REPUBLIC OF ESTONIA
POLICE AND BORDER GUARD BOARD

LoA Mapping of the Estonian ID card on level “High”

2026

Table of contents

List of Definitions

Term	Definition
authentication	A unique identification of a person by checking their alleged identity.
biometric data	Biometric data is a facial image, fingerprint images and signature or image of signature.
certificate	Public key, together with additional information, laid down in the certificate profiles, rendered unforgeable via encipherment using the private key of the Certification Authority which issued the certificate.
electronic identification	The process of using person identification data in electronic form uniquely representing either a natural or legal person, or a natural person representing a legal person.
electronic identification scheme	A system for electronic identification under which electronic identification means are issued to natural or legal persons, or natural persons representing legal persons.
electronic signature	Data in electronic form which is attached to or logically associated with other data in electronic form, and which is used by the signatory to sign. Signatory means natural person who creates an electronic signature.
Estonian citizen	A person who holds Estonian citizenship according to the Estonian Citizenship Act.
Estonian population register	A database which unites the main personal data on Estonian citizens, citizens of the EU and third-country national who have been granted a residence permit or right of residence in Estonia.
foreign representation of the Republic of Estonia	An official unit (embassies, consulates, representations) operating under the MFA in foreign country, responsible for representing Estonia's interests, maintaining diplomatic and consular relations, and providing consular activities.
foreigner	A citizen of a member state of the European Union, except Estonia, or of a member state of the European Economic Area or of the Swiss Confederation (hereinafter a *citizen of the European Union*); or a third-country national.
HUB	HUB is a secure data exchange interface between the PBGB, the card manufacturer, and Certification Authority to support standardised data exchange related to the issuance of ID-1 format identity documents.
ID card	A mandatory identity document of Estonian citizens and EU citizens permanently residing in Estonia. In addition to regular identification purposes, an ID card can also be used for identification in an electronic environment and for providing digital signatures. Estonian citizens can also use the ID card as a travel document within the EU.
ID card administration portal	Portal for looking up given PUK code and re-key of certificates, available at https://www.idhaldusportaal.ee/en/.
ID software	An end-user desktop application for personal maintenance of smartcard-based eID.

ID-1 format identity documents	Documents in ID-1 format are ID card, e-resident digital ID, residence permit card and diplomatic identity card.
identity documents database (ITDAK)	A record-keeping system for ensuring the internal security of the state, including the identification of persons and the issuance and revocation of identity documents specified in subsection 15 (4) of the IDA, as well as people who have applied for mentioned documents. The basic data collected by the information system are: - Data related to the identification or verification of a person's identity, - Data related to the applicant for an identity document, - Data on the application for an identity document, - Data on the identity document.
Ministry of Foreign Affairs (MFA)	In this document, the MFA includes either both or one: the MFA headquarters and/or foreign represenations abroad (i.e. embassies, consulates, honorary consuls, consular missions).
personal identification code	A unique 11-digit identifier for individuals in Estonia based on a person's gender, date of birth, serial number and check digit.
PIN code	Activation code for the certificate enabling digital authentication and the certificate enabling qualified electronic signatures.
private key	The key of a key pair that is assumed to be kept in secret by the owner of the key pair, and that is used to create electronic signatures and/or to decrypt electronic messages, records or files that were encrypted with the corresponding public key.
public key	The key of a key pair that may be publicly disclosed by the owner of the corresponding private key and that is used by relying parties to verify electronic signatures created with the owner's corresponding private key and/or to encrypt messages, records and files so that they can be decrypted only with the owner's corresponding private key.
PUK	Personal unlocking key.
register for authentic documents	Database of documents of the European Union, of its member states, and other countries, e.g. PRADO (Public Register of Authentic identity and travel Documents Online).
revocation portal	Portal for revocation of certificates, available at https://revocation-portal.eidpki.ee/en/landing.
secure service provider for handing out identity documents	External service provider with the competency to hand out identity documents.
self-service	Digital environment, where a person can apply for an identity document, available at https://etaotlus.politsei.ee/ekpid/login.
Web eID	The Web eID solution enables the use of ID-1 format identity documents for secure authentication and digital signing on the web.
X-tee	Data exchange platform that allows secure and standardised data exchange between different institutions, including state authorities and private sector, available at https://www.x-tee.ee/home.

