B, section 5.3: Information systems security**  The identification scheme information systems must be planned, executed and maintained with:  a) access control according to the principle of least privilege;  b) unique identification of the users of the systems;  c) hardening of the systems;  […]  e) ability to trace security events and tracing procedure;  […] | 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. |
|  | S, H | Information system security:  Access privileges are controlled and **maintained so they are up to date**. | **M72B, section 5.3: Information systems security**  The identification scheme information systems must be planned, executed and maintained with:  a) access control according to the principle of least privilege;  b) unique identification of the users of the systems;  c) hardening of the systems;  […]  e) ability to trace security events and tracing procedure;  f) ability to detect security incidents and repair procedure; as well as  […] | 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 |  |
|  | S, H | Information system security:  Staff **duties and functions must be defined** to prevent a situation where one person could cause a severe security incident through their own actions deliberately or by accident (high-risk job combinations). | **M72B, section 5.3: Information systems security**  The identification scheme information systems must be planned, executed and maintained with:  a) access control according to the principle of least privilege;  b) unique identification of the users of the systems;  c) hardening of the systems;  […]  e) ability to trace security events and tracing procedure;  f) ability to detect security incidents and repair procedure; as well as  ~~[…]~~ |  | For example, the possibility of a dishonest or negligent employee granting an identification means in violation of the requirements can be prevented through task definitions and other controls that reduce the risk of error and abuse.  As for other sections, the assessment must take both moderate and high attack potentials into account as required by the assurance levels for each identification means. |
|  | S, H | Information system security:  **Hardening** of the identification scheme is ensured; a procedure is in place for the systematic installation of systems, resulting in a hardened installation.  The identification scheme **only** uses the services, functions, processes, equipment and components specifically **required** for its operation. Their usage is defined so that all unnecessary access rights and functions/elements are removed from the installations. | **M72B, section 5.3: Information systems security**  The identification scheme information systems must be planned, executed and maintained with:  […]  c) hardening of the systems;  […] | A.12.5. Control of operational software | See also data communications.  Guideline 211/2016 included the following criteria, which are included here for reference:  A hardened installation only contains the components and services as well as user and process rights that are essential for meeting operational requirements and ensuring security.  Only the functions, hardware and services essential for operating requirements and data processing are in use. |
|  | S, H | Information system security:  Identification, prevention and correction of adverse impacts and threats caused by **malware** is ensured. | **M72B, section 5.3: Information systems security**  The identification scheme information systems must be planned, executed and maintained with:  […]  d) malware protection;  e) ability to trace security events and tracing procedure;  f) ability to detect security incidents and repair procedure; as well as  […] | A.12.2 Protection from malware  A.12.6 Technical vulnerability management | See also incident observation capacity. |
|  | S, H | Information system security:  The identification scheme uses fully recommendable **encryption solutions**. | **M72B, section 5.3: Information systems security**  The identification scheme information systems must be planned, executed and maintained with:  […]  g) employing internationally or nationally recommended encryption methods. | A.10.1 Cryptographic controls  A.18.1.5 Regulation of 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) |
|  | 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 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.  **M72B, section 5.3: Information systems security**  The identification scheme information systems must be planned, executed and maintained with:  a) access control according to the principle of least privilege;  b) unique identification of the users of the systems;  c) hardening of the systems;  […]  g) employing internationally or nationally recommended encryption methods.  **M72B, section 5.4: Safety of operation**  The identification scheme operation must be planned, executed and maintained with:  […]  b) confidential data processing environment and storage based on data classification;  […]  f) employing internationally or nationally recommended encryption methods. | A.8.2.1 Classification of information  A.10.1.1 Policy on the use of cryptographic controls  A.10.1.2 Cryptography / Key management | Guideline 211/2016 included the following observations, which are included here for reference:  Private keys shall only be available to authorised users and processes.  The processes and practices of private key management are documented and appropriately implemented.  The processes require at least the use of cryptographically strong keys, secure key distribution, secure key storage, regular key exchanges, replacement of old or revealed keys and the prevention of unauthorised key exchanges.  KATAKRI 2015 (I12) |

## Operator security

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 3.3 Operator security | | | | | |
| **NO.** | **LEVEL OF ASSURANCE** | **REQUIREMENT PERTAINING TO THE IDENTIFICATION SERVICE (SUMMARY)** | **PROVISIONS** | **STANDARD REFERENCE** | **NOTES** |
|  | **S, H** | Operator security:  **Change management** of the identification scheme is planned and careful. | **M72B, section 5.4: Safety of operation**  The identification scheme operation must be planned, executed and maintained with:  a) change management;  […] | A.12.1.2 Operations security / Operational procedures and responsibilities: Change management  A.14.2.2 System acquisition, development and maintenance / Security in development and support processes: System change control procedures  A.14.2.3 Technical review of applications after operating platform changes  A.14.2.4 Restrictions on changes to software packages | Clear processes have been defined for change management. In the implementation of new features or changes, the testing plan also takes into account negative test cases. Testing is not based solely on automatic tests. |
|  | 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  **M72B, section 5.4: Safety of operation**  The identification scheme operation must be planned, executed and maintained with:  […]  d) software development and software vulnerability management;  […] | A.12.5.1 Operations security: Installation of software on operational systems  A.12.6.1 Operations security: Management of technical vulnerabilities  A.14.2 System acquisition, development and maintenance / Security in development and support processes  A.14.2.1 Secure development policy  A.14.2.2 System change control procedures  A.14.2.3 Technical review of applications after operating platform changes  A.14.2.4 Restrictions on changes to software packages  A.14.2.5 Secure system design principles  A.14.2.6 Secure development environment  A.14.2.7 Outsourced development  A.14.2.8 System security testing  A.14.2.9 System acceptance testing | The organisation must maintain a database or listing of all different software components of the identification scheme.  The organisation must have a process for the detection and monitoring of software vulnerabilities. Exposed software components must be updated to current versions.  The software used in the identification scheme must comply with secure programming principles.  New versions of the identification scheme must be tested, also by including negative test cases. |
|  |  | Operator security:  The identification scheme operation must be planned, executed and maintained with:  Software development management | **M72B, section 5.4: Safety of operation**  The identification scheme operation must be planned, executed and maintained with:  a) change management;  […];  d) software development and software vulnerability management;  […] | See previous | The management of software development must pay particular attention to the supply chain structure and maintain information about the different components of the software and monitor their updates.  Safe software development  Testing |
|  | 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.  **M72B, section 5.4: Safety of operation**  The identification scheme operation must be planned, executed and maintained with:  […]  e) backup procedures; and  […] | A.12.3.1 Information backup | Guideline 211/2016 included the following observations, which are included here for reference:  The physical location of back-up copies is sufficiently separate from the actual system. |

