NOTIFICATION FORM FOR ELECTRONIC IDENTITY SCHEME UNDER ARTICLE 9 (5) OF REGULATION (EU) NO. 910/2014

The Republic of Estonia hereby notifies the European Commission of an electronic identification scheme to be published in the list referred to in article 9 (3) of Regulation (EU) no. 910/2014, and confirms the following:

— the information communicated in this notification is consistent with the information which has been communicated to the Cooperation Network in accordance with article 7 (g) of Regulation (EU) no. 910/2014, and

— the electronic identification scheme can be used to access at least one service provided by a public-sector body in the Republic of Estonia.

Date 27/02/2018

[signed electronically]

1. General information

Title of scheme	Level(s) of assurance (low, substantial, or high)
Estonian eID scheme: ID card	**high**
Estonian eID scheme: RP card	**high**
Estonian eID scheme: Digi-ID	**high**
Estonian eID scheme: e-Residency Digi-ID	**high**
Estonian eID scheme: Mobiil-ID	**high**
Estonian eID scheme: diplomatic identity card	**high**

2. Authority/authorities responsible for the scheme

Name(s) of authority/authorities	Postal address(es)	Email address(es)	Telephone no.
Police and Border Guard Board (PBGB) (eID scheme operator)	Pärnu mnt 139, 15060 Tallinn	Homepage: https://www.politsei.ee/en/ Email: info@politsei.ee	Client information: +372 612 3000
Ministry of the Interior (policy-making in identity documents)	Pikk 61, 15065 Tallinn	Homepage: https://www.siseministeerium.ee/en Email: info@siseministeerium.ee	+372 612 5008
Ministry of Economic Affairs and Communications (policy-making in IT and trust services)	Harju 11, 15072 Tallinn	Homepage: https://www.mkm.ee/en Email: info@mkm.ee	+372 625 6342
Information System Authority (EISA) (technical architecture of eID and cybersecurity incident management CERT-EE)	Pärnu mnt 139a, 15169 Tallinn	Homepage: https://www.ria.ee/en/ Email: ria@ria.ee ID support homepage: http://www.id.ee/?lang=en ID support email: abi@id.ee	+ 372 663 0200 ID support number: +372 677 3377

Technical Regulatory Authority (ETRA) (supervision of trust service providers)	Sõle 23a, 10614 Tallinn	Homepage: http://tja.ee/en QTSP: http://sr.riik.ee/en.html Email: info@tja.ee	+372 667 2000
Ministry of Foreign Affairs (identity documents management in embassies, identity management, and issuance of diplomatic identity cards)	Islandi väljak 1, 15049 Tallinn	Homepage: http://www.vm.ee/en Email: vminfo@vm.ee	+372 637 7000

3. Information on relevant parties, entities, and bodies (where there are multiple parties, entities, or bodies, please list them all in accordance with article 3 (2) and (3))

3.1. Entity which manages the registration process of the unique person identification data

The Estonian PBGB manages the registration process of the unique person identification data.

The registration process of a diplomatic identity document, or if the registration process of the unique person identification data takes place in a foreign country, is managed by the Ministry of Foreign Affairs in cooperation with the PBGB.

3.2. Party issuing the electronic identification means

The electronic identity means are issued, according to article 7 (a) (i) of Regulation (EU) no. 910/2014, by the notifying Member State, the Republic of Estonia, in particular the PBGB or the Ministry of Foreign Affairs (in case of the diplomatic identity card).

3.3. Party operating the authentication procedure

The authentication procedure is assured (granted) by the PBGB and the Ministry of Foreign Affairs (in case of the diplomatic identity card) through a subcontracted qualified trust service provider (certification authority).

3.4. Supervisory body

The Estonian PBGB is a government body supervised according to national laws and other legal acts applicable to government bodies.

The Ministry of the Interior is the main supervisory body of the PBGB.

The Ministry of Foreign Affairs is a government body supervised according to national laws and other legal acts applicable to government bodies.

The Estonian Information System Authority (EISA) and the Estonian Technical Regulatory Authority (ETRA) cover specific supervisory roles of eID schemes.

