Overview of the Estonian eID system

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

Table of contents

Disclaimer: this document is partly based on Cybernetica's overview of the Estonian electronic identity system which has been written at the request of the Estonian Information System Authority (RIA) to explain the setup, organisation, and the uses of the Estonian e-identity ecosystem.

1. Introduction

This document gives an overview of the Estonian eID means. The following eID means can be used for physical and electronic identification:

- Identity card (ID card)
- Residence permit card (RP card)
- Diplomatic identity card

Smart ID, Mobile ID and e-resident's digital ID can be only used for electronic identification.

Reliable and secure personal identification as well as physical and digital identity management are the basis for a credible process of issuing identity documents. Estonia has long-term experience (from the beginning of 2002) in using electronic authentication and is a global leader in the context of e-government.

All Estonian eID means fulfil all requirements of the eIDAS [1] Level of Assurance "high".

The general principles of identity management policy include the following:

- the state determines the person's identity,
- one person has one identity,
- use of another person's identity or identity document is forbidden,
- identity management is performed by the state and in a centralised manner,
- both physical and digital identity documents are inextricably and uniquely linked to the document holder's identity,
- certificates that enable digital identification and a qualified electronic signature for digital identity of a document are uniquely associated with the document holder's personal data,
- data of both physical and digital documents, including certificates for authentication and electronic signing, are publicly verifiable,
- identity documents and the supporting software are secure.

Estonian eID scheme is based on using PKI (public key infrastructure) with cryptography according to best practises and using QSCD (qualified signature creation device) smartcards.

1.1 Historic overview

The public service side of the Estonian eID ecosystem is built on legal foundations that regulate its operation. When the Estonian ID card was first created (initially only as one specific kind of identity document), rules regarding the issuance of the card were laid down in:

- Identity Documents Act [2] (February 15th, 1999),
- Digital Signatures Act [3] (March 8th, 2000).

The Identity Documents Act regulated, inter alia, the physical features of the ID card while the electronic features of the card were regulated by the Digital Signatures Act. Neither act contained any references to the other.

Estonian ID cards with digital functionality were first issued in 2002, which allowed to start using authentication and digital signing widely in digital environment. Estonia is internationally recognised as E-state, we have implemented digital signing and digital e-services with wide-spread usage of eID means.

1.2 Unique usage environment

The complexity of the Estonian eID ecosystem is very high.
The eID ecosystem can be broken down into the following aspects which must be considered as a single functional entity:

- **legal** (laws, regulations, directives)
- **organisational** (collaboration, data exchange between institutions and private companies)
- **technical** (protocols, standards, devices)
- **security** (incident reporting, accountability, responsible vulnerability notification)
- **supervision**

The ecosystem is **pervasive**, **universal**, and **ubiquitous in its use**. These three key features emphasise the importance of the consistency of new solutions with the existing Estonian eID ecosystem. To maintain the present lifestyle of Estonian residents, it is vital to ensure the cohesion of new systems with existing ones.

The functionality of the Estonian eID ecosystem is universal. The eID means (ID card, RP card, diplomatic identity card, e-resident digital ID, Mobile-ID, Smart-ID) can be used for authentication and the creation of digital signatures. In most cases they can provide similar user experience and be equally used in all e-services. The eID means issued to citizens and residents are identical in their functionality.

With this in mind the use of the Estonian eID ecosystem among Estonian citizens and residents is extensive and ubiquitous. It involves all walks of life, starting from signing contracts and declaring taxes, education and health, and ending with numerous government and commercial portals. Excluding shopping in global e-stores, everything vital can be done remotely, using standard eID means.

2. The concept of identity and the nature of the eID ecosystem

For a person to be issued with an eID means, they must have a base identity duly registered in the Estonian population register [4]. Identity is based on the personal identification number. For applying eID means, the issuing authorities verify (PBGB, MFA) the person's identity. On fundamental bases the

identity data comprises of the person's name and personal identification number. The personal identification number is used for linking specific eID means with the base identity.

