# NOTIFICATION FOR FOR DIPLOMATIC IDENTITY CARD OF THE REPUBLIC OF ESTONIA

Police and Border Guard Board
Address: Pärnu mnt 139
15060 Tallinn
Estonia
Email: ppa@politsei.ee
Webpage: www.politsei.ee

2026

# 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 Group 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.

Egert Belitšev
Director General of the Police and Border Guard Board

## 1. General information

| **Title of scheme** | **Level of assurance** |
|---|---|
| LoA Mapping of the Estonian diplomatic identity card | high |

## 2. The authority/authorities responsible for the electronic identification scheme

| Name of the authority | Email address |
|---|---|
| **Ministry of Foreign Affairs (MFA)**<br>identity document management in embassies, identity management, and issuance of diplomatic identity cards | vminfo@mfa.ee |
| **Police and Border Guard (PBGB)**<br>eID scheme operator, and procurement of card blanks, personalisation and certificates | ppa@politsei.ee |
| **Ministry of the Interior**<br>policymaking in the field of identity management and personal identity documents | info@siseministeerium.ee |
| **Ministry of Justice and Digital Affairs**<br>policymaking in the field of IT and trust services | info@justdigi.ee |
| **Information System Authority (RIA)**<br>technical architecture of eID and cybersecurity incident management, supervision of trust service providers | ria@ria.ee |

## 3. Information on relevant parties, entities and bodies involved in the electronic identification scheme

### 3.1 Name of the entity or entities managing the registration process of the unique person identification data

The registration process of a diplomatic identity document is managed by MFA in cooperation with PBGB.

### 3.2 Party issuing the electronic identification means

The diplomatic 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 MFA.

### 3.3 Party operating the authentication procedure

The authentication procedure is assured (granted) by PBGB through a subcontracted qualified trust service provider (certification authority, CA).

### 3.4 Supervisory body

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

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

The MFA is a government body supervised according to national laws and legal acts applicable to government bodies. Supervisory body of the MFA is the Government of Estonian Republic.

RIA is the supervisory body of trust service providers.

## 4. Description of the electronic identification scheme

There are three types of Estonian eID means that are both physical identification documents as well as digital identity documents:

- ID card,
- the residence permit card (please see notification form for the ID card and residence permit card separately),
- diplomatic identity card.

This notification form covers the diplomatic identity card.

Estonian eID scheme is based on using PKI with cryptography according to best practices and using QSCD smartcards. All aforementioned cards have public key certificates (authentication, signing, encryption), also stored on the smart card.

The secure module on the smart card is a QSCD certified device. Smart card solution protects the private key from unauthorised access, copying, or tampering. Identity data (person’s first and last name and a personal identification code) is stored in the public key certificate. These certificates are accessible on the smart card and in the public LDAP repository.

The following parties are involved in the management of the eID scheme.

- The MFA is responsible for identity management and issuance of diplomatic identity cards. The issuing of the cards are regulated by the Foreign Relations Act, the Identity Documents Act and the Regulation 7 of the Minister of the Foreign Affairs, as of 09.03.2017.
- RIA is a government body which is responsible mainly for the governance of public sector IT. RIA also hosts the national CERT-EE and serve as a supervisory body for trust service providers. In terms of eID, RIA is responsible for eID hardware and software requirements. RIA maintains a set of requirements for eID, participates in procurements, and validates results as a partner organisation for PBGB. In addition, RIA develops and maintains middleware software and ID software for maintaining eID cards, also software for e-signatures.

- PBGB is operating under the authorisation of the Estonian Government to represent MFA for procurement of card blanks, personalisation and certificates. PBGB has a contractor for manufacture and personalisation of ID-1 format identity documents. Card manufacturer is Thales DIS Finland OY with a subcontractor for personalisation – Hansab AS.
- The CA is a qualified trust service provider – Zetes SA. Zetes SA is responsible for issuance of qualified certificates for electronic signatures and certificates for authentication for Estonian identity documents. They are responsible for the certificate life cycle: creation, activation, suspension and revocation.

Issuance of the diplomatic identity card is described in section 2.2.2 of the LoA mapping document.

Authentication mechanisms are described in section 2.3 of the LoA mapping document.

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

**List of the additional attributes which may be provided in relation to natural persons under the electronic identification scheme if requested by a relying party**

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.

**List of the additional attributes which may be provided in relation to legal persons under the electronic identification scheme if requested by a relying party**

Estonian eID means 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 Description of the supervisory regime of the electronic identification scheme including the evaluation process

### (a) The supervisory regime applicable to the party or parties issuing the electronic identification means

The MFA is supervised according to national laws and legal acts applicable to government bodies.