The EISA is the supervisory body of certification service providers in terms of security incident management (responsible for article 19 of Regulation (EU) no. 910/2014).

4. Description of the electronic identification scheme

(a) Briefly describe the scheme including the context within which it operates and its scope

There are six types of Estonian eID. Three of them are both physical identification documents and digital identity documents. The other three are digital identity documents only.

Physical identification documents are the ID card, the RP card, and the diplomatic identity card.

Solely digital identity documents are Digi-ID, e-Residency Digi-ID, and Mobiil-ID.

Technically, all Estonian eIDs are PKI-based solutions, where the private key is on a secure module of the chip. On Mobiil-ID, the eID chip with the secure module is embedded in the SIM card. Smart card-based solutions (ID card, RP card, Digi-ID, e-Residency Digi-ID, diplomatic identity card) have public key certificates in addition to a public certificate repository, also stored on the smart card. The chips are SSCD/QSCD-certified devices. These tokens are smart card-based solutions, which protects the private key from unauthorised access, copying, or tampering. Identity data – the person's first name, last name, and unique identifier (personal identification code) – is stored in the public key certificate. These certificates are freely accessible on the smart card or in the public LDAP catalogue. A prerequisite for Mobiil-ID is having either an ID card or RP card. A SIM card with Mobiil-ID readiness can be obtained from Estonian mobile operators under a contractual agreement. Thereafter, the person needs to activate the Mobiil-ID functionality in the Mobiile-ID application environment with their ID card or RP card or at a service point of the issuing authority.

In the management of the eID scheme, the following parties are involved:

- As the issuing authority, the Estonian PBGB and the Ministry of Foreign Affairs (for the issuance of the diplomatic identity card, the official foreign representations of the Republic of Estonia).
- The Information System Authority (EISA) is a state institution which is responsible mainly for the governance of public sector IT. Furthermore, they host the national CERT-EE and serve a role as the supervisory body for CIIP and trust service providers (more information at https://www.ria.ee/en/). In terms of eID, the EISA is responsible for eID hardware and software requirements. In general, the EISA maintains a set of requirements for eID, participates in procurements, and validates results as a partner organisation to the PBGB. In addition, the EISA develops and maintains middleware software and end-user software for maintaining eID cards (PIN code and official email address management), also software for e-signatures.
- The PBGB has a contractor for manufacturing and personalisation of identity documents, Gemalto AG. Personalisation is done by Gemalto AG subsidiary Trüb Baltic AS, located in Estonia.
- The certification authority (certification service provider) is a qualified trust service provider (according to the eIDAS Regulation): SK ID Solutions AS. They are the contracting party for supplying the Mobiil-ID service (SIM cards and qualified trust services) and a subcontractor for qualified trust services for identity documents of the PBGB. Their responsibility is maintenance of certificate lifecycle: creation, activation, suspension, and revocation.

- Mobile operators (Telia Eesti AS, Elisa Eesti AS, Tele2 Eesti AS) are the subcontractors of SK ID Solutions AS. They deliver SIM cards, which are the carriers of state-issued eID with the functionality of electronic authentication and a qualified digital signature, to Mobiil-ID users.
- Mobiil-ID certificate creation and activation are done on behalf of the PBGB after user identity-proofing by the PBGB.

Issuance of the ID card, the RP card, Digi-ID, e-Residency Digi-ID, the diplomatic identity card, or Mobiil-ID is described in section 2.2.1. of the corresponding LoA mapping documents.

eID technical descriptions are provided in section 2.3.1. of the corresponding LoA mapping documents.

Assurance requirements come from European legislation (i.e., the eIDAS Regulation, GDPR, etc.) and national legislations (i.e., the Electronic Identification and Trust Services for Electronic Transactions Act, the Emergency Act, and other national acts) for both public and private parties involved. Additional requirements from tender documents and contract(s) apply for identity documents manufacturing and personalisation, and for the qualified trust service provider.

The minimum data set is provided to the requesting party. No additional attributes are provided for natural persons under the scheme if requested by a relying party.

Estonian eIDs are used only for identification of natural persons; therefore, no additional attributes are provided for legal persons under the scheme if requested by a relying party.