List of Acronyms

Acronyms	Definition
ABIS	Automated Biometric Identification System
CA	Certification Authority
CC	Common Criteria
CCA	Client Certificate Authentication
CERT	Computer Emergency Response Team
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List, a list of invalid (revoked) certificates
EAL	Evaluation Assurance Level
eID	Electronic Identity
eIDAS	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 (always referred together as eIDAS regulation)
E-ITS	Estonian Information Security Standard
ENISA	The European Union Agency for Cybersecurity
ETSI	The European Telecommunications Standards Institute
EU	European Union
GDPR	General Data Protection Regulation - Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data
ICT	Information and communication technology
IDA	Identity Documents Act
ISO	International Organization for Standardization
ITDAK	Identity Documents Database
LDAP	Lightweight Directory Access Protocol
LoA	Levels of Assurance
MFA	The Ministry of Foreign Affairs
OCSP	Online Certificate Status Protocol
OTP	One Time Password
PCI	Payment Card Industry
PBGB	The Estonian Police and Border Guard Board
PKI	Public Key Infrastructure
QSCD	Qualified Signature Creation Device
QTS	Qualified Trust Service
QTSP	Qualified Trust Service Provider
RIA	Information System Authority of the Republic of Estonia (Riigi Infosüsteemi Amet)
RSA	Rivest-Shamir-Adleman
SMIT	The IT and Development Centre of the Ministry of the Interior
TARA	State Authentication Service
TLS	Transport Layer Security

1. Introduction

The present document explains how the Estonian ID card meets the requirements for the Level of Assurance (LoA) 'high' pursuant to the requirements of the eIDAS LoA defined in Commission Implementing Regulation (EU) 2015/1502 [1] pursuant to Article 8(3) of the eIDAS Regulation [2] [(EU) 910/2014], as amended by Regulation (EU) 2024/1183 as regards establishing the European Digital Identity Framework (always referred together).

2. Technical specification and procedures

The elements of technical specifications and procedures outlined in this annex of the Commission Implementing Regulation (EU) 2015/1502 [1] will be used to determine how the requirements and criteria of article 8 of Regulation (EU) will be applied for electronic identification means issued under an electronic identification scheme.

ID-1 is an Estonian eID platform that is implemented on top of Aquarius chip (product name: AQUARIUS_CA_09) from Thales, which is CC EAL6+ certified. The eID functionality is managed by the application IAS Classic v5.2.1 with MOC Server v3.1 (EAL5+) on the operating system MultiApp V5.1 (version C, EAL6+)
ID-1 operates on:

- Globalplatform 2.3.1
  - Secure messaging: SCP03 i= 00, 01, 10, 11, 20, 21, 30, 31, 60, 61, 70 & 71 (AES 128, 192, 256);
  - Optional and Mandated DAP up to RSA2K: applet versioning and integrity during post-issuance;
  - Delegated Management up to RSA2K: secure postissuance card management delegation operations;
  - Multiple Security Domains: Segregation of roles on the same card;
  - Extradition: extradites an application from a Security Domain to another.
- Globalplatform Privacy Framework
  - Privacy Enhanced ID Configuration: SCP 21.
- Java Card 3.1;
  - Multiple Logical channels: concurrent applets addressed simultaneously during the same card session;
  - Garbage collector: recovers memory space of deleted or useless objects.
- Applet optimiser: Saves at least 10% of NVM memory required by applications.
- PACE support: privacy protection with explicit user consent.

Applet supports all required minimum public key features for easy integration in various PKI. It includes the certificate for electronic authentication and encryption as well as certificate for providing a qualified electronic signature, that are stored on the chip. In addition, the certificate for authentication and encryption is also available in LDAP (Lightweight Directory Access Protocol) repository.

The certificates are valid until the date of expiry of the ID card, meaning up to five years depending on the validity of the physical ID card.

2.1. Enrolment

The ID card is a mandatory identity document from the age of 15 which is issued to Estonian and EU citizens living in Estonia.

2.1.1. Application and registration

LOW
1. Ensure the applicant is aware of the terms and conditions related to the use of the electronic identification means.

The issuance of ID card and the obligations of the document holder are regulated by

- eIDAS Regulation [2],
- IDA [3],
- Subscriber Terms and Conditions for Certificates issued by Zetes Estonia OÜ for ID-1 format identity documents of the Republic of Estonia [4],
- Electronic Identification and Trust Services for Electronic Transactions Act [5],
- Certificate Policy for ID-1 format identity documents of the Republic of Estonia (eID CP) [6] and
- Certification Practice Statement for the Intermediate certificates for ID-1 Documents of the Republic of Estonia (eID CPS) [7].

According to article 11^4 of the IDA [3], the initial ID card can be applied for only in person (or via a legal guardian) in a service point of the issuing authority or in the foreign representation of the Republic of Estonia (hereinafter foreign representation). The exception is a minor under the age of 15 whose legal guardian applies for the document and is documented by the issuing authority and whose legal guardian proves their parental relationship.