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

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| KEY PROVISIONS  M72B, section 15: Conformity assessment criteria  The identification service assessment shall cover the requirements concerning the following:  1) certain properties of the functions affecting the provision of the identification service (the identification scheme), namely:  d) technical measures (controls)  General requirements  ITSA, section 8: Requirements posed on the electronic identification scheme  4) The identification scheme is reliable and safe so that, at a minimum, it meets the conditions for assurance level substantial laid down in sections … 2.4.6 of the Annex to the Act on Level of Assurance in Electronic Identification and takes into account the threats to the information security of the technology available at the time  LOA Annex, section 2.4.6: Technical controls  1. The existence of proportionate technical controls to manage the risks posed to the security of the services, protecting the confidentiality, integrity and availability of the information processed.  4. Procedures exist to ensure that security is maintained over time and that there is an ability to respond to changes in risk levels, incidents and security breaches.  ITSA, section 16: Notifications of the identification service provider concerning threats or disruptions to their operations and protection of data  Notwithstanding any secrecy provisions, an identification service provider shall inform the parties relying on their identification service, holders of identification means, other agreement parties operating in the trust network and the Finnish Transport and Communications Agency without undue delay of all significant threats or disruptions to the operation of the service, information security or the use of an electronic identity. […]  The notification specified in subsection 1 above shall also include information about measures the parties involved have for use to counter such threats and risks, as well as the estimated expenses incurred by these measures.  …  The requirements are specified in M72B, sections 5 and 11. | | | | | |
| **NO.** | **LEVEL OF ASSURANCE** | **REQUIREMENT PERTAINING TO THE IDENTIFICATION SERVICE (SUMMARY)** | **PROVISIONS** | **STANDARD REFERENCE** | **NOTES** |
|  | 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.  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. | **M72B, section 5.2: Communications security**  The identification scheme communications must be planned, executed and maintained with:  […]  d) administration of filtering and control systems;  […]  **M72B, section 5.3: Information systems security**  The identification scheme information systems must be planned, executed and maintained with:  a) access control according to the principle of least privilege;  b) unique identification of the users of the systems;  […]  e) ability to trace security events and tracing procedure;  f) ability to detect security incidents and repair procedure; as well as  […] | A.12.4.1 Operations security: Event logging  A.12.4.2 Operations security: Protection of log information  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  A.16.1.6 Learning from information security incidents | The processes contain both automatic and manual means. The processes are maintained. |
|  | S, H | The **control logs** of the identification scheme are defined and separated from other log data. Their integrity is ensured. | **M72B, section 5.2: Communications security**  The identification scheme communications must be planned, executed and maintained with:  […]  d) administration of filtering and control systems;  e) secure administration connections; as well as  […]  **M72B, section 5.3: Information systems security**  The identification scheme information systems must be planned, executed and maintained with:  a) access control according to the principle of least privilege;  b) unique identification of the users of the systems;  […]  e) ability to trace security events and tracing procedure;  f) ability to detect security incidents and repair procedure; as well as  […] | A.12.4.1 Operations security: Event logging  A.12.4.2 Operations security: Protection of log information  A.12.1.4 Separation of development, testing and operational environments | Information on changes implemented in the identification scheme are saved in control logs. |
|  | S, H | The operation, changes and events in the identification scheme are **monitored** to detect any irregularities and information security violations.  **Irregularities and malfunctions of the identification scheme are processed and analysed**, and their impact/severity is classified in a systematic and organised manner. | **M72B, section 5.2: Communications security**  The identification scheme communications must be planned, executed and maintained with:  […]  d) administration of filtering and control systems;  […]  **M72B, section 5.3: Information systems security**  The identification scheme information systems must be planned, executed and maintained with:  […]  e) ability to trace security events and tracing procedure;  f) ability to detect security incidents and repair procedure; as well as  […] | A.16.1 Information security incident management / Management of information security incidents, events and weaknesses:  A.16.1.2 Reporting information security events  A.16.1.3 Reporting information security weaknesses  A.16.1.4 Assessment and decision on information security events | All observations are discussed and their impact is classified according to predetermined criteria.  Log analysis is performed with automatic processes/tools, such as SIEM. |
|  |  | **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. | **M72B, section 5.2: Communications security**  The identification scheme communications must be planned, executed and maintained with:  […]  d) administration of filtering and control systems;  […]  **M72B, section 5.3: Information systems security**  The identification scheme information systems must be planned, executed and maintained with:  […]  e) ability to trace security events and tracing procedure;  f) ability to detect security incidents and repair procedure; as well as  […] | A.16.1 Information security incident management / Management of information security incidents, events and weaknesses:  A.16.1.5 Response to information security incidents  7.5 Documented information  10.1 Nonconformity and corrective action | Corrective measures must be documented.  Service-level agreements (SLA) are contractual matters. Their non-discriminatory nature must be ensured. |
|  | S, H | The incident management processes feature a **requirement to report to other identification services within the trust network.** | **ITSA, section 16: Notifications of the identification service provider concerning threats or disruptions to their operations and protection of data**  Notwithstanding any secrecy provisions, an identification service provider shall inform […] other agreement parties operating in the trust network […] without undue delay of all significant threats or disruptions to the operation of the service, information security or the use of an electronic identity. […]  An identification service provider can, without prejudice to secrecy provisions, notify all members of a trust network of the threats and disruptions referred to in subsection 1 and of service providers of whom there is reason to believe that they are seeking unauthorised financial gain, giving false or misleading information that is significant or processing personal data illegally.  **Application:**  The trust network collaboration group has drafted a joint policy for malfunction situations requiring mutual notification as well as notification thresholds. | 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. |
|  | S, H | The incident management process features a **requirement to notify users and relying parties.** | **ITSA, section 16: Notifications of the identification service provider concerning threats or disruptions to their operations and protection of data**  An identification service provider shall inform the parties relying on their identification service, holders of identification means, […] without undue delay of all significant threats or disruptions to the operation of the service, information security or the use of an electronic identity. The notification shall also include information about measures the parties involved have for use to counter such threats and risks, as well as the estimated expenses incurred by these measures. | A.16.1.2 Information security incident management / Management of information security incidents, events and weaknesses: Reporting information security events | Responsibilities related to incidents and stakeholder communications have been defined.  Relying parties mean eServices. |
|  | S, H | The incident management process features a **requirement to notify the Finnish Transport and Communications Agency.** | **ITSA, section 16: Notifications of the identification service provider concerning threats or disruptions to their operations and protection of data**  Notwithstanding any secrecy provisions, an identification service provider shall inform […] the Finnish Transport and Communications Agency without undue delay of all significant threats or disruptions to the operation of the service, information security or the use of an electronic identity. The notification shall also include information about measures the parties involved have for use to counter such threats and risks, as well as the estimated expenses incurred by these measures.  **M72B, section 11: Incident notifications by the identification service provider to the Finnish Transport and Communications Agency**  **11.1 Significant threats and disruptions**  Significant disruptions to the identification service that need to be reported to the Finnish Transport and Communications Agency according to section 16 of the Identification and Trust Services Act include events that are connected to incorrectness or abuse of electronic identity or to an information security threat or disruption that compromises the integrity and reliability of identification. Unforeseeable disruptions with greater than minor effects on the trust network are also considered significant.  **11.2 Reported information**  Notifications of significant threats or disruptions provided to the Finnish Transport and Communications Agency shall contain at least the following information:  1) identification means or identification broker service affected by the disruption or threat;  2) description of the disruption or threat and any known reasons for it and its duration;  3) description of the impact of the disruption or threat, including the impact on the issuance of new identification means, their users, relying parties, other parties of the trust network, and cross-border use;  4) description of corrective measures; and  5) description of the provision of information on the disruption or threat to relying parties, identification means holders and the trust network as well as information on notifying other authorities.  **11.3 Reporting procedure**  Significant disruptions or threats must be reported to the Finnish Transport and Communications Agency electronically by using an online form, e-mail or secure e-mail.  The report may be amended later on if all of the information is not available at the time of the initial report submitted without undue delay in accordance with section 16 of the Identification and Trust Services Act.  **MPS72B explanatory note on the threshold of notification to the Finnish Transport and Communications Agency,** chapter 4.11.1 Provision 11.1:  Section 11.1 of the Regulation defines, at a general level, the factors deemed relevant in judging the significance of the disturbance or threat, i.e. the notification threshold. Such significant disturbances include:  issuing an identification means to the wrong person  disturbances related to the functioning of a revocation list in which an up-to-date revocation list is not available  intrusions in the systems of the service provider  disclosure of the identification means provider’s certificate signature keys  serious abuse of identification means, such as incidents related to the chaining of identification means  serious internal misconduct.  The threshold for deeming faults or abuse related to electronic identities significant is very low, and the same applies to vulnerabilities or flaws that compromise the correctness of the identification data. With respect to usability or quality issues, on the other hand, the notification threshold is, in principle, somewhat higher, and they are deemed more significant mainly in the cases where the issue affects other trust network parties. Such issues include extended disruptions in the identification means or identification broker service that prevent the provision of identification services to e-services. Extended disruptions preventing the chaining of initial identification are significant. | A.16.1.2 Information security incident management / Management of information security incidents, events and weaknesses: Reporting information security events | The document on the notification threshold defined by the trust network is complied with. [document number]  Responsibilities related to incidents and stakeholder communications have been defined. |