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 PBGB is a government body under the ministry.

RIA is also the supervisory body, who is responsible for supervisory tasks that are set out in article 17 of the eIDAS Regulation (the assessment of qualified status of trust services and issuance of licenses to provide trust services, the managing of trust list of Estonian trust service providers and supervising of notified trust services providers in meeting the established requirements).

**(b) The supervisory regime applicable to the party or parties operating the eIDAS node**

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

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

RIA is acting as 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 signing (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 8 of subsection 1 of § 36 of the Emergency Act.

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

Supervisory control of RIA is done by the Ministry of Justice and Digital Affairs.

Supervisory control is conducted in administrative authority by a higher authority over a subordinate governmental body in terms of lawfulness in action 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 means are 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 or parties issuing the electronic identification means under Article 11(2) of Regulation (EU) No 910/2014**

MFA has full liability in identity management for issuing of diplomatic identity cards.

**(c) Liability of the party or parties operating the eIDAS node 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 CA or a certification service provider who is a qualified trust service provider (in accordance with the eIDAS Regulation): Zetes SA.

### 4.1.3 Applicable management arrangements

Suspension by certificate owner of eID means after issuance is not possible by the request of the document holder. Only revocation is allowed.

According to section 17(1) of the Electronic Identification and Trust Services for Electronic Transactions Act a trust service provider has the right to suspend a certificate if there is a suspicion that incorrect data have been entered in the certificate or that it is possible to use the private key corresponding to the public key contained in the certificate without the consent of the certificate holder.

The legal framework of revocation of the electronic identification means is set by the eIDAS Regulation, with its implementing acts, and is regulated at the national level by the IDA and eID CP. The document holder is obliged to notify the issuing authority in case of theft or loss of the ID card, so that the certificates can be revoked.

Revocation of certificates can be done in person by appearing in a service point of the issuing authority or using revocation portal which is accessible 24/7. Revocation of the certificates means that the certificates are revoked; therefore, electronic functionality cannot be used.

## 4.2 Electronic identification scheme components

### 4.2.1 Enrolment

**(a) Application and registration**

Application and registration is described in section 2.1.1 of the LoA mapping document for diplomatic identity card.

**(b) Identity proofing and verification of a natural person**

Identity proofing and verification (natural person) is described in section 2.1.2 of the LoA mapping document for diplomatic identity card.

**(c) Identity proofing and verification of a legal person**

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

**(d) binding between the electronic identification means for natural and legal persons**

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

### 4.2.2 Electronic identification means management

**(a) Characteristics and design of the electronic identification means, including information on security certification**

eID means characteristics and design are described in section 2.2.1 of the LoA mapping document for diplomatic identity card.

**(b) Issuance, delivery and activation**

Issuance, delivery and activation is described in section 2.2.2 of the LoA mapping document for diplomatic identity card.

#### (c) Suspension, revocation and reactivation

Suspension and therefore reactivation of eID means by document holder is not possible; revocation is described in section 2.2.3 of the LoA mapping document for diplomatic identity card.