4.1. Applicable supervisory, liability, and management regime

4.1.1. Applicable supervisory regime

Describe the supervisory regime of the scheme with respect to the following:

(a) Supervisory regime applicable to the party issuing the electronic identification means

The PBGB is a government body supervised according to national laws and other legal acts applicable to government bodies. Supervisory control is done by the Ministry of the Interior, as the PBGB is an agency under the ministry.

The Ministry of Foreign Affairs is responsible for forwarding collected applications to the PBGB for issuing and giving out issued Estonian identity documents in the official foreign representations of the Republic of Estonia. The Ministry of Foreign Affairs is issuing Estonian diplomatic identity cards and is responsible for identity management in case of issuance of diplomatic identity cards.

The Estonian Information System Authority (EISA) is responsible for technical architecture, development of client/end-user software and chip-technical specification, and application for eID, an information security standard that is developed for the Estonian public sector (ISKE[1]), cybersecurity incident management by the CERT-EE and supervision of vital services (incl. the trust service provider).

[1] ISKE – https://www.ria.ee/en/iske-en.html

All public sector bodies have to follow a three-level IT baseline security system: ISKE (a detailed description of ISKE is available on the EISA webpage and in LoA mapping documents section 2.4.).

The Estonian Technical Regulatory Authority (ETRA) is the supervisory body who is responsible for supervisory tasks that are established in article 17 of the eIDAS Regulation. The ETRA is managing trust list of Estonian qualified trust service providers and supervising trust service providers in meeting the requirements.

(b) Supervisory regime applicable to the party operating the authentication procedure

Public and private parties act in accordance with European legislation (e.g., the eIDAS Regulation, GDPR, etc.) and national legislation (e.g., the Electronic Identification and Trust Services for Electronic Transactions Act, the Emergency Act, etc.).

The PBGB is responsible for identity management procedures, and the same supervisory regime as in point (a) is applicable.

The EISA is acting as the supervisory body according to article 19 of the eIDAS Regulation and section 45 of the Estonian Emergency Act. Section 36 of the Emergency Act lists electronic authentication and digital signature (qualified electronic signature) as vital services. Subsection 9^4 (3^1) of the Identity Documents Act states that the provider of certification service that enables digital identification and digital signing with the certificate which is entered in the documents issued on the basis of this act is the provider of vital service specified in clause 36 (1) 8) of the Emergency Act.

The ETRA is acting as the supervisory body according to article 17 of the eIDAS Regulation, as the electronic authentication and qualified trust services (including qualified e-signature) are using the same means (QSCD).

Supervisory control of the EISA and the ETRA is done by the Ministry of Economic Affairs and Communications.

Supervisory control is conducted in administrative authority by a higher authority over the subordinate administrative agency in terms of the lawfulness in actions and feasibility in functions. Supervisory control of Estonian governmental authorities and agencies is regulated by chapter 7 of the Government of the Republic Act.

4.1.2. Applicable liability regime

(a) Liability of the Member State under article 11 (1) of Regulation (EU) no. 910/2014

Estonian eID is subject to European and national laws; therefore, it is a liability of the Estonian government. Supervisory control is conducted in an administrative authority by a higher authority over the subordinate administrative agency in terms of the lawfulness in actions and feasibility in functions. Chapter 7 of the Government of the Republic Act regulates supervisory control of Estonian governmental authorities and agencies; hence, this requirement is fulfilled.

(b) Liability of the party issuing the electronic identification means under article 11 (2) of Regulation (EU) no. 910/2014

The Estonian PBGB has full liability in identity management and in issuing the ID card, the RP card, Digi-ID, e-Residency Digi-ID, and Mobiil-ID.

The Estonian Ministry of Foreign Affairs has full liability in case of the diplomatic identity card identity management and issuance.

(c) Liability of the party operating the authentication procedure under article 11 (3) of Regulation (EU) no. 910/2014

Liability for operating the authentication procedure under Article 11(3) of Regulation (EU) no 910/2014 is held by the certification authority or a certification service provider who is a qualified trust service provider (in accordance with the eIDAS Regulation): SK ID Solutions AS.