# Storage and handling of data

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| M72B, section 15: Conformity assessment criteria  The identification service assessment shall cover the requirements concerning the following:  1) certain properties of the functions affecting the provision of the identification service (the identification scheme), namely:  b) record keeping and data processing;  d) technical measures (controls)  General requirements  ITSA, section 13: General obligations of an identification service provider  The storage of data, the personnel and subcontracted services used by an identification service provider in association with identification shall, at a minimum, meet the requirements laid down for assurance level substantial in sections 2.4.4 and 2.4.5 of the Annex to the Act on Level of Assurance in Electronic Identification.  […]  The identification service provider shall also protect personal data referred to in section 32 of the Personal Data Act and ensure adequate information security.  LOA Annex, section 2.4.4: Record keeping   1. Record and maintain relevant information using an effective record-management system, taking into account the applicable legislation and good practice in relation to data protection and data retention. 2. Retain, as far as it is permitted by national law or other national administrative arrangement, and protect records for as long as they are required for the purpose of auditing and investigation of security breaches, and retention, after which the records shall be securely destroyed.   ITSA, section 8: Requirements posed on the electronic identification scheme  4) The identification scheme is reliable and safe so that, at a minimum, it meets the conditions for assurance level substantial laid down in sections … 2.4.6 of the Annex to the Act on Level of Assurance in Electronic Identification and takes into account the threats to the information security of the technology available at the time  LOA Annex, section 2.4.6: Technical controls  1. The existence of proportionate technical controls to manage the risks posed to the security of the services, protecting the confidentiality, integrity and availability of the information processed.  Sensitive cryptographic material, if used for issuing electronic identification means and authentication, is protected from tampering. | | | | | |
| **NO.** | **LEVEL OF ASSURANCE** | **REQUIREMENT PERTAINING TO THE IDENTIFICATION SERVICE (SUMMARY)** | **PROVISIONS** | **STANDARD REFERENCE** | **NOTES** |
|  | 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.  **M72B, section 5.4: Safety of operation**  The identification scheme operation must be planned, executed and maintained with:  […]  b) confidential data processing environment and storage based on data classification; | A.8.2.1 Asset management / Information classification: Classification of information  A.18.1.4 Compliance / Compliance with legal and contractual requirements: Privacy and protection of personally identifiable information | The classification takes cryptographic information, identification event information, personal data, business secrets and information related to system security into account. |
|  | 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.  **M72B, section 5.4: Safety of operation**  The identification scheme operation must be planned, executed and maintained with:  […]  b) confidential data processing environment and storage based on data classification; | A.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.  As a detail, using the attribute ftn\_chain\_level in connection with initial identification.  Guideline 211/2016 included the following observations, which are included here for reference:  A sufficiently long time shall be determined for the storage of log data in case of later inspection. |
|  | S, H | Compliance with the **specific data retention obligations specified in section 24 of the Identification Act** is ensured. | **ITSA, section 24: Storage and use of data regarding the identification event and means**  The identification service provider shall store:  1) data required for performing an individual authentication event and an electronic signature;  2) data on preclusions or restrictions on the use of identification means referred to in section 18; and  3) data content of the certificate as set out in section 19.  The provider of an identification means shall store the necessary data about the initial identification of an applicant referred to in section 17 and 17 a and the document or electronic identification used therein.  The data referred to above in section 1 subsection 1 shall be stored for five years from the authentication event. Other data referred to above in section 1 subsection 2 shall be stored for five years from the termination of a permanent customer relationship.  Personal data generated during the authentication event shall be destroyed after the event, unless they are required to be kept to verify an individual authentication event.  The identification service provider may process stored data only to perform and maintain the service, for invoicing, to protect its rights in case of disputes, to investigate misuse of personal data as well as upon request by the service provider using the identification service or the holder of the identification means. The identification service provider shall store data on processing, the time, reason, and person processing it.  If the service provider only issues identification means (devices):  1) subsection 1, paragraph 1 and subsection 4 do not apply to the provider;  2) The five-year record-keeping period referred to in subsection (3) above will then be calculated from the date the identification means validity expires. | A.12.4.1 Operations security: Event logging | “…*only issues identification means (devices)*" in the Act refers to identification services such as the Population Register Centre certificate where the provider of the identification means does not relay identification messages in an identification event. |
|  | S, H | **A special requirement of section 24** of the Identification Act on storing of information related to the processing of information that is required to be stored. | **Provisions on identification events and processing related to the identification service are given in section 24 of the Identification Act.**  **ITSA, section 24**  **…**  The identification service provider may process stored data only to perform and maintain the service, for invoicing, to protect its rights in case of disputes, to investigate misuse of personal data as well as upon request by the service provider using the identification service or the holder of the identification means. The identification service provider shall store data on processing, 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. |
|  | S, H | **Technical measures are taken to ensure the integrity and confidentiality of the information that is processed and stored** in the identification scheme. | **ITSA, section 8: Requirements posed on the electronic identification scheme**  4) The identification scheme is reliable and safe so that, at a minimum, it meets the conditions for assurance level substantial laid down in sections … 2.4.6 of the Annex to the Act on Level of Assurance in Electronic Identification and takes into account the threats to the information security of the technology available at the time  **LOA Annex, section 2.4.6: Technical controls**  1. The existence of proportionate technical controls to manage the risks posed to the security of the services, protecting the confidentiality, integrity and availability of the information processed.  Sensitive cryptographic material, if used for issuing electronic identification means and authentication, is protected from tampering.  **M72B, section 5.4: Safety of operation**  The identification scheme operation must be planned, executed and maintained with:  […]  b) confidential data processing environment and storage based on data classification;  […]  e) backup procedures; and  f) employing internationally or nationally recommended encryption methods.  **M72B, section 7: Identification scheme interface encryption requirements**  **7.1 Communications encryption methods**  7.1.1  Interfaces between identification service providers and interfaces between an identification service provider and relying parties shall be encrypted. The following methods shall be used in the encryption, key exchange, digital certificates and signing:   1. Key exchange: In key exchange, DHE methods or ECDHE methods with elliptic curves shall be used. The size of the finite field to be used in calculations shall be at least 2,048 bits in DHE and at least 224 bits in ECDHE. 2. Signature or asymmetric encryption: When using the RSA for electronic signatures or encryption, the key length shall be at least 2,048 bits. When using the ECDSA or EdDSA methods with elliptic curves, the size of the finite field must be at least 224 bits. 3. Symmetrical encryption: The encryption algorithm must be AES, Serpent or ChaCha20. The key length shall be at least 128 bits. The encryption mode must be CBC, CCM, GCM or CTR. 4. Hash functions: The hash function or authentication code must be SHA-2, SHA-3, Whirlpool or Poly1305.   7.1.2  In addition to methods and values mentioned in section 7.1.1, methods and values that have been assessed as secure in use specified in subsections 1–4 in the current versions of the following documents may also be complied with:   1. Kryptografiset vahvuusvaatimukset luottamuksellisuuden suojaamiseen - kansalliset turvallisuusluokat (Dnro 190/651/2015) instruction (in Finnish) issued by the Crypto Approval Authority operating within the Finnish Transport and Communications Agency, or 2. SOG-IS Crypto Evaluation Scheme Agreed Cryptographic Mechanisms of the SOGIS-MRA (Senior Officers Group for Information Systems, Mutual Recognition Agreement), an agreement between certain certification bodies of EU or EEA Member States.   7.1.3  Encryption settings shall be technically forced to the minimum levels listed above to avoid a situation where settings weaker than the minimum levels are adopted following connection handshakes.  **7.2 Communications encryption protocol**  If the TLS protocol is used, version 1.2 of TLS or newer shall be used. | A.9.1.1 Access control policy  A.9.1.2 Access to networks and network services  A.10.1.1 Policy on the use of cryptographic controls  A.12.4.2 Operations security: Protection of log information | Data encryption and/or access control.  Separation as required (cf. especially cryptographic material).  Backup copies/recoverability.  Key exchange as defined in the recommendation may be relevant between the identification service and its subcontractors although it is not relevant in drive encryption.  Managing and securing the secrets underlying the trust.  Storage must take the separation of the physical storage space from the actual system into account. |
|  | H | Strict/substantial-level encryption requirements as specified in the **recommendation** are followed in the processing and storage of data. | **MPS72B, section 4.7.1.3 (20 May 2022) recommendation**  At the high level of assurance, instead of using the requirements for substantial level of assurance provided in section 7.1 of the Regulation, it is recommended to apply the following values in parentheses, **which will meet the minimum assurance level of 128 bits**, to the identification scheme:  1) **Key exchange**: In key exchange, DHE methods or ECDHE methods with elliptic curves shall be used. The size of the finite field to be used in calculations shall be at least 2,048 (**4,096 at high level of assurance**) bits in DHE and at least 224 (**256 at high level of assurance**) bits in ECDHE.  The DH groups 14 to **21**, 23, 24 and 26 (**from 16 to 21** at high level of assurance) of IANA’s IKEv2 specifications meet the above requirements.  2) Signature or asymmetric encryption: When using the RSA for electronic signatures or encryption, the key length shall be at least 2,048 (**3,072 at high level of assurance**) bits. When using the elliptic curve method ECDSA or EdDSA, the underlying field size shall be at least 224 (**256 at high level of assurance**) bits.  3) Symmetrical encryption: The encryption algorithm must be AES, Serpent or ChaCha20 (***AES or Serpent* at high level of assurance**). The key length shall be at least 128 (**128 at high level of assurance**) bits. The encryption mode must be CBC, CCM, GCM or CTR.  4) Hash functions: The hash function or authentication code must be SHA-2, SHA-3, Whirlpool or Poly1305. SHA-2 refers to functions SHA224, SHA256, SHA384 and SHA512 (**SHA-3-256, SHA-3-384, SHA-3-512 at high level of assurance**). | See above. | Key exchange between the identification service and its subcontractors may be relevant here. |
|  | S, H | All **media** containing personal, cryptographic or other sensitive information is stored, transported and disposed of in a safe and secure manner. | **LOA Annex, section 2.4.6: Technical controls**  5) All media containing personal, cryptographic or other sensitive information is stored, transported and disposed of in a safe and secure manner.  **M72B, section 5.4: Safety of operation**  The identification scheme operation must be planned, executed and maintained with:  […]  b) confidential data processing environment and storage based on data classification;  […] | A.8.3 Asset management / Media handling  A.11.2.6 Security of equipment and assets off-premises  A.11.2.7 Secure disposal or re-use of equipment | Management, disposal and transfer. |