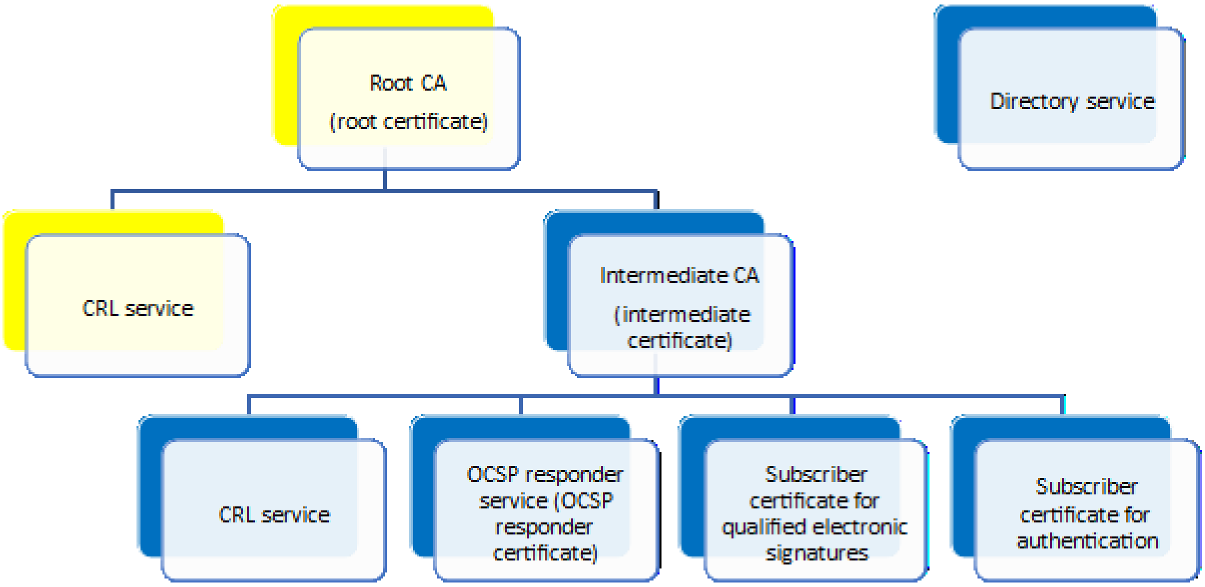
#### (d) Renewal and replacement

Renewal and replacement is described in section 2.2.4 of the LoA mapping document for diplomatic identity card.

### 4.2.3 Authentication

In general, there are no restrictions for the use of Estonian eID-based electronic authentication. The authentication is an establishment of TLS (transport layer security) communication with the client certificate, and everyone (public and private sector) can use it. The only limitation is the use of the OSCP (online certificate status protocol) service for checking certificate validity.

The diagram below illustrates the complete CA hierarchy and related services. In the schema below "Intermediate CA" represents the qualified CA that issues the Subscriber Certificates.


Root CA
(root certificate)
Directory service
CRL service
Intermediate CA
(intermediate certificate)
CRL service
OCSP responder service (OCSP responder certificate)
Subscriber certificate for qualified electronic signatures
Subscriber certificate for authentication

*Caption 1 CA hierarchy and related services for the Republic of Estonia*

The authentication mechanism of the ID card (including the diplomatic identity card) in case of TLS Client Certificate Authentication (CCA) is described in section 2.3 of the LoA mapping document for diplomatic identity card.

### 4.2.4 Management and organisation

#### (a) General provisions on management and organisation

General provisions are described in section 2.4.1 of the LoA mapping document for diplomatic identity card.

### (b) Published notices and user information

Published notices and user information is described in section 2.4.2 of the LoA mapping document for diplomatic identity card.

### (c) Information security management

Information security management is described in section 2.4.3 of the LoA mapping document for diplomatic identity card.

### (d) Record keeping

Record keeping is described in section 2.4.4 of the LoA mapping document for diplomatic identity card.

### (e) Facilities and staff

Facilities and staff are described in section 2.4.5 of the LoA mapping document for diplomatic identity card.

### (f) Technical controls

Technical controls are described in section 2.4.6 of the LoA mapping document for diplomatic identity card.

### (g) Compliance and audit

Compliance and audit are described in section 2.4.7 of LoA mapping document for diplomatic identity card.

## 4.3 Interoperability

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 Estonian 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 Estonian population register to perform public duties, where the performance of public duties must be based on the main information of the Estonian population register. Natural and legal persons with legitimate interest can also access information in the Estonian population register. Information in the Estonian population register is preserved for an unspecified term. The use of information in the Estonian 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 Estonian population register, the protection of the private life of individuals is ensured.

The Estonian eIDAS Node managed by RIA is integrated into the eIDAS Interoperability Framework in accordance with the eIDAS Technical Specifications of the eIDAS Technical Subgroup on eID of the EUDI Cooperation Group.