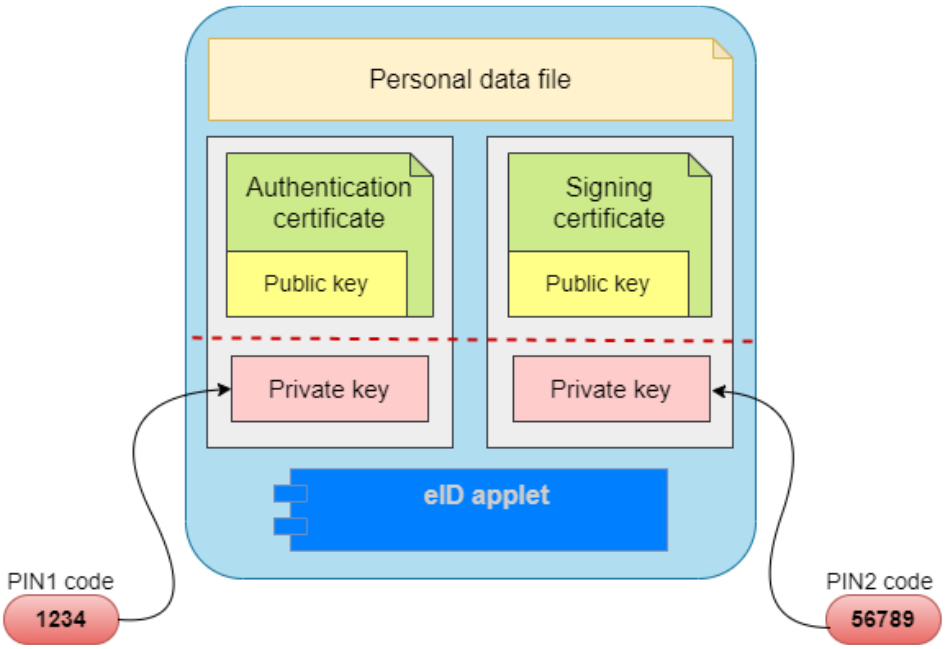
3. eID means

An eID means is used for the storage of cryptographic keys necessary for the use of eID and allows these keys to be used materially.

Smart card based eID means store private keys on the chip, while authentication and digital signature functions have been implemented in the form of a special program (applet) loaded on the card.

In addition to authentication and qualified digital signature creation, the eID means can also be used for encrypting and decrypting documents (only applicable for ID cards, RP cards and diplomatic identity cards). In case there is a need to forward confidential information via e-mail to other parties. ID software allows to easily encrypt both digitally signed and unsigned documents.

The figure below illustrates the key elements of an eID means, using the ID card as an example. The actual means may contain more elements, such as previous keys, platform-specific keys, owner's technical keys for the addition of personal certificates, etc. The means may also contain fewer elements.



Caption 1 Key elements of eID means

For security reasons, it is recommended that a person simultaneously have multiple eID means of different types, but the identity of the person always remains the same. This enables them to carry on living a normal electronic life even if one of the eID means has expired, is not functioning properly, or its security is temporarily compromised.

In certain cases, an eID means can be registered in an electronic environment on the basis of another valid eID means. This simplifies the registration process, as the user does not need to visit a service office.

Estonian ID card

Estonia issues the ID card as the primary and mandatory document for identifying its citizens and European Union citizens living in Estonia. The first ID cards were issued on January 28th, 2002. The ID card is a physical identification document and has advanced electronic functions that facilitate secure authentication and a legally binding qualified electronic signature enabling safe access to e-services and convenient way to make electronic transactions.
The ID card is recognised as a travel document for Estonian citizens.
State fee is established for ID card.

The Estonian Police and Border Guard Board (hereinafter PBGB) is responsible for issuance of the ID card.

Caption 2 Specimen of the ID card issued since November 15, 2025

Residence permit card

Estonia issues the RP card as a mandatory identity document for third-country nationals who are residing in Estonia based on a valid residence permit or right of residence since 2011. The RP card is a physical identification document and has advanced electronic functions that facilitate secure authentication and a legally binding qualified electronic signature enabling safe access to e-services and convenient way to make electronic transactions. The RP card is not a travel document but must be carried along with the passport of the country of citizenship in order to return to Estonia.
RP card is not a travel document.
State fee is established for RP card.

The PBGB is responsible for issuance of the RP card.

Caption 3 Specimen of the RP card issued since November 15, 2025

Diplomatic identity card

The diplomatic identity card is a physical identification document and has advanced electronic functions that facilitate secure authentication and a legally binding qualified electronic signature enabling safe access to e-services and convenient way to make electronic transactions.