# Security of physical premises

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| M72B, section 15: Conformity assessment criteria  The identification service assessment shall cover the requirements concerning the following:  1) certain properties of the functions affecting the provision of the identification service (the identification scheme), namely:  c) facilities and […]  ITSA, section 8: Requirements posed on the electronic identification scheme  4) The identification scheme is reliable and safe so that [...] the premises used for providing an identification service are safe in compliance with the provisions laid down in section 2.4.5 of the Annex to the Act on Level of Assurance in Electronic Identification. | | | | | |
| **NO.** | **LEVEL OF ASSURANCE** | **REQUIREMENT PERTAINING TO THE IDENTIFICATION SERVICE (SUMMARY)** | **PROVISIONS** | **STANDARD REFERENCE** | **NOTES** |
|  | S, H | **Security of physical premises**  Facilities of the identification scheme are divided into security zones based on the confidentiality and criticality of the information that is processed. | **LOA Annex, section 2.4.5: Facilities and staff**  3. Facilities used for providing the service are continuously monitored for, and protected against, damage caused by environmental events, unauthorised access and other factors that may impact the security of the service.  4. Facilities used for providing the service shall ensure access to areas holding or processing personal, cryptographic or other sensitive information is limited to authorised staff or subcontractors. | A.11.1 Secure physical and environmental areas / Security perimeters:  A.11.1.1 Physical security perimeter | All facilities related to or affecting the production of the identification services, including subcontractors.  By default, KATAKRI compliance is sufficient, if the identification service is produced in said facilities. The scope of other standards has not been established. |
|  | 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.  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. | **LOA Annex, section 2.4.5: Facilities and staff**  3. Facilities used for providing the service are continuously monitored for, and protected against, damage caused by environmental events, unauthorised access and other factors that may impact the security of the service.  4. Facilities used for providing the service shall ensure access to areas holding or processing personal, cryptographic or other sensitive information is limited to authorised staff or subcontractors. | A.11.1.2 Physical entry controls    A.11.1.3 Securing 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 |  |
|  | S, H | Security perimeters are used to ensure that no **unauthorised** equipment or connections are used. | **LOA Annex, section 2.4.5: Facilities and staff**  3. Facilities used for providing the service are continuously monitored for, and protected against, damage caused by environmental events, unauthorised access and other factors that may impact the security of the service.  4. Facilities used for providing the service shall ensure access to areas holding or processing personal, cryptographic or other sensitive information is limited to authorised staff or subcontractors. | A.11 Physical and environmental security |  |

# Sufficiency and competence of human resources

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| M72B, section 15: Conformity assessment criteria  The identification service assessment shall cover the requirements concerning the following:  1) certain properties of the functions affecting the provision of the identification service (the identification scheme), namely:  c) […] and staff | | | | | |
| **NO.** | **LEVEL OF ASSURANCE** | **REQUIREMENT PERTAINING TO THE IDENTIFICATION SERVICE (SUMMARY)** | **PROVISIONS** | **STANDARD REFERENCE** | **NOTES** |
|  | S, H | **Availability and competence of staff**  The production organisation of the identification service must have sufficient expertise and human resources available to ensure information security and privacy. | **ITSA, section 13: General obligations of an identification service provider**  […] the personnel and subcontracted services used by an identification service provider in association with identification shall, at a minimum, meet the requirements laid down for assurance level substantial in sections … 2.4.5 of the Annex to the Act on Level of Assurance in Electronic Identification.  **LOA Annex, section 2.4.5: Facilities and staff**  Requirements concerning the facilities, personnel and (if applicable) subcontractors who carry out tasks related to the scope of application of this regulation. The requirements must be commensurate with the risk related to the level of assurance that is provided.  1. The existence of procedures that ensure that staff and subcontractors are sufficiently trained, qualified and experienced in the skills needed to execute the roles they fulfil.  2. The existence of sufficient staff and subcontractors to adequately operate and resource the service according to its policies and procedures. | A.7.2.2 Human resource security / During employment: Information security awareness, education and training | Assessment  - sufficiency of human resources considering the nature of the operations (24/7/365)  - assessment of technical controls; no precise requirements for the number of employees or on-call availability  - expertise in the required competence areas such as technical and legal competence (due to the processing of personal information). |
|  | S, H | Subcontracted services used in the identification scheme are identified and documented.  The competence and availability of the subcontractors’ personnel resources is ensured. | **See previous row.** | See previous row.  A.15.1.1 Information security policy for supplier relationships  A.15.2.1 Monitoring and review of supplier services | Information on subcontractors of the identification scheme (office systems, operator services, software applications, infrastructure...) and assessment of their human resources at least on a general level. |

# Information security management

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| M72B, section 15: Conformity assessment criteria  The identification service assessment shall cover the requirements concerning the following:  1) certain properties of the functions affecting the provision of the identification service (the identification scheme), namely:  a) information security management  M72B, section 4: Information security management system of the identification service provider  4.1 Information security management standard  The identification service provider must comply with the ISO/IEC 27001 standard or another corresponding, well-known information security management standard in the management of the information security of its identification scheme. Information security management may also be based on the combination of several standards.  4.2 Information security management scope  Information security management shall cover the following aspects concerning the provision of identification service:  1) overall context of the identification service provider;  2) governance, organisation and maintenance of information security management;  3) management of information security risks related to the provision of the identification service;  4) resources allocated to information security, competences, staff awareness of information security, communication, documentation and the management of documented information;  5) planning and steering of the provision of the identification service for the purpose of meeting information security requirements; and  6) evaluation of the efficiency and functionality of information security management.  ITSA, section 8: Requirements posed on the electronic identification scheme  An electronic identification scheme must fulfil the following requirements:  5) Information security management is ensured so that, at a minimum, the conditions for assurance level substantial laid down in the introduction to section 2.4 and in sections 2.4.3 and 2.4.7 of the Annex to the Act on Level of Assurance in Electronic Identification are met.  LOA Annex, section 2.4: Management and organisation  All participants providing a service related to electronic identification in a cross-border context (“providers”) shall have in place documented information security management practices, policies, approaches to risk management, and other recognised controls so as to provide assurance to the appropriate governance bodies for the electronic identification schemes in the respective Member States that effective practices are in place. Throughout section 2.4, all requirements/elements shall be understood as commensurate to the risks at the given level.  LOA Annex, section 1: Applicable definitions  4. ‘information security management system’ means a set of processes and procedures designed to manage to acceptable levels risks related to information security.  LOA Annex, section 2.4.7: Compliance and audit  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** |
|  | 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 Policies for information security | ISO 27001 compliance without substantial deviations is considered proof of meeting the information security management requirements. |
|  | S, H | The information security management system is based on a universally applied standard or set of standards. | **M72B, section 4: Information security management system of the identification service provider**  **4.1 Information security management standard**  The identification service provider must comply with the ISO/IEC 27001 standard or another corresponding, well-known information security management standard in the management of the information security of its identification scheme. Information security management may also be based on the combination of several standards. |  |  |
|  | S, H | The information security management system covers all substantial internal and external technical, legal and administrative requirements and needs with impacts on the identification scheme. | **M72B, section 4.2: Information security management scope**  Information security management shall cover the following aspects concerning the provision of identification service:  1) overall context of the identification service provider;  2) governance, organisation and maintenance of information security management;  […] | 4 Context of the Organisation | The identification service must follow current legislation and regulations, such as the Identification and Trust Services Act, Regulation 72 and the General Data Protection Regulation. |
|  | S, H | The information security management system covers the management, organisation and maintenance of the management procedures.  An up to date **information security policy** approved by the management of the organisation is in place. Security principles and policies are sufficiently extensive and appropriate for the organisation and the items to be protected.    Information security responsibilities of the staff and the subcontractors are defined. | **M72B, section 4.2: Information security management scope**  Information security management shall cover the following aspects concerning the provision of identification service:  […]  2) governance, organisation and maintenance of information security management;  […]  4) resources allocated to information security, competences, staff awareness of information security, communication, documentation and the management of documented information;  […] | 5 Leadership  9.2 Internal audit  9.3 Management review  10 Improvement  A.5.1.1 Policies for information security  A.6.1.1 Information security roles and responsibilities  A.15.1.1 Information security policy for supplier relationships |  |
|  | S, H | The information security management system covers the management of information security risks related to the offering of the identification service.  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. | **M72B, section 4.2: Information security management scope**  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;  […] | MPS72 reference:  6 Planning  8 Operation |  |
|  | S, H | The information security management system covers the resources allocated to information security, competence requirements, staff awareness of information security, communication, documentation and the management of documented information.  Up to date information security guidelines and policies are available to everyone working with tasks related to electronic identification.  Information security training given to the staff is regular and documented. Efficiency of the training is monitored. | **M72B, section 4.2: Information security management scope**  Information security management shall cover the following aspects concerning the provision of identification service:  […]  4) resources allocated to information security, competences, staff awareness of information security, communication, documentation and the management of documented information;  […] | MPS72:  7 Support |  |
|  | 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. | **M72B, section 4.2: Information security management scope**  Information security management shall cover the following aspects concerning the provision of identification service:  […]  5) planning and steering of the provision of the identification service for the purpose of meeting information security requirements; and  […] | 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) |
|  | S, H | The information security management system features regular assessment of information security efficiency and functionality. | **M72B, section 4.2: Information security management scope**  Information security management shall cover the following aspects concerning the provision of identification service:  […]  6) evaluation of the efficiency and functionality of information security management. | MPS72:  9.1 Monitoring, measurement, analysis and evaluation | How effective the information security management is concerning the factors, processes and problems that affect the information security of the identification scheme. |