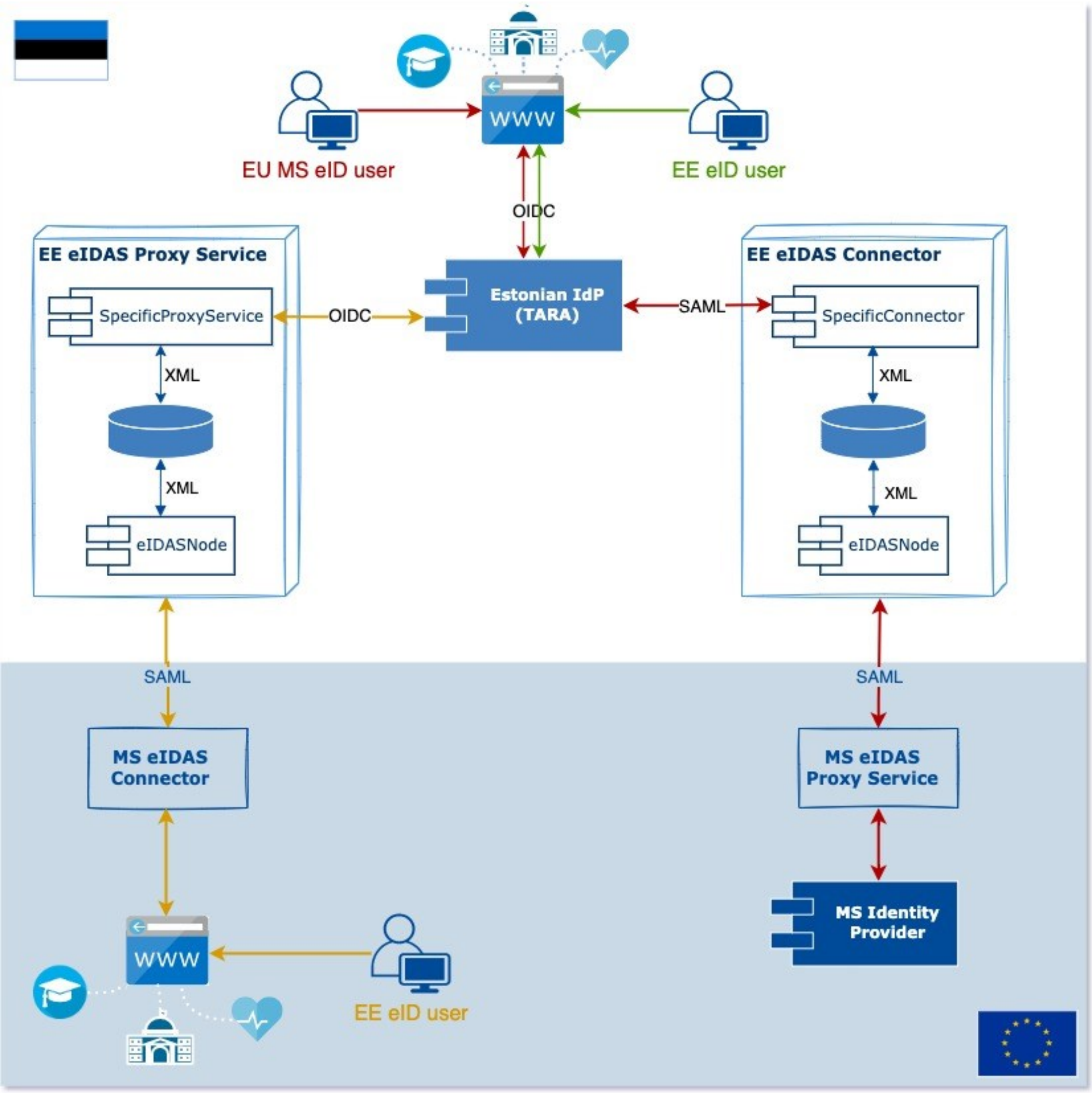
For cross-border interoperability, the RIA operates centralized eIDAS Node services, where:

1) eIDAS Proxy Service enables authentication requests from another EU Member State with Estonian notified eID schemes,

2) eIDAS Connector enables authentication in Estonian public sector online services with notified eID schemes of the EU.

The figure below presents main use cases and technical components for national and cross-border authentication. Each arrow indicates different scenarios, where:

- yellow indicates Estonian eID user who initiates authentication in the EU Member State (MS) e-service provider
- red indicates EU Member State (MS) eID user who initiates authentication in the Estonian e-service provider
- green indicates Estonian eID user who initiates authentication in the Estonian e-service provider.



*Caption 2 Main technical components for national and cross-border authentication*

The Estonian eIDAS Proxy Service uses the State Authentication Service (TARA) interface, acting as an eIDAS Identity Provider (IdP).

Estonian eIDAS Proxy Service structure relies on the operating principles of the eIDAS Node sample software, including two Java web applications (SpecificProxyService and eIDAS Node) and a database. The SpecificProxyService is responsible for a communication with the TARA, which uses OIDC protocol as an authentication protocol. The eIDAS Node application in the Estonian eIDAS Proxy Service implementation is part of the European Commission's eIDAS Node sample software 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.

On a successful authentication, the minimum set of personal data is sent back to the requesting party. The minimum data set of 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 of a legal person contains current legal name, Business Registry code (identifier for a legal person in Estonia). The minimum data set attributes of a natural person are based on a data available on the diplomatic identity card certificate; the legal person's minimum data set attributes are requested from Estonian e-Business Registry using X-Road data exchange layer.

