Estonian eID schemes fulfilment of interoperability requirements according to (EU) 2015/1501

Version 1.0

Version History			
Date	**Version**	**Version info**	**Author**
19.11.2025	1.0	Final version	Information System Authority (RIA), Republic of Estonia

1. Introduction

This document describes how Estonian eID schemes (ID card, RP card and diplomatic identity card) meet the interoperability and minimum technical and operational security requirements of Commission Implementing Regulation (EU) 2015/1501. The above-mentioned eID schemes were initially notified in 2018.

2. Interoperability Requirements

Article	Requirement	Description
Art. 4	**Mapping of national assurance levels** The mapping of national assurance levels of the notified electronic identification schemes shall follow the requirements laid down in Implementing Regulation (EU) 2015/1502. The results of the mapping shall be notified to the Commission using the notification template laid down in Commission Implementing Decision (EU) 2015/1505.	The Estonian eID schemes meet all requirements of the eIDAS level of assurance 'high' laid down in the Commission Implementing Regulation (EU) 2015/1502. The detailed mapping is given in [1].
Art. 5	**Nodes** 1. A node in one Member State shall be able to connect with nodes of other Member States. 2. The nodes shall be able to distinguish between public sector bodies and other relying parties through technical means. 3. A Member State implementation of the technical requirements set out in this Regulation shall not impose disproportionate technical requirements and costs on other Member States for them to interoperate with the implementation adopted by the first Member State.	The Estonian eIDAS Node operated by RIA is operational and integrated into the eIDAS Interoperability Framework [2] in accordance with the eIDAS Technical Specifications [3] of the eIDAS Technical Subgroup on eID of the EUDI Cooperation Group. Connectivity tests are performed regularly. The Estonian eIDAS Node relies on a sample software of eIDAS Node developed by the European Commission that implements the eID Profile [3]. The current Estonian eID schemes have been made available through Estonian government e-identification gateway (TARA) that integrates Estonian eIDAS-Proxy-Service to eIDAS-Connectors of other Member States. A temporary restriction has been applied in TARA and in Estonian eIDAS-Proxy-Service for ID cards under the Estonian eID scheme issued from 17 November 2025 that cannot be used in eIDAS Network. After completion of the revision process of the updates to current Estonian eID scheme the cards issued from 17 November 2025 will be made available in Estonian eIDAS-Proxy-Service.

		The Estonian eIDAS Node and TARA distinguish public-sector bodies from other relying parties via the eIDAS SAML message format element “SPType” with values “public” or “private”.
Art. 6	**Data privacy and confidentiality** 1. Protection of privacy and confidentiality of the data exchanged and the maintenance of data integrity between the nodes shall be ensured by using best available technical solutions and protection practices. 2. The nodes shall not store any personal data, except for the purpose set out in Article 9(3).	The Estonian eIDAS Node is integrated into the eIDAS Interoperability Framework [2] in accordance with the eIDAS Technical Specifications [3] of the eIDAS Technical Subgroup on eID of the EUDI Cooperation Group. Protection of data privacy, confidentiality and integrity for the communication between Estonian eIDAS Node and eIDAS Network is ensured via cryptographically protected SAML messages and TLS (SHA-256 with RSA 2048 bits) to protect the transport layer. eIDAS Proxy Service allows authentication requests from another EU Member State with Estonian notified eID scheme, providing eIDAS minimum data set (MDS). The Estonian eIDAS Node does not store personal data beyond what is strictly necessary under Article 9(3) of Implementing Regulation (EU) 2015/1501. Data storing is limited to technical logging needed in the event of an incident.
Art. 7	**Data integrity and authenticity for the communication** Communication between the nodes shall ensure data integrity and authenticity to make certain that all requests and responses are authentic and have not been tampered with. For this purpose, nodes shall use solutions which have been successfully employed in cross-border operational use.	The Estonian eIDAS Node is integrated into the eIDAS Interoperability Framework [2] in accordance with the eIDAS Technical Specifications [3] of the eIDAS Technical Subgroup on eID of the EUDI Cooperation Group. The eIDAS-Node application in the Estonian eIDAS Proxy Service implementation is part of the European Commission’s eIDAS-Node sample software [4] that is responsible for a secure communication between member states eIDAS Nodes using the eIDAS SAML protocol. Both applications use a database as a background channel and a special XML intermediate protocol developed by European Commission (so-called LightRequest and LightResponse) to communicate with each other.