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

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **M72B, section 15: Conformity 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  **ITSA, section 8: Requirements posed on the electronic identification scheme**  An electronic identification scheme must fulfil the following requirements:  1) The identification means shall be based on initial identification according to section 17 and section 17 a, where the relevant data can be verified afterwards as set out in section 24;  2) The identification means can be used for unambiguously identifying the holder of the identification means in a way that, at a minimum, fulfils the requirements on assurance level substantial laid down in sections 2.1.2, 2.1.3 and 2.1.4 of the Annex to the Commission Implementing Regulation (EU) 2015/1502 on setting out minimum technical specifications and procedures for assurance levels for electronic identification means pursuant to Article 8(3) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market, hereinafter *the Act on Level of Assurance in Electronic Identification*.;  […]  **ITSA, section 17: Identifying a natural person applying for an identification means**  The initial identification of a natural person shall be made personally or electronically in a way that fulfils the requirements for assurance level substantial or high laid down in section 2.1.2 of the Annex of the Act on Level of Assurance in Electronic Identification. The proofing of a person’s identity may be based on a document issued by an authority showing the person’s identity or a strong electronic identification means referred to in this Act. In addition, the proofing of an identity may be based on a procedure used at an earlier date by a public or private entity for a purpose other than the issuing of a strong electronic identification means, which the Finnish Transport and Communications Agency approves pursuant to regulations and regulatory control on the procedure, or pursuant to a confirmation by a conformity assessment body referred to in section 28, subsection 1.  In initial identification that is solely based on a document issued by an authority showing the person’s identity, the only acceptable documents are a valid passport or a personal identity card issued by an authority of a member state of the European Economic Area, Switzerland or San Marino. If the identification means provider so desires, they may also verify the identity from a valid passport granted by an authority of another state.  If the identity of an applicant cannot be reliably established, the police will perform the initial identification for the application. […]  **LOA Annex, section 2.1.2: Identity proofing and verification (natural person)**  **LEGAL PERSON**  **Requirements for granting of identification means to legal persons are not discussed in more detail in these criteria. In cases of an identification service provider offering strong identification means to legal persons, the assessment must take the applicable provisions into account.**  **ITSA, section 17 a: Identifying a legal person applying for an identification means**  The reported identity of a legal person must be verified from the Business Information Register or by means that, at a minimum, meet the requirements laid down for the identity proofing and verifying of a legal person at assurance level substantial laid down in section 2.1.3 of the Annex to the Act on Level of Assurance in Electronic Identification.  **ITSA, section 7 a: Using the data in the Business Information System**  The provider of an identification means and a certification service provider offering a trust service must use the Business Information System to obtain and update the data they need in order to be able to offer a service for identifying a legal person. The identification service provider shall also ensure that the data it needs for the 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**  **ITSA, section 2: Definitions**  7) initial identification means the verification of the identity of the applicant for an identification means in connection with the issuing of the means;  **LOA Annex, section 1: Applicable definitions**   1. 'authoritative source' means any source irrespective of its form that can be relied upon to provide accurate data, information and/or evidence that can be used to prove identity.   Standard: ETSI TS 119 461 | | | | | |
| **NO.** | **LEVEL OF ASSURANCE** | **REQUIREMENT PERTAINING TO THE IDENTIFICATION SERVICE (SUMMARY)** | **PROVISION** | **STANDARD** | **NOTES** |
| **Method 1: Initial identification is based on the presentation of an identity document approved in Finland** | | | | | |
|  | S, H | Identify proofing is based on approved identity documents defined in the Identification Act.  The acceptance of identity documents issued by countries other than those listed in the Act is clearly defined. | **ITSA, section 17**  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. |
|  | 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.  It is ensured that the identity document belongs to the person presenting the document. | **ITSA, section 17: Identifying a natural person applying for an identification means**  The initial identification of a natural person shall be made personally or electronically in a way that fulfils the requirements for assurance level substantial or high laid down in section 2.1.2 of the Annex of the Act on Level of Assurance in Electronic Identification. The proofing of a person’s identity may be based on a document issued by an authority showing the person’s identity or a strong electronic identification means referred to in this Act.  **LOA Annex, section 2.1.2**  1. The person has been verified to be in possession of evidence recognised by the Member State in which the application for the electronic identity means is being made and representing the claimed identity  and  the evidence is checked to determine that it is genuine; or, according to an authoritative source, it is known to exist and relates to a real person  and  steps have been taken to minimise the risk that the person’s identity is not the claimed identity, taking into account for instance the risk of lost, stolen, suspended, revoked or expired evidence;  or  2. An identity document is presented during a registration process in the Member State where the document was issued and the document appears to relate to the person presenting it  and  steps have been taken to minimise the risk that the person’s identity is not the claimed identity, taking into account for instance the risk of lost, stolen, suspended, revoked or expired evidence; |  | In case a remote identification solution is used, see the criteria in section Method 5. |
|  | 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. | **ITSA, section 17: Identifying a natural person applying for an identification means**  The initial identification of a natural person shall be made personally or electronically in a way that fulfils the requirements for assurance level substantial or high laid down in section 2.1.2 of the Annex of the Act on Level of Assurance in Electronic Identification. The proofing of a person’s identity may be based on a document issued by an authority showing the person’s identity or a strong electronic identification means referred to in this Act.  **LOA Annex, section 2.1.2**  1. The person has been verified to be in possession of evidence recognised by the Member State in which the application for the electronic identity means is being made and representing the claimed identity  and  the evidence is checked to determine that it is genuine; or, according to an authoritative source, it is known to exist and relates to a real person  and  steps have been taken to minimise the risk that the person’s identity is not the claimed identity, taking into account for instance the risk of lost, stolen, suspended, revoked or expired evidence;  or  2. An identity document is presented during a registration process in the Member State where the document was issued and the document appears to relate to the person presenting it  and  steps have been taken to minimise the risk that the person’s identity is not the claimed identity, taking into account for instance the risk of lost, stolen, suspended, revoked or expired evidence; |  | See section 3.9 of this document. |
|  | 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 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. | **LOA Annex, section 2.1.2 high**  1.a) Where the person has been verified to be in possession of photo or biometric identification evidence recognised by the Member State in which the application for the electronic identity means is being made and that evidence represents the claimed identity, the evidence is checked to determine that it is valid according to an authoritative source;  and  the applicant is identified as the claimed identity through comparison of one or more physical characteristics of the person with an authoritative source; |  | See section 3.9 of this document. |
|  | 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;  **ITSA, section 7 b: Information on the validity of a passport or a personal identity card**  An identification service provider has the right to obtain via an interface or other electronic means and without prejudice to secrecy provisions information from the information system of the police about the validity of a passport or a personal identity card used for initial identification. |  | Not a requirement but has an impact on risk assessment and may have an impact on liabilities.  On the high level of assurance this requirement is mandatory. |
|  | S, H | The existence of the person is verified from the population information system. | **ITSA, section 7: Use of data stored in the Population Information System**  The provider of an identification means and a certification service provider offering a trust service must use the Population Information System to obtain and update the data they need in order to be able to offer a service for identifying a natural person. The identification service provider shall also ensure that the data it needs for the purpose of offering identification services are up-to-date with the data in the Population Information System. |  | Applies to all initial identification procedures. |
| **Method 2: Initial identification using an electronic identification means** | | | | | |