There are two types of Estonian diplomatic identity cards: diplomatic card and service card.

1) A diplomatic card is issued to a diplomat of a foreign diplomatic mission and consular post accredited to Estonia (hereinafter referred to as *a foreign mission*) and his/her family member who is a foreign national.

2) A service card is issued to a foreign national who is the administrative or technical employee of a foreign mission and his/her foreign national family member, a foreign national who is a private servant, a foreign national employee of a mission of an international organization and an international organization or other institution established by an international agreement located in Estonia (hereinafter referred to as *other institution*) and his/her foreign national family member, an honorary consul and, in other justified cases provided for in an international agreement, an Estonian citizen or permanent resident working in a foreign mission or other institution.

Below is the caption of the specimens of the cards manufactured since November 15th, 2025. There are eight different categories with 18 series of cards:

1) Diplomatic card category A (series A1, A2, A3) and category B (series B1, B2, B3),
2) Service card category C (series C1, C2, C3), category D (series D1, D2); category E, category F, category HC and category G (series G1, G2, G3, G4).

The reverse side of the card includes text based on the privileges of the bearer of the card. In addition, the reverse side contains information about the right of residence in Estonia and conditions to enter the territory of Schengen States.

Caption 4 Specimen of the Diplomatic Card issued since 15.11.2025

Caption 5 Specimen of the Service Card issued since 15.11.2025

A diplomatic identity card is issued free of charge and grants the document holder immunities and privileges outlined in the Vienna Convention on Diplomatic Relations [5] and other international conventions and treaties according to the relevant category. 09.03.2017 regulation no. 7 of the Minister of Foreign Affairs (MFA) [6] establishes the procedure for issuing a diplomatic identity card, the format and technical specification of the card, and the list of information entered on the card.
PBGB provides production and delivery service for the MFA.
The MFA is responsible for issuance of the diplomatic identity card

Mobile-ID and Smart-ID

Mobile-ID and Smart-ID both provide authentication and digital signature creation functions. Private keys for Mobile-ID are stored on SIM card. For Smart-ID the private keys are split into two parts (smart device and server), and they are never combined in one place, increasing their security. Smart card readers are not required neither for Mobile-ID nor Smart-ID.

Smart-ID is a private scheme and not notified, but it has been evaluated for national use. Smart-IDs issued to persons with Estonian personal identification numbers meets the criteria of high assurance level for electronic identification [7].

Mobile ID is a state issued digital ID and is notified to LoA high.

4. Fields and responsibilities

For the operational management of the Estonian eID ecosystem the following parties are involved.

4.1 Public authorities

Ministry of the Interior
The role of the Ministry of the Interior in the eID ecosystem is to develop legal bases for the administration of identity policy.

Ministry of Justice and Digital Affairs
The Ministry of Justice and Digital affairs organises, promotes, and coordinates the digital development of the public sector, coordinates the development of public services and information systems, and organises the development of national digital solutions and the provision of shared information technology services.

Ministry of Foreign Affairs
In the context of the eID ecosystem, the role of the Ministry of Foreign Affairs is to issue, deliver, and revoke diplomatic identity cards. Foreign missions can also accept applications for and issue some other national eID means.

Private sector eID means providers
The Estonian eID ecosystem currently includes one eID means provided by a private company: Smart-ID, which is provided and administered by SK ID Solutions AS.

Estonian Information System Authority
The functions of RIA are regulated by its statutes [60]. RIA is a government agency consisting of a number of departments focusing on different fields. In the context of the eID ecosystem, RIA's role is to act as a competence centre responsible for formulating visions and strategies for the development of the eID field, as well as to advocate for and shape the positions of the eID field in Estonia. RIA's roles in the eID ecosystem are as follows:

In the sphere of the state information system:

- Coordinates the development of authentication, digital signature creation, and encryption software, and the Internet-based authentication and digital signature creation system, including:
    - Coordination of the long-term evolution of the entire eID field with the involvement of various institutions,
    - Maintenance of the id.ee portal,
    - Development of software components used in the eID ecosystem, such as:
        - Development of the DigiDoc4 desktop application,
        - Development of the RIA DigiDoc application for smart devices,
        - Development of the Web eID web-based authentication and signature creation solution,
        - Development of libraries, such as *digidoc4j* and *libdigidocpp*, etc.
    - Maintenance of various services provided to public-sector institutions that are critical for the operation of the Estonian eID ecosystem, as well as servers hosting these services, including:

        - Authentication services (TARA - State Authentication Service, used for authentication by public sector institutions, state SSO (single sign-on access) service),
        - SiGa digital signature creation service,
        - SiVa digital signature validation service,
        - timestamping service intermediation,
        - Web eID solution (web-based authentication and digital signature creation);
    - Customer support (including by phone),
- Procurements.