4.1.3. Applicable management arrangements

The holder of Estonian eIDs can check all their activities performed via the OCSP at the following link: https://minutoimingud.sk.ee/

The validity of Estonian identity documents (ID card, RP card, Digi-ID, e-Residency Digi-ID) can be checked at the following link: https://www.politsei.ee/en/teenused/inquiries/

Arrangements for suspending or revoking the Estonian eID means are provided in sections 2.2.3., "Suspension, revocation, and reactivation", and 2.4.1., "General provisions", clause 5 of the corresponding LoA mapping documents.

4.2. Description of the scheme components

4.2.1. Enrolment

(a) Application and registration

Application and registration is described in section 2.1.1. of the corresponding LoA mapping documents.

(b) Identity-proofing and verification (natural person)

Identity-proofing and verification (natural person) is described in section 2.1.2. of the corresponding LoA mapping documents.

(c) Identity-proofing and verification (legal person)

Estonian eID is used only for identification of natural persons; therefore, this is not applicable.

(d) Binding between the electronic identification means of natural and legal persons

Estonian eID is used only for identification of natural persons; therefore, this is not applicable.

4.2.2. Electronic identification means management

(a) Electronic identification means characteristics and design (including, where appropriate, information on security certification)

Electronic identification means characteristics and design are described in section 2.2.1. of the corresponding LoA mapping documents.

(b) Issuance, delivery, and activation

Issuance, delivery, and activation is described in section 2.2.2. of the corresponding LoA mapping documents.

(c) Suspension, revocation, and reactivation

Suspension, revocation, and reactivation is described in section 2.2.3. of the corresponding LoA mapping documents.