|  | S | Identity proofing is based on strong electronic identification means approved in the Identification Act. | **ITSA, section 17: Identifying a natural person applying for an identification means**  The initial identification of a natural person shall be made personally or electronically in a way that fulfils the requirements for assurance level substantial or high laid down in section 2.1.2 of the Annex of the Act on Level of Assurance in Electronic Identification. The proofing of a person’s identity may be based on a document issued by an authority showing the person’s identity or a strong electronic identification means referred to in this Act.  **LOA Annex, section 2.1.2**  4. Where electronic identification means are issued on the basis of a valid notified electronic identification means having the assurance level substantial or high, and taking into account the risks of a change in the person identification data, it is not required to repeat the identity proofing and verification processes. Where the electronic identification means serving as the basis has not been notified, the assurance level substantial or high must be confirmed by a conformity assessment body referred to in Article 2(13) of Regulation (EC) No 765/2008 or by an equivalent body. |  | If initial identification based on strong electronic identification is used.  Identification means used for the substantial level of assurance are registered in Traficom's register as required by the Identification Act. |
|  | 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 high, it is not required to repeat the identity proofing and verification processes. Where the electronic identification means serving as the basis has not been notified, the assurance level high must be confirmed by a conformity assessment body referred to in Article 2(13) of Regulation (EC) No 765/2008 or by an equivalent body.  and  steps are taken that the results of this previous issuance procedure of a notified electronic identification means remain valid. |  | If initial identification based on strong electronic identification is used.  Identification means used for the high level of assurance are registered in Traficom's register as required by the Identification Act. |
| **Method 3: Initial identification based on identification made for other purpose (“prior customer relationship”)** | | | | | |
|  | S, H | Identify proofing relies on a procedure where an identity has been proven and verified earlier for purposes other than issuing an electronic identification means.  The procedure is based on regulations other than the Identification Act or eIDAS regulation and is supervised by an authority.  The procedure offers assurance similar to the procedure based on the presentation of an identity document or identification using electronic means of identification. | **ITSA, section 17: Identifying a natural person applying for an identification means**  The initial identification of a natural person shall be made personally or electronically in a way that fulfils the requirements for assurance level substantial or high laid down in section 2.1.2 of the Annex of the Act on Level of Assurance in Electronic Identification. The proofing of a person’s identity may be based on a document issued by an authority showing the person’s identity or a strong electronic identification means referred to in this Act. In addition, the proofing of an identity may be based on a procedure used at an earlier date by a public or private entity for a purpose other than the issuing of a strong electronic identification means, which the Finnish Transport and Communications Agency approves pursuant to regulations and regulatory control on the procedure, or pursuant to a confirmation by a conformity assessment body referred to in section 28, subsection 1.  **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 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; |  | The use of such an initial identification procedure is subject to express approval from the Finnish Transport and Communications Agency. Notification of such a procedure must be accompanied by a conformity assessment. |
| **Method 4: Initial identification by the police** | | | | | |
|  | S, H | If required, an initial identification should be performed by police. | **ITSA, 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. |  |  |
| **Method 5: Remote initial identification** | | | | | |
|  | S | The remote initial identification solution must be based on a risk assessment (Level of Identity Proofing, LoIP). | **Reference (LOA Guidance, M72B)**  e.g. ITSA, section 8: Requirements posed on the electronic identification scheme.  **M72B, section 6.1: Identification means characteristics and its resistance**  6.1.1  The authentication factors, authentication mechanism and security measures of the identification means must be planned, executed and maintained so that they protect the integrity and confidentiality of the identification means. The identification means must be able to resist at least moderate or high-level threats and attack potential specified in section 2.3 of the appendix to the regulation on *Level of Assurance in Electronic Identification* in accordance with the assurance level of the identification service.  The resistance must be based on a risk assessment including specific assessments of threats directed at an authentication mechanism and authentication factors based on possession, knowledge and inherence as well as assessment of security measures in place to protect against these threats.  **LOA Annex, section 2.4.3: Information security management**  Low:  There is an effective information security management system for the management and control of information security risks.  Substantial:  The information security management system adheres to proven standards or principles for the management and control of information security risks. | ETSI TS 119 461  ISO/IEC TS 29003:2018 | Attack potential (substantial/high) and its calculation, defined criteria that must be met to complete the issuing process, supply chain security if a service provider is used, is it based on the examination of a photo (selfie) or video material, criteria for moving from an automatic process to a manual process. |
|  | S | Informing the customer of terms and conditions | **ITSA, section 20: Issuing an identification means**  The issuance of an identification means is based on the agreement between the applicant for the identification means and the identification service provider. The agreement must be in writing. The agreement can be in electronic format, provided that its content cannot be changed unilaterally and that it remains available to the parties. The identification service provider shall treat its customers in a non-discriminatory way and the identification means applicants fairly when entering into the agreement.  […]  **ITSA, section 23: Obligations of the identification means holder**  The identification means holder shall use the means according to the terms and conditions of the agreement. The holder shall store the identification means with care. The holder’s duty of care for the identification means starts with its acceptance.  The identification means holder shall not make the use of the means available to any other person.  **LOA 2.1.1. Application and registration**  1. Ensure the applicant is aware of the terms and conditions related to the use of the electronic identification means.  2. Ensure the applicant is aware of recommended security precautions related to the electronic identification means.  […] |  |  |
|  | S | Approved initial identification documents and checking their validity. | **ITSA, section 17: Identifying a natural person applying for an identification means**  […]  In initial identification that is solely based on a document issued by an authority showing the person’s identity, the only acceptable documents are a valid passport or a personal identity card issued by an authority of a member state of the European Economic Area, Switzerland or San Marino. If the identification means provider so desires, they may also verify the identity from a valid passport granted by an authority of another state.  […]  **ITSA, section 7 b: Information on the validity of a passport or a personal identity card**  An identification service provider has the right to obtain via an interface or other electronic means and without prejudice to secrecy provisions information from the information system of the police about the validity of a passport or a personal identity card used for initial identification.  **LOA section 2.1.2: Identity proofing and verification (natural person)**  Low:  1. The person can reasonably be assumed to be in possession of evidence recognised by the Member State in which the application for the electronic identity means is being made and representing the claimed identity.  2. The evidence can be assumed to be genuine, or to exist according to an authoritative source, and the evidence appears to be valid.  3. It is known by an authoritative source that the claimed identity exists and it may be assumed that the person claiming the identity is one and the same.  Substantial:  Level Low, plus one of the alternatives listed under level Substantial, e.g.  1. The person has been verified to be in possession of evidence recognised by the Member State in which the application for the electronic identity means is being made and representing the claimed identity  and  the evidence is checked to determine that it is genuine; or, according to an authoritative source, it is known to exist and relates to a real person  and  steps have been taken to minimise the risk that the person’s identity is not the claimed identity, taking into account for instance the risk of lost, stolen, suspended, revoked or expired evidence; |  | In practice, this currently applies to passports, possibly also to identity cards. The validity of the initial identification document must be checked against the interface of the Police or other internationally trusted interface (Interpol). |
|  | S | The existence of the person is verified from the population information system. | **ITSA, section 7: Use of data stored in the Population Information System**  The provider of an identification means and a certification service provider offering a trust service must use the Population Information System to obtain and update the data they need in order to be able to offer a service for identifying a natural person. The identification service provider shall also ensure that the data it needs for the purpose of offering identification services are up-to-date with the data in the Population Information System.  **LOA section 2.1.2: Identity proofing and verification (natural person)**  Low:  3. It is known by an authoritative source that the claimed identity exists and it may be assumed that the person claiming the identity is one and the same. |  | Applies to all initial identification procedures. |