In cases of expiry, loss, theft or damage of the ID card, Estonian citizens and EU citizens can apply for a recurring ID card in one of the following methods:

- in self-service, available only for Estonian citizens, who have been previously issued an ID card and for those who are legal guardians,
- in a service point of the issuing authority,
- in a foreign representation,
- via post,
- via email.

Terms and conditions for the use of certificates on the ID card are publicly available on the www.id.ee website [8], and a printout can be requested from the issuing authority or the foreign representation. The applicant must explicitly agree to the terms and conditions that are in force at time of application. Important points related to the use of the electronic identification means of the ID card are available on PBGB website [9] as well as on a paper carrier of the ID card.

2. Ensure the applicant is aware of recommended security precautions related to the electronic identification means.

The obligations of a document holder and return of an ID card are stated in article 14 of the IDA [3]. When a document holder forgets their PIN codes, they can use the PUK in the ID software to set new PIN codes. In case the PUK is forgotten, they can use another state accepted digital document to access ID card administration portal and view the PUK code of their ID card. Alternatively, an application can be submitted in the issuing authority service point and the PUK will be sent by post. PUK can be sent to Estonian postal address only. If the PUK is blocked, the document can be used only as a physical identity document, for the use of certificate, a new document must be applied for.

Recommended security precautions related to the electronic identification means are listed on the paper carrier of the ID card, on PBGB's webpage [9], and in the terms and conditions for the use of the certificates mentioned above [8]; for example, not to hand over one's ID card, to keep the PIN codes secret from others, how to act in case document is lost or stolen etc.

3. Collect the relevant identity data required for identity proofing and verification.

Collecting the relevant identity data required for identity-proofing and verification is regulated based on Regulation 20 of the Minister of the Interior, as of 01.08.2025 [10]. Collecting application and relevant identity data required for identity-proofing in the foreign representation is additionally regulated by the Consular Act [11] and regulations of the minister responsible. Collected identity data is checked against the database of the Estonian population register, identity documents database (ITDAK) and automated biometric identification system (ABIS) [12].

The issuer identifies physically the person at least once during the issuance process, taking into account the exceptions described in this document (minors under the age of 15).

For identity-proofing, the applicant provides the following information to the issuing authority:

- a valid identity or travel document (except in cases where the application is done via regular mail, by a legal guardian, electronically, or when applying for an initial document) Estonian citizen's expired document is allowed in service point, when applying for a recurring document, in that case the PBGB official uses other evidence and databases for identity-proofing),
- a photo taken in the issuing authority service point or individually a maximum of 6 months prior to the application date (requirements are set out in Regulation 62 of the Minister of the Interior, adopted on 01.12.2015 [13]),
- fingerprints from the age of 12,
- signature sample (mandatory from the age of 15, voluntary from the age of 7 to the age of 14),
- place of hand-over,
- reason for applying,
- date,
- the minimum data set listed in article 5 of Regulation 20 of the Minister of the Interior, as of 01.08.2025 [10], involves collecting the relevant identity data required to verify the identity of a person beyond doubt at the time of application, including the following:

1) personal data (first name(s), last name(s), Estonian personal identification code or date of birth, place of birth, sex),
2) citizenship,
3) contact information (street, house, apartment, city or village, county, postal code, country, phone, email address),

- other information, when necessary.

SUBSTANTIAL

Same as level low.

HIGH

Same as level low.

2.1.2. Identity proofing and verification (natural person)

LOW

1. The person can 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.

N/A because, in case of the ID card, the identity of the applicant and the validity and authenticity of their document is always verified, not assumed. Please see the description in the following paragraphs for substantial and high.

2. The evidence can be assumed to be genuine, or to exist according to an authoritative source and the evidence appears to be valid.

N/A because, in case of the ID card, the identity of the applicant and the validity and authenticity of their document is always verified, not assumed.

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.

N/A because, in case of the ID card, the identity of the applicant and the validity and authenticity of their document is always verified, not assumed.

SUBSTANTIAL

Level low, plus one of the alternatives listed in points 1 to 4 has to be met:

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.

Estonian eID is always issued as a part of the ID card issuance. The ID card is issued to both Estonian citizens and EU citizens. The ID card issued to Estonian citizens is recognised as a travel document. The ID card issued to EU citizens is valid for person's identification, proof of right of residence and using Estonian e-services but is not recognised as a travel document. Data about every ID card application is recorded in the ITDAK and in ABIS [14] in accordance with IDA [3].

Foreigners who have been issued an Estonian identity document under IDA [3] and all Estonian citizens have a personal identification code and are recorded centrally in the Estonian population register. Personal identification code is used as unique identifier.