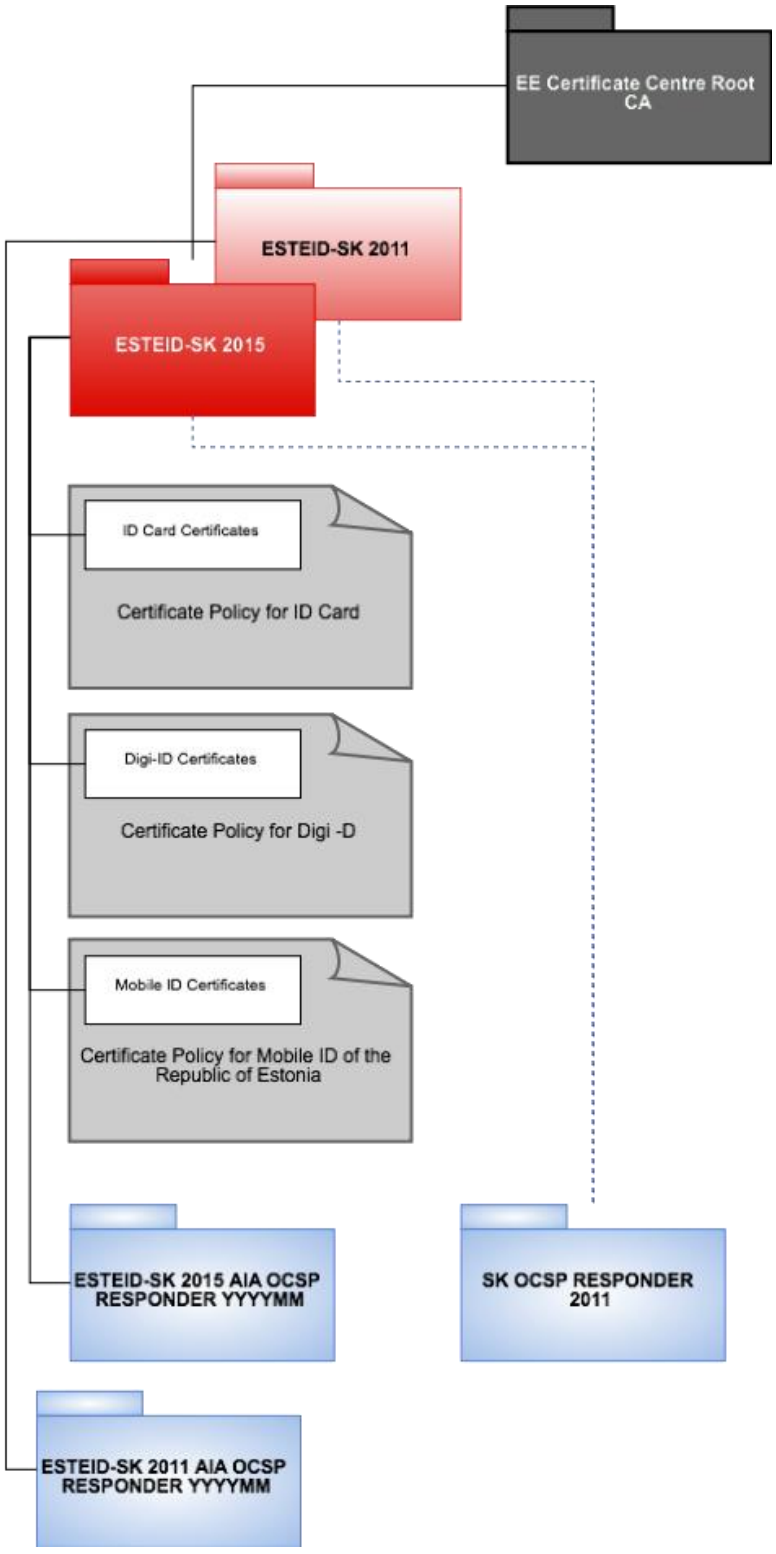
(d) Renewal and replacement

Renewal and replacement is described in section 2.2.4. of the corresponding LoA mapping documents.

4.2.3. Authentication

Describe the authentication mechanism, including the terms of access to authentication by relying parties other than public sector bodies

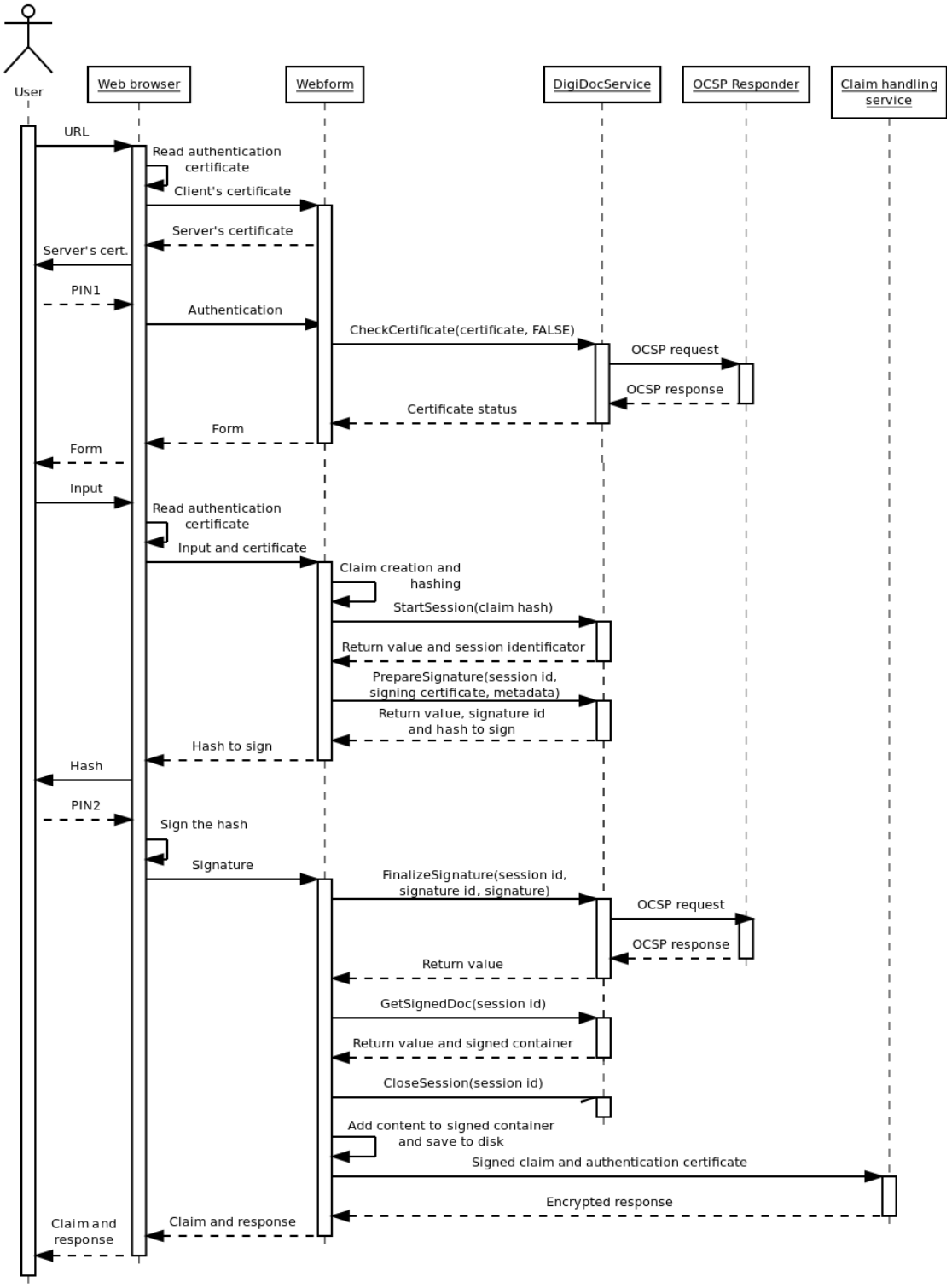
In general, there are no restrictions for the use of Estonian eID-based electronic authentication. Technically, authentication is an establishment of SSL/TLS communication with the client certificate. This means everyone (public or private sector) can use it. The only limitation is the use of the OSCP service for checking certificate validity – this service requires an agreement/contract with the CA. In terms of Mobiil-ID, for access to the central service, an agreement with a service provider is required. On the other hand, the CRL is publicly available, but, since CRL technology has its limitations, it is rarely used by the public sector and only with systems where reliability requirements are low.