|  | S | The application and external solutions or components carrying out remote initial identification must be assessed. | **ITSA, section 29: Conformity assessment of an electronic identification service**  An identification service provider must regularly subject their service to an assessment by an assessment body referred to in section 28 to determine whether the identification service meets the requirements on interoperability, information security, data protection and other reliability laid down in this Act.  […]  **M72B, section 4.2: Information security management scope**  Information security management shall cover the following aspects concerning the provision of identification service:  1) overall context of the identification service provider;  2) governance, organisation and maintenance of information security management;  3) management of information security risks related to the provision of the identification service;  4) resources allocated to information security, competences, staff awareness of information security, communication, documentation and the management of documented information;  5) planning and steering of the provision of the identification service for the purpose of meeting information security requirements; and  6) evaluation of the efficiency and functionality of information security management.  **M72B, section 15: Conformity assessment criteria**  15.1 Identification scheme and identification means features to be assessed  The identification service assessment required in section 29 of the Identification and Trust Services Act must cover all of the requirements specified in the Act and in this regulation, which pertain to:  1) certain properties of the functions affecting the provision of the identification service (the identification scheme), namely:  a) information security management;  b) record keeping and data processing;  c) facilities and staff;  d) technical measures (controls); and  […]  2) the identification means, meaning certain properties of the identification means, namely:  a) application and registration;  b) identity proofing and verification of the applicant;  […]  d) issuance, delivery and activation;  e) suspension, revocation and reactivation;  f) renewal and replacement; and  g) authentication mechanisms.  **LOA section 2.1.2: Identity proofing and verification (natural person)**  Substantial:  1. The person has been verified to be in possession of evidence recognised by the Member State in which the application for the electronic identity means is being made and representing the claimed identity  and  the evidence is checked to determine that it is genuine; or, according to an authoritative source, it is known to exist and relates to a real person  and  steps have been taken to minimise the risk that the person’s identity is not the claimed identity, taking into account for instance the risk of lost, stolen, suspended, revoked or expired evidence; | ETSI TS 119 461  ISO/IEC TS 29003:2018  ISO/IEC 30107 | Assessment by an assessment body, FAR value, on which data the FAR is based, correspondence to attack potential (substantial/high). PAD ability (Presentation Attack Detection). FRR not essential. The application must also be assessed or its security otherwise verified with a procedure in accordance with Annex C or similar |
|  | S | The authenticity of the presented document and the unaltered nature of the data is verified. Active and passive authentication of the document used for initial identification, document examination across video link (MRZ, visual security features) | **LOA Annex, section 2.1.2: Identity proofing and verification (natural person)**  Low:  2. The evidence can be assumed to be genuine, or to exist according to an authoritative source, and the evidence appears to be valid.  Substantial:  1.  […]  the evidence is checked to determine that it is genuine; or, according to an authoritative source, it is known to exist and relates to a real person  […] |  | The authenticity of the initial identification document (passport, identity card) and of the data stored on the chip must be verified. |
|  | S | The remote identification event and person verification via video link is carried out in conditions for which minimum requirements are defined. | **LOA Annex, section 2.1.2**  Substantial:  1. The person has been verified to be in possession of evidence recognised by the Member State in which the application for the electronic identity means is being made and representing the claimed identity  and  the evidence is checked to determine that it is genuine; or, according to an authoritative source, it is known to exist and relates to a real person  and  steps have been taken to minimise the risk that the person’s identity is not the claimed identity, taking into account for instance the risk of lost, stolen, suspended, revoked or expired evidence; |  | The remote initial identification event is carried out in a situation or conditions where the realisation of automatic security controls can be maximised. |
|  | S | The automatic security controls analysing the biometrics in remote initial identification are random. | **LOA Annex, section 2.1.2**  Low:  3. It is known by an authoritative source that the claimed identity exists and it may be assumed that the person claiming the identity is one and the same.  Substantial:  1. The person has been verified to be in possession of evidence recognised by the Member State in which the application for the electronic identity means is being made and representing the claimed identity  and  the evidence is checked to determine that it is genuine; or, according to an authoritative source, it is known to exist and relates to a real person  and  steps have been taken to minimise the risk that the person’s identity is not the claimed identity, taking into account for instance the risk of lost, stolen, suspended, revoked or expired evidence; |  | The aim is to prevent e.g. the creation of prepared video feeds. |
|  | S | Technical minimum requirements are defined for a remote initial identification event; unless they are met, the remote initial identification cannot be carried out | **LOA Annex, section 2.1.2**  Low:  3. It is known by an authoritative source that the claimed identity exists and it may be assumed that the person claiming the identity is one and the same.  Substantial:  […]  and  the evidence is checked to determine that it is genuine; or, according to an authoritative source, it is known to exist and relates to a real person  and  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; |  | E.g. minimum requirements for hardware levels, smoothness and speed of data communication connections, resolution, camera abilities, appearance of artefacts, Annex C resilience criteria. |
|  | S | Data transfer, storage | **LOA Annex, section 2.4.4: Record keeping**  1. Record and maintain relevant information using an effective record-management system, taking into account the applicable legislation and good practice in relation to data protection and data retention.  2. Retain, as far as it is permitted by national law or other national administrative arrangement, and protect records for as long as they are required for the purpose of auditing and investigation of security breaches, and retention, after which the records shall be securely destroyed.  **also M72B, section 7: Identification scheme interface encryption requirements** |  | Data protection, especially if data is transferred outside the EU. Saving for later examination e.g. in case of detected misuse. |
|  | S | The software component carrying out remote initial identification must be authenticated. | **ITSA, section 13: General obligations of an identification service provider**  […]  The identification service provider is responsible for the reliability and functionality of services and products provided by persons contributing to the identification service process.  **LOA Annex, section 2.4.6: Technical controls**  1. The existence of proportionate technical controls to manage the risks posed to the security of the services, protecting the confidentiality, integrity and availability of the information processed.  2. Electronic communication channels used to exchange personal or sensitive information are protected against eavesdropping, manipulation and replay.  […]  **15 Conformity assessment criteria**  **15.1 Identification scheme and identification means features to be assessed**  The identification service assessment required in section 29 of the Identification and Trust Services Act must cover all of the requirements specified in the Act and in this regulation, which pertain to:  1) certain properties of the functions affecting the provision of the identification service (the identification scheme), namely:  a) information security management; |  | In practice, a mobile application and the application attestation to the back-end system. |
|  | S | Remote identification must be based at least in part on automated processes. | **LOA Annex, section 2.4.6: Technical controls**  4. Procedures exist to ensure that security is maintained over time and that there is an ability to respond to changes in risk levels, incidents and security breaches. |  | Using only an official for remote initial identification is not sufficient, but the process must be based at least in part on computerised comparison of the above-mentioned criteria. |
|  | S | Staff participating in the remote identification process must be trained. | **LOA Annex, section 2.4.5: Facilities and staff**  1. The existence of procedures that ensure that staff and subcontractors are sufficiently trained, qualified and experienced in the skills needed to execute the roles they fulfil.  2. The existence of sufficient staff and subcontractors to adequately operate and resource the service according to its policies and procedures. |  | If an employee takes part in the decision-making of a remote initial identification process, they must be adequately trained in assessing the authenticity of any video material and initial identification document authenticity factors. |