Similarly to the Estonian eIDAS Proxy Service, the Estonian eIDAS Connector structure relies on the operating principles of the eIDAS Node sample software, including two Java web applications (SpecificConnector and eIDAS Node) and a database.
The SpecificConnector is responsible for a communication with the TARA and the Estonian eIDAS Node application.
The Estonian eIDAS Connector is integrated with German eIDAS middleware instance that implements an adapted eID server with an eIDAS interface and realises the server-side component of the authentication process with the online ID function for German notified eID.

The Estonian eIDAS Node services and the TARA are operated within Estonian Information Security Standard (E-ITS) aligned to ISO/IEC 27001 and Estonian public-sector security baseline requirements. Through this mechanism, the requirements under the Commission Implementing Regulation (EU) 2015/1502 are met.

## 4.4 Supporting documentation

Documentation presented
LoA mapping document for diplomatic identity card on level "High"
White paper
Interoperability mapping

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

- Aliens Act, https://www.riigiteataja.ee/en/eli/ee/506012026003/consolide/current
- Citizenship Act, https://www.riigiteataja.ee/en/eli/528072025002/consolide
- Civil Service Act, https://www.riigiteataja.ee/en/eli/ee/512082025001/consolide/current
- Consular Act, https://www.riigiteataja.ee/en/eli/516122025001/consolide
- Electronic Identification and Trust Services for Electronic Transactions Act, https://www.riigiteataja.ee/en/eli/530122025007/consolide
- Emergency Act, https://www.riigiteataja.ee/en/eli/ee/514012026006/consolide/current
- General Part of the Economic Activities Code Act, https://www.riigiteataja.ee/en/eli/511092025011/consolide
- Government of the Republic Act, https://www.riigiteataja.ee/en/eli/ee/504092025010/consolide/current
- Identity Documents Act, https://www.riigiteataja.ee/en/eli/ee/505012026002/consolide/current
- Foreign Relations Act, https://www.riigiteataja.ee/en/eli/ee/530092025011/consolide/current
- Personal Data Protection Act, https://www.riigiteataja.ee/en/eli/ee/522092025009/consolide/current

- Police and Border Guard Act, https://www.riigiteataja.ee/en/eli/527102025003/consolide
- Population Register Act, https://www.riigiteataja.ee/en/eli/503122025003/consolide
- Public Information Act, https://www.riigiteataja.ee/en/eli/ee/511092025008/consolide/current
- Regulation 62 of the Minister of the Interior, as of 01.12.2015 (in Estonian only), https://www.riigiteataja.ee/akt/118112016005?leiaKehtiv
- Regulation 78 of the Minister of the Interior, as of 18.12.2015 (Statutes of the Identity Documents Database, in Estonian only), https://www.riigiteataja.ee/akt/114012017016?leiaKehtiv
- Regulation 20 of the Minister of the Interior, as of 01.08.2025 (in Estonian only), https://www.riigiteataja.ee/akt/129072025001
- Statutes of the Data Protection Inspectorate (in Estonian only), https://www.riigiteataja.ee/akt/118092025005?leiaKehtiv
- Statutes of the IT and Development Centre, Ministry of the Interior (in Estonian only), https://www.riigiteataja.ee/akt/109072024006?leiaKehtiv
- Statutes of the Ministry of the Interior (in Estonian only), https://www.riigiteataja.ee/akt/122012025004
- Statutes of the Ministry of Foreign Affairs (in Estonian only), https://www.riigiteataja.ee/akt/114072023002?leiaKehtiv
- Statutes of the Ministry of Justice and Digital Affairs (in Estonian only), https://www.riigiteataja.ee/akt/116092025018?leiaKehtiv
- Statutes of the Police and Border Guard Board (in Estonian only), https://www.riigiteataja.ee/akt/128062025002?leiaKehtiv
- Statutory Fees Act, https://www.riigiteataja.ee/en/eli/ee/530122025005/consolide/current
- RIA statutes (in Estonian only), https://www.riigiteataja.ee/akt/127122024010?leiaKehtiv
- Regulation 7 of the Minister of the Foreign Affairs, as of 09.03.2017 (in Estonian only), https://www.riigiteataja.ee/akt/126082025005?leiaKehtiv
- Regulation 3 of the Minister of Foreign Affairs, as of 23/05/2016," (in Estonian only), https://www.riigiteataja.ee/akt/126092025004?leiaKehtiv