Caption 1 - certificate chain in Estonian PKI

The authentication mechanism is described in section 2.3. of the corresponding LoA mapping documents.

The process flow of the Estonian eID electronic authentication and qualified electronic signature functionality in a web browser is demonstrated in the following caption.



Caption 2 – electronic authentication and qualified electronic signature functionality process flow in a web browser

4.2.4. Management and organisation

Describe the management and organisation of the following aspects:

(a) General provisions on management and organisation

General provisions are described in section 2.4.1. of the corresponding LoA mapping documents.

(b) Published notices and user information

Published notices and user information are described in section 2.4.2. of the corresponding LoA mapping documents.

(c) Information security management

Information security management is described in section 2.4.3. of the corresponding LoA mapping documents.

(d) Record-keeping

Record-keeping is described in section 2.4.4. of the corresponding LoA mapping documents.

(e) Facilities and staff

Facilities and staff are described in section 2.4.5. of the corresponding LoA mapping documents.

(f) Technical controls

Technical controls are described in section 2.4.6. of the corresponding LoA mapping documents.

(g) Compliance and audit

Compliance and audit is described in section 2.4.7. of the corresponding LoA mapping documents.

4.3. Interoperability requirements

Authorisation/access to Estonian e-services are based on a unique identifier. In the Estonian national infrastructure, the personal identification code is used as the unique identifier. Aliens who have been issued an Estonian identity document under the Identity Documents Act and all Estonian citizens have a personal identification code and are recorded centrally in the Estonian population register. The personal identification code consists of 11 digits, the first of which shows the sex of the person and the next six of which show her or his date of birth. The following three digits are sequential numbers for children born on the same day, and the last digit is a control number.