# Lifecycle of identification means

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **M72B, section 15: Conformity 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; and  g) […] | | | | | |
| **NO.** | **LEVEL OF ASSURANCE** | **REQUIREMENT PERTAINING TO THE IDENTIFICATION SERVICE (SUMMARY)** | **PROVISIONS** | **STANDARD** | **NOTES** |
|  | S, H | The identification is not connected to the person (personalised) before initial identification. The identification means factors are connected to the identification means holder. | **M72B, section 6.3: Connecting identification means to a person**  6.3.1  The authentication factors of the identification means must be bound to the identification means holder in the identification scheme.  6.3.2  An identification means shall not be bound to an applicant before the applicant has passed initial identification or it has been otherwise ensured in the process of granting an identification means that the identification means is not functional before the initial identification referred to in section 17 of the Identification and Trust Services Act has been performed. |  |  |
|  | S, H | The personal data of a natural person is checked from the population information system when issuing an identification means and regularly during the validity of the identification means. | **ITSA, section 7: Use of data stored in the Population Information System**  The provider of an identification means and a certification service provider offering a trust service must use the Population Information System to obtain and update the data they need in order to be able to offer a service for identifying a natural person. The identification service provider shall also ensure that the data it needs for the purpose of offering identification services are up-to-date with the data in the Population Information System.  […]  **See M72B, section 12: Minimum set of data to be relayed in a trust network**  **LOA Annex, section 2.1.2: Identity proofing and verification (natural person)**  Substantial:  1. The person has been verified to be in possession of evidence recognised by the Member State in which the application for the electronic identity means is being made and representing the claimed identity  and  the evidence is checked to determine that it is genuine; or, according to an authoritative source, it is known to exist and relates to a real person  and  steps have been taken to minimise the risk that the person’s identity is not the claimed identity, taking into account for instance the risk of lost, stolen, suspended, revoked or expired evidence; |  | The frequency of regular verification has not been defined.  Weekly verification is a good established practice.  Cf. (no reference in the Identification Act; applied formally only if the procedure is notified)  **LOA 2.1.1: Application and registration**  3. Appropriate identification data required for identity proofing is collected. |
|  | S, H | **Issuance, delivery and activation of an identification means**  An issuance procedure is used to ensure that the identification means does not unlawfully end up in the possession of a third party when the identification means is being released. | **ITSA, section 20: Issuing an identification means**  The issuance of an identification means is based on the agreement between the applicant for the identification means and the identification service provider. The agreement must be in writing. The agreement can be in electronic format, provided that its content cannot be changed unilaterally and that it remains available to the parties.  […]  cf. (there is no reference to LOA 2.1.1 in the Identification Act; it is therefore applied formally only in case the procedure is notified)  **LOA 2.1.1: Application and registration**  1. Ensure the applicant is aware of the terms and conditions related to the use of the electronic identification means.  2. Ensure the applicant is aware of recommended security precautions related to the electronic identification means.  **ITSA, section 21: Delivering the identification means to the applicant**  The identification service provider shall deliver the identification means to the applicant as stated in the agreement. The identification service provider must ensure that when the identification means is handed over, it does not become subject to unauthorised possession. The method for ensuring this must meet, at a minimum, the requirements laid down for assurance level substantial in section 2.2.2 of the Annex of the Act on Level of Assurance in Electronic Identification.  **LOA Annex, section 2.2.2: Issuance, delivery and activation**  After issuance, the electronic identification means is delivered via a mechanism by which it can be assumed that it is delivered only into the possession of the person to whom it belongs. |  | Contract terms (such as those mentioned in section 15 of the Identification Act) are to be arranged by the service providers and are not within the scope of the audit.  The verification requirement specified in section 8 of the ITSA and section 2.2.1 of the LOA that only the holder of a means of identification may use that means is also related to the separate requirement on release in section 21, according to which the identification service provider must ensure that the identification means does not become subject to unauthorised possession when it is handed over.  See LOA Guidance:  Possible mechanisms include:  • delivery in person  • delivery by registered mail  • using some activation process, where it can be reasonably assumed that only the subject has the necessary information to activate the means (e.g. a transport-PIN delivered separately from the identification means).  For Substantial, multiple authentication factors shall be used. Activation codes are not necessarily required. Several issuance, delivery and activation combinations are possible that meet Substantial:  • The delivery of the electronic identification means can be done via regular mail, its activation by sending a code to the bank account of the subject. The applicant enters the code to activate the electronic identification means. The assumption here is that bank authentication is of at least level Substantial.  • Separate delivery of the electronic identification means and the activation code via regular mail to the verified address of the subject.  • Delivery of the electronic identification means via regular mail to the address of the applicant.  • The electronic identification means is handed over after having verified the identity of the applicant. |
|  | H | **Issuance, delivery and activation of an identification means**  An issuance procedure is used to ensure that the identification means does not unlawfully end up in the possession of a third party when the identification means is being released. | **LOA Annex, section 2.2.2: Issuance, delivery and activation**  **high**  The activation process verifies that the electronic identification means was delivered only into the possession of the person to whom it belongs. |  | The activation process primarily requires the use of an activation code. In particular, it must be ensured that the activation code cannot become available to third parties in the delivery process, and that the activation code is single-use and cannot be used e.g. for reactivation or creating a new PIN code. |
|  | S, H | **Suspension, revocation and reactivation of the identification means**  The identification means provider has a revocation service with 24/7 availability available to the users, a revocation list available to the relying parties and the capacity to technically prevent the use of any identification means reported as lost or stolen by the user. | **ITSA, section 25: Cancellation and prevention of use of identification means**  The identification means holder shall notify the identification service provider or a designated party if the identification means has been lost, is in the unauthorised possession of another person or of any unauthorised use immediately upon detection of this fact.  The identification means provider shall provide an opportunity to submit a notification as set out in subsection 1 at any time. Upon receipt of the notification, the identification service provider shall immediately cancel the identification means or prevent its use.  The identification means provider shall properly and without delay enter in its system the information about the time of cancellation or prevention of use. The holder of the identification means has the right to request proof of submitting a notification mentioned in subsection 1. Such request must be made within 18 months from the notification.  The system shall be designed to allow a service provider using an identification service to easily verify the information entered at any time. However, such obligation to create an opportunity to verify information does not exist if the use of the identification means can be prevented or blocked by technical means.  […]  **Section 26: Identification service provider’s right to suspend or revoke the use of an identification means**  In addition to the provisions of section 25, the identification service provider may suspend or revoke the use of an identification means if:  1) the identification service provider has reason to believe that someone other than the person to whom the means was issued is using it;  2) the identification means is obviously defective;  3) the identification service provider has reason to believe that the safe use of the means is at risk;  4) the identification means holder is using the identification means contrary to the agreed terms of use; or  5) the identification means holder has died.  The identification service provider shall notify the holder as soon as possible about the revocation or suspension of use of the identification means, as well as the time of and reasons for such action.  The identification service provider shall renew, reactivate or replace the ability to use the identification means or give the identification means holder a new means immediately after removal of reasons referred to in subsection 1(2 and 3).  **LOA Annex, section 2.2.3: Suspension, revocation and reactivation**  1. It is possible to suspend and/or revoke an electronic identification means in a timely and efficient manner.  2. The existence of measures taken to prevent unauthorised suspension, revocation and/or reactivation.  3. Reactivation shall take place only if the same assurance requirements as established before the suspension or revocation continue to be met. |  | cf. (there is no reference to LOA 2.2.3 in the Identification Act; it is therefore applied only in case the procedure is notified)  **LOA Annex, section 2.2.3: Suspension, revocation and reactivation**  1. It is possible to suspend and/or revoke an electronic identification 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. |
|  | S, H | **Renewal and replacement of an identification means** | **ITSA, section 22: Renewal of the identification means**  The identification service provider may provide a new identification means without explicit request to the holder only if a previously delivered identification means needs to be replaced. The renewal of the identification means must follow, at a minimum, the requirements laid down for assurance level substantial in section 2.2.4.  **LOA Annex, section 2.2.4: Renewal and replacement**  Taking into account the risks of a change in the person identification data, renewal or replacement needs to meet the same assurance requirements as initial identity proofing and verification or be based on a valid electronic identification means of the same, or higher, assurance level.  **LOA Annex, section 2.2.1: Electronic identification means characteristics and design**  Substantial:  2. The electronic identification means is designed so that it can be assumed to be used only if under the control or possession of the person to whom it belongs.  **LOA Annex, section 2.2.2: Issuance, delivery and activation**  Substantial:  After issuance, the electronic identification means is delivered via a mechanism by which it can be assumed that it is delivered only into the possession of the person to whom it belongs. |  | The verification requirement set out in section 8 of the ITSA and sections 2.2.1 and 2.2.2 of the LOA (the identification means is used only under the control or possession of the person to whom it belongs) must be fulfilled in all situations where some or all authentication factor or activation codes are issued in connection with renewal, replacement or reactivation.  See 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> |
|  | 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.  **LOA Annex, section 2.2.1: Electronic identification means characteristics and design**  High:  2. The electronic identification means is designed so that it can be reliably protected by the person to whom it belongs against use by others.  **LOA Annex, section 2.2.2: Issuance, delivery and activation**  High:  The activation process verifies that the electronic identification means was delivered only into the possession of the person to whom it belongs. |  | The verification requirement set out in section 8 of the ITSA and sections 2.2.1 and 2.2.2 of the LOA (the identification means is used only under the control or possession of the person to whom it belongs) must be fulfilled in all situations where some or all authentication factor or activation codes are issued in connection with renewal, replacement or reactivation. |