		Data integrity and authenticity for the communication between Estonian eIDAS Node and eIDAS Network is ensured via cryptographically protected SAML messages and TLS (SHA-256 with RSA 2048 bits) to protect the transport layer.
Art. 8	**Message format for the communication** The nodes shall use for syntax common message formats based on standards that have already been deployed more than once between Member States and proven to work in an operational environment. The syntax shall allow: (a) proper processing of the minimum set of person identification data uniquely representing a natural or legal person; (b) proper processing of the assurance level of the electronic identification means; (c) distinction between public sector bodies and other relying parties; (d) flexibility to meet the needs of additional attributes relating to identification.	The Estonian eIDAS Node is integrated into the eIDAS Interoperability Framework [2] in accordance with the eIDAS Technical Specifications [3] of the eIDAS Technical Subgroup on eID of the EUDI Cooperation Group following the common message formats set out in the specifications that has proven to work in an operational environment. The Estonian eIDAS Proxy Service uses the government e-identification gateway (TARA) interface, acting as an eIDAS Identity Provider (IdP). The SpecificProxyService is responsible for a communication with the government e-identification gateway (TARA), which uses OIDC protocol as an authentication protocol. The Estonian eIDAS Node and TARA distinguish public-sector bodies from other relying parties via the eIDAS SAML message format element “SPType” with values “public” or “private”.

Art. 9	**Management of security information and metadata** 1. The node operator shall communicate the metadata of the node management in a standardised machine processable manner and in a secure and trustworthy way. 2. At least the parameters relevant to security shall be retrieved automatically. 3. The node operator shall store data which, in the event of an incident, enable reconstruction of the sequence of the message exchange for establishing the place and the nature of the incident. The data shall be stored for a period of time in accordance with national requirements and, as a minimum, shall consist of the following elements: (a) node's identification; (b) message identification; (c) message date and time.	The Estonian eIDAS Node is integrated into the eIDAS Interoperability Framework [2] in accordance with the eIDAS Technical Specifications [3] of the eIDAS Technical Subgroup on eID of the EUDI Cooperation Group following the common message formats set out in the specifications that has proven to work in an operational environment. The Estonian eIDAS Node metadata is communicated in a standardised machine processable manner in a secure and trustworthy in line with the requirements of metadata format set out in technical specifications. The Estonian eIDAS Node stores data what is necessary under Article 9 of Implementing Regulation (EU) 2015/1501 [2] needed in the event of an incident enabling reconstruction of the sequence of the message exchange for establishing the place and nature of the incident.
Art. 10	**Information assurance and security standards** 1. Node operators of nodes providing authentication shall prove that, in respect of the nodes participating in the interoperability framework, the node fulfils the requirements of standard ISO/IEC 27001 by certification, or by equivalent methods of assessment, or by complying with national legislation. 2. Node operators shall deploy security critical updates without undue delay.	The Estonian eIDAS Node and TARA are operated within Estonian Information Security Standard (E-ITS) aligned to ISO/IEC 27001 and Estonian public-sector security baseline requirements. The standard is based on the German BSI IT-Grundschutz (BSIG) baseline protection system and on the EVS-ISO/IEC 27001:2014 standard. Information assurance is demonstrated through periodic audits and compliance with national regulations. Security testing for eIDAS Node and TARA is performed regularly and upon major updates. Security-critical updates are deployed without undue delay.

Art. 11	**Person identification data** 1. A minimum set of person identification data uniquely representing a natural or a legal person shall meet the requirements set out in the Annex when used in a cross-border context. 2. A minimum data set for a natural person representing a legal person shall contain the combination of the attributes listed in the Annex for natural persons and legal persons when used in a cross-border context. 3. Data shall be transmitted based on original characters and, where appropriate, also transliterated into Latin characters.	The Estonian eIDAS Proxy Service uses the government e-identification gateway (TARA) interface, acting as an eIDAS Identity Provider (IdP). The SpecificProxyService is responsible for a communication with the government e-identification gateway (TARA), which uses OIDC protocol as an authentication protocol. On a successful authentication, the MDS is sent back to the requesting party. The electronic identification means under the Estonian eID scheme enable identification of natural persons only. Legal person attributes are used in the context of representation, where natural person to acts on behalf of a legal person. The MDS for a natural person contains current family name(s), current first name(s), date of birth and unique persistent identifier (Estonian personal identification code). The minimum data set for a legal person contains current legal name, Business Registry code (identifier for a legal person in Estonia). MDS attributes for a natural person are based on data on the eID certificate, for legal person the MDS attributes are requested from Estonian e-Business Registry using X-Road data exchange layer. The MDS provided by Estonian eID schemes meet the requirements set out in the Annex set out in the Commission Implementing Regulation (EU) 2015/1502 [2]. The Estonian eIDAS Node transmits data using original characters and, where appropriate, transliterated into Latin characters.

3. References

[1] eID level of assurance mapping for Estonian eID according to Article 8 (3) of Regulation (EU) No. 910/2014.

[2] COMMISSION IMPLEMENTING REGULATION (EU) 2015/1501 - of 8 September 2015 on the interoperability framework pursuant to Article 12(8) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market.

[3] Technical Specifications under the eIDAS eID Profile: eIDAS Interoperability Architecture, eIDAS SAML Message Format, eIDAS SAML Attribute Profile, eIDAS Cryptographic Requirements for the Interoperability Framework.

[4] eIDAS-Node Integration Package.