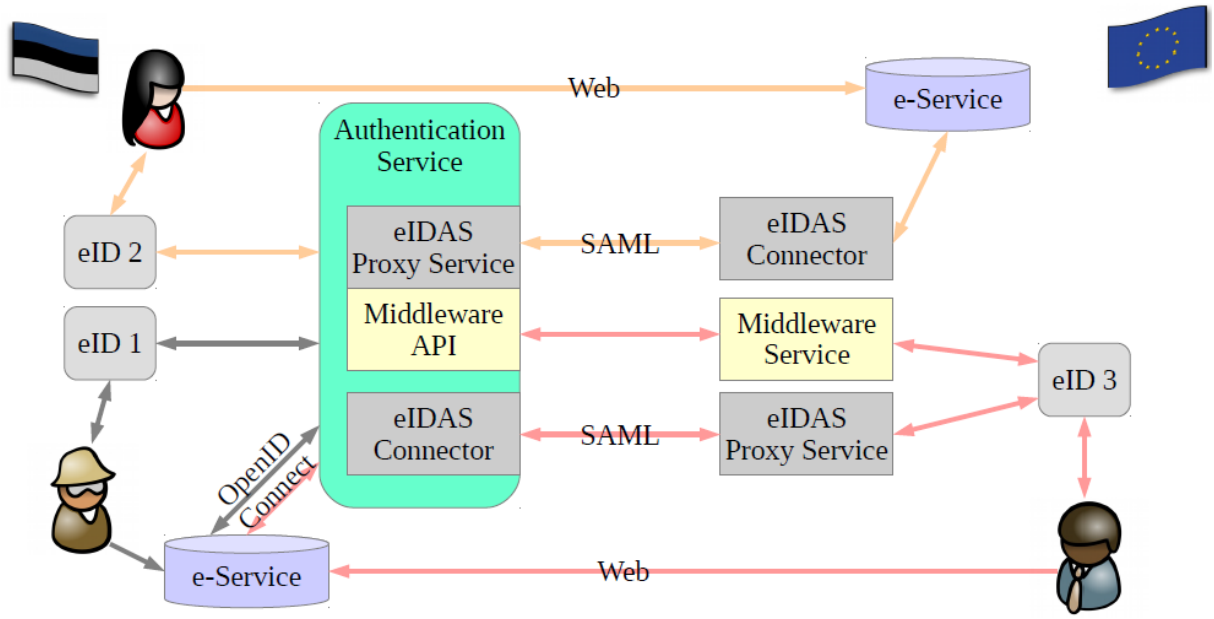
The population register is a database which unites the main personal data on Estonian citizens, citizens of the European Union who have registered their residence in Estonia, and aliens who have been granted a residence permit or right of residence in Estonia. State and local government agencies and legal and natural persons can access information in the population register in order to perform public duties, where the performance of public duties must be based on the main information of the population register. Natural and legal persons with legitimate interest can also access information in the population register. Information in the population register is preserved for an unspecified term. The use of information in the population register is guided by the provisions of the Population Register Act and the Personal Data Protection Act. The protection of data is monitored by the Data Protection Inspectorate and the Ministry of the Interior as the authorised administrator. Upon maintenance of the population register, the protection of the private life of individuals is ensured.

For cross-border interoperability within the EU, the Estonian state provides two central eIDAS-Node services:

1) the service node, for authentication with notified Estonian eID in another EU Member State e-service, and
2) the connector node, for authentication in Estonian public sector e-services with EU notified eID schemes.

The picture below describes scenarios and major components for domestic and cross-border authentication. Arrow colour indicates different scenarios:

yellow –Estonian eID holder authenticates in other EU Member State service portal or service; red – other EU Member State eID holder authenticates in the Estonian state service portal or service; grey – Estonian eID holder authenticates in the Estonian state service portal or service.



Both node services are operated by the EISA.

The service node has a landing page for SSL authentication. The OCSP service is used for certificate validation. On successful authentication, the minimum set of personal data is sent back to the requesting party. This data contains the person's name, unique identifier (personal identification code), and date of birth (also a part of the personal identification code).