When an Estonian citizen applies for an ID card, their data is checked against the population register, the ITDAK and ABIS in accordance with the IDA [3] and regulations issued based on that Act. The ITDAK ascertains whether an Estonian identity document is valid but also provides information about the personal data of the document holder, as well as about the status of the previously issued identity document(s), including information about whether the document(s) has/have been lost, stolen, revoked, or expired. The applicant's biometric data is checked in ABIS.

When an EU citizen applies for an ID card, their right of residence is checked against the Estonian population register and the ITDAK to determine whether there have been any previous encounters with the Republic of Estonia. An EU citizen needs to present a valid identity document issued by the EU Member State of their citizenship when applying for an ID card. The authenticity of the presented identity document is verified in accordance with the sample documents presented by other Member States in the register for authentic documents.

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 documents.

In case of Estonian citizens, the initial identity-proofing is done on the basis of a birth certificate, kinship in the Estonian population register, and in accordance with the Citizenship Act [15]; in case of a recurring ID card, the identification is done based on the previous ID card and the Estonian population register, ITDAK and ABIS; in case of EU citizens, based on a valid identity document of their country of citizenship.

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 [16] of the European Parliament and of the Council [1] or by an equivalent body.

N/A

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 [16] or by an equivalent body.

N/A

HIGH

Requirements of either point 1 or 2 have to be met:

1. Level substantial, plus one of the alternatives listed in points (a) to (c) has to be met:

(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 characteristic of the person with an authoritative source.

When applying for an ID card a valid identity document is checked in accordance with the IDA [3] and regulations issued based on that Act, as well as with the internal procedures and regulations of the issuing authority. The personnel of the issuing authority follow the routine procedure to check that the document is genuine and corresponds to the data and biometric data provided in either national or international registers, whether the document provided is valid and not listed as lost, stolen, revoked, or expired. In case of expired document, it is possible to apply in self-service with another state approved eID means. During application in a service point, a physical identity check is conducted, together with a system checks into national and if needed also in available international databases.

(b) 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 high, 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 [16] or by an equivalent body and steps are taken to demonstrate that the results of the earlier procedures remain valid;

N/A

(c) Where electronic identification means are issued on the basis of a valid notified electronic identification means having the assurance level 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 high must be confirmed by a conformity assessment body referred to in Article 2(13) of Regulation (EC) No 765/2008 [16] or by an equivalent body and steps are taken to demonstrate that the results of this previous issuance procedure of a notified electronic identification means remain valid.

N/A

or

2. Where the applicant does not present any recognised photo or biometric identification evidence, the very same procedures used at the national level in the Member State of the entity responsible for registration to obtain such recognised photo or biometric identification evidence are applied.

In exceptional cases where a valid document issued by the Republic of Estonia is lost or stolen, the person is identified based on the information entered previously into the ITDAK and ABIS.

2.1.3. Identity proofing and verification (legal person)

The ID card is used only for identification of natural persons; therefore 2.1.3. is not applicable.

2.1.4. Binding between the electronic identification means of natural and legal persons

The ID card is used only for identification of natural persons; therefore 2.1.4. is not applicable.

2.2. Electronic identification means management

2.2.1. Electronic identification means characteristics and design

LOW
1. The electronic identification means utilises at least one authentication factor.

Please see the description in the following paragraphs for substantial and high.

2. The electronic identification means is designed so that the issuer takes reasonable steps to check that it is used only under the control or possession of the person to whom it belongs.

Please see the description in the following paragraphs for substantial and high.

SUBSTANTIAL
1. The electronic identification means utilises at least two authentication factors from different categories.

A two-factor authentication is required for using the eID functionality of the ID card: an ID card and PIN codes. The first factor of authentication is being in possession of an ID card. The second factor of authentication are the PIN codes that are issued together with the ID card. The person receives a securely sealed envelope with three codes in it (PIN1, PIN2, PUK): PIN1 for authentication and encryption purposes, PIN2 for a qualified electronic signature (compulsory change before first use), and PUK to reset blocked PIN codes in the ID software.

The document holder possesses a unique private key which is used for authentication. Functions for using this private key are protected with a PIN code, known only by the document holder.

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.

The private key is stored in a secure module of a microchip on the ID card. The ID card with the secure module is a physical device under the document holder's control.

HIGH

Level substantial, plus:

1. The electronic identification means protects against duplication and tampering as well as against attackers with high attack potential

The secure module on the ID card is a QSCD (Qualified Signature Creation Device) certified device.

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.

The document holder has physical control over the authentication device. The document holder has the option to change the PIN codes at any time by using ID software when they know their PIN or PUK code. PIN 2 change is compulsory before first use. Certificate revocation service is available in revocation portal using OTP (One-Time Password) or alternative state approved eID means 24/7, and in service points during their operating hours.

2.2.2. Issuance, delivery and activation