In the sphere of cybersecurity:

- Organisation of the protection of critical information infrastructure (CIIP)
- Carries out administrative and state supervision (including supervision over the Estonian eID ecosystem in accordance with legislation).
- Enforces administrative procedures and handles misdemeanours.

RIA also organises various awareness-raising campaigns and trainings in different spheres, including eID ecosystem-related areas.

The RIA Cybersecurity Centre is responsible for cybersecurity, one of RIA's two core areas of activity.

Police and Border Guard Board

The roles and responsibilities of the PBGB in the Estonian eID ecosystem are:

- Issuance of identity documents (including documents that can be used as eID means),
- Development of identity documents, managing contracts with service providers,
- Procurement of ID-1 format identity documents.

IT and Development Centre of the Ministry of the Interior

The IT and Development Centre of the Ministry of the Interior (SMIT, www.smit.ee) develops and maintains the technology (including software) and systems required for the performance of the PBGB's functions. This also includes the development and maintenance of the systems required for identity management and the issuance and management of identity documents.

4.2 Private parties

Trust service providers

In the context of the Estonian eID ecosystem, a trust service provider (TSP) is an organisation responsible for the management and storage of personal certificates related to the eID ecosystem. Other examples of trust services also include timestamping services. A number of services in Estonia are divided between the controller (in most cases, PBGB) and the processor. The immediate service provider in these situations is the processor. The next two subsections present an overview of the key trust service providers operating in the Estonian eID – SK ID Solutions AS and Zetes Estonia OÜ.

SK ID Solutions AS

For a long time, a single Estonian company provided trust services as a core business: this was SK ID Solutions AS. SK ID Solutions AS maintains the certificates for ID cards, RP cards, diplomatic identity cards and e-resident digital IDs issued until November 15th 2025, Mobile-ID and Smart-ID.

SK ID Solutions AS provides the following services to Estonian eID ecosystem participants:

- Issuance of qualified signature creation certificates,
- Issuance of authentication certificates,
- Electronic timestamping service,
- Provision of access to the registry of certificates associated with ID cards, RP cards and diplomatic identity cards via LDAP,
- Responding to electronic queries about certificate validity (OCSP/CRL),
- Deactivation or revocation of certificates, if necessary.

SK ID Solutions AS is the owner, developer, issuer, and service provider of the Smart-ID. They also issue e-seal certificates to companies and agencies and maintain the Mobile-ID scheme. SK ID Solutions AS is categorised as a vital service provider.

Zetes Estonia OÜ

As of the launch of new ID cards on November 15th, 2025, the trust service provider for the new generation ID-1 format identity documents is Zetes SA. The PBGB has a contract with Zetes SA for the provision of certification and qualified trust services, who has transferred the obligation to execute the contract on Zetes Estonia OÜ, a 100% subsidiary of Zetes SA.

The duties of the certification authority in certification service and qualified trust service cover the following:

- issuance of root certificates and intermediate certificates for the creation of a certificate chain,
- issuance of qualified certificates for electronic signatures and certificates for authentication and encryption,
- service of Subscriber certificates,
- provision of Online Certificate Status Protocol (OCSP) responder service,
- provision of Certificate Revocation List (CRL) service,
- provision of Lightweight Directory Access Protocol (LDAP) directory service,
- provision of test services.

Card manufacturer

Thales DIS Finland OY

The PBGB has a contract with Thales DIS Finland OY for ID-1 format identity document blanks, personalisation and related services. Thales DIS Finland OY's subcontractor is Hansab AS.

Thales DIS Finland OY is responsible for:

- production, processing and logistics of document blanks with a chip certified as a QSCD,

- the provision of document personalisation services (provided by subcontractor of card manufacturer),
- the provision of post-issuance services for documents,
- processing of personal data in accordance with Estonian, EU and international regulations, standards, requirements and instructions.