The connector node is also used as subservice for a national authentication service. E-service providers can connect either directly to the connector node using a SAML protocol or through the national authentication service by using the OpenID Connect protocol. The connector node accepts only EU-notified eID schemes, and the national authentication service accepts additionally some national non-notified schemes (as a condition, these schemes have to be assessed against the LoA by the Estonian state). Among all IT security requirements, the ISKE sets requirements for authentication methods. This part also refers to the eIDAS LoA by mapping these towards the ISKE levels. Through this

mechanism, e-service providers will know which levels of eID means they can accept (both national non-notified and EU-notified ones).

Central eIDAS node services (operated by the EISA) are subject to the ISKE regulation and, through this mechanism, the requirements under the Commission Implementing Regulation (EU) 2015/1501 are met.

4.4. Supporting documents

List here all supporting documentation submitted and state to which of the elements above they relate. Include any domestic legislation which relates to the electronic identification provision relevant to this notification. Submit an English version or English translation whenever available.

Level of assurance mapping documents:
EE eID LoA mapping – ID card;
EE eID LoA mapping – RP card;
EE eID LoA mapping – Digi-ID;
EE eID LoA mapping – e-Residency Digi-ID;
EE eID LoA mapping – Mobiil-ID;
EE eID LoA mapping – diplomatic identity card.

List of national legislation related to the electronic identification in Estonia:

- Aliens Act, https://www.riigiteataja.ee/en/eli/501112017003/consolide
- Archives Act, https://www.riigiteataja.ee/en/eli/504032016002/consolide
- Citizenship Act, https://www.riigiteataja.ee/en/eli/513012017001/consolide
- Civil Service Act, https://www.riigiteataja.ee/en/eli/502012018003/consolide
- Consular Act, https://www.riigiteataja.ee/en/eli/527012016004/consolide
- Electronic Identification and Trust Services for Electronic Transactions Act, https://www.riigiteataja.ee/en/eli/527102016001/consolide
- Emergency Act, https://www.riigiteataja.ee/en/eli/505012018004/consolide
- Foreign Relations Act, https://www.riigiteataja.ee/en/eli/501022017002/consolide
- General Part of the Economic Activities Code Act, https://www.riigiteataja.ee/en/eli/504012018003/consolide
- Government of the Republic Act, https://www.riigiteataja.ee/en/eli/516102017008/consolide
- Identity Documents Act, https://www.riigiteataja.ee/en/eli/521062017003/consolide
- Personal Data Protection Act, https://www.riigiteataja.ee/en/eli/507032016001/consolide
- Police and Border Guard Act, https://www.riigiteataja.ee/en/eli/515092017001/consolide.
- Public Information Act, https://www.riigiteataja.ee/en/eli/516102017007/consolide
- Regulation 181 of the Government of the Republic, as of 22/12/2011, (in Estonian only), https://www.riigiteataja.ee/akt/113012015021?leiaKehtiv
- Regulation 2 of the Minister of the Foreign Affairs, as of 18/02/2017, (in Estonian only), https://www.riigiteataja.ee/akt/115022017008

- Regulation 3 of the Minister of Foreign Affairs, as of 23/05/2016, (in Estonian only), https://www.riigiteataja.ee/akt/118082017002
- Regulation 62 of the Minister of the Interior, as of 01/12/2015, (in Estonian only), https://www.riigiteataja.ee/akt/118112016005
- Regulation 77 of the Minister of the Interior, as of 18/12/2015, (in Estonian only), https://www.riigiteataja.ee/akt/102022018002
- Regulation 78 of the Minister of the Interior, as of 18/12/2015, (in Estonian only), https://www.riigiteataja.ee/akt/114012017016
- State Fees Act, https://www.riigiteataja.ee/en/eli/502012018002/consolide
- Statutes of the Identity Documents Database, (in Estonian only), https://www.riigiteataja.ee/akt/102022018003
- Statutes of the Information System Authority, (in Estonian only), https://www.riigiteataja.ee/akt/129122016014
- Statutes of the IT and Development Centre, Ministry of the Interior, (in Estonian only), https://www.smit.ee/pdf/pohimaarus.pdf
- Statutes of the Police and Border Guard Board, (in Estonian only), https://www.riigiteataja.ee/akt/128062017043
- Statutes of the Technical Regulatory Authority, (in Estonian only), https://www.riigiteataja.ee/akt/106012017003