External Service Provider
The issuer of the document may hand over the document through a secure service provider if requested by the applicant at application. The secure service provider shall be determined by the issuing authority of the document.

The PBGB has a contract with Hansab AS for external service provision. Hansab AS provides the service of handing over identity documents through a subcontractor, who hands out documents in external service provider's service points nation-wide.

Requirements for external service providers must ensure that the service provided is equally secure as the service provided by the issuing authority and the foreign representations. Requirements for the external service provider are set out in the contract.

5. Authentication

In the context of web technology, technical verification of identity denotes an operation whereby the user is required to sign session data transmitted by the server using a private key found on their eID means and return the signature and authentication certificate. The server then verifies the validity of the certificate (e.g. over OCSP – online certificate status protocol) and whether it has been issued by a trusted certification authority. The server then uses the public key found in the certificate to verify the validity of the submitted cryptographic signature and whether it has been created for the data transmitted by the server. If all the verification steps are passed, then the user participating in the session can be assumed to have control over their eID means and the user identity presented as a part of the certificate can be considered verified. The authentication solution described above can also be characterised as an **external authentication vector** from the information system's perspective.

The authentication normative [8] sets out two main requirements for public sector information systems. First, an authentication module should not be built in-house; relevant RIA libraries should be used for this purpose. Second, the authentication module should be isolated from the information system. This is a major difference compared to systems not using the possibilities afforded by eID, as the latter need to keep local account of persons, their identities and identity carriers or usernames and passwords (credentials), which increases the complexity of the system.

Authentication can be carried out either directly by the information system offering an electronic service or via other 'middlemen', such as authentication services (TARA, GovSSO – government single sign-on access). The e-service provider is frequently also called the relying party.

6. Life cycle

ID-1 format identity documents are issued by the issuing authorities.

In case of ID-1 format identity documents, necessary data of the applicant is captured and is transferred to the card manufacturer via a secure exchange interface for card personalisation. The card manufacturer produces, and their subcontractor personalises the ID-1 format identity document. Upon receiving the card, the applicant also receives a securely sealed envelope with three codes in it (PIN1, PIN2 and PUK): PIN1 for authentication and encryption purposes, PIN2 for a qualified electronic signature and PUK to reset blocked PIN codes in the ID software.

The ID card or RP card is handed over in person, to a legal guardian or an authorised representative in a service point of PBGB, external service provider service point or a foreign representation. In case of diplomatic identity cards, the cards are handed over by MFA official. After hand-over of the document, the card is activated by the issuing authority after the identity-proofing of the receiver.

In order to avoid illegitimate use of lost or stolen eIDs, the holder of the Estonian eID means needs to be able to revoke certificates. The certificates of the card can be revoked in the issuing authority service point in person and in the case of documents issued from November 15th, 2025 also in the revocation portal [9]. A certificate owner may request revocation of their own certificates or for another person over whom they have legal custody.
E-services cannot be used/accessed if the certificates are revoked.

After revocation the certificates cannot be used. To regain access to e-services after revocation has been completed, a new document must be applied for (with new certificates).

List of References

[1]	eIDAS Regulation – Regulation (EU) 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market, as amended by Regulation (EU) 2024/1183 as regards establishing the European Digital Identity Framework https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02014R0910-20241018
[2]	Identity Documents Act https://www.riigiteataja.ee/en/eli/ee/521052024002/consolide/current
[3]	Digital Signatures Act (not in force currently) https://www.riigiteataja.ee/akt/71878
[4]	Population Register Act https://www.riigiteataja.ee/en/eli/ee/503122025003/consolide/current
[5]	Vienna Convention on Diplomatic Relations https://treaties.un.org/pages/viewdetails.aspx?src=treaty&mtdsg_no=iii-3&chapter=3&clang=_en
[6]	Regulation 7 of the Minister of the Foreign Affairs, as of 09.03.2017 (in Estonian only) https://www.riigiteataja.ee/akt/126082025005
[7]	Information System Authority. Integration tools of eID. https://www.ria.ee/en/state-information-system/electronic-identity-eid-and-trust-services/integration-tools-eid
[8]	Information System Authority. Requirements for authentication solutions within the information system of the Republic of Estonia (authentication normative), 2017 (in Estonian). https://ria.ee/media/1971/download
[9]	Revocation portal https://revocation-portal.eidpki.ee/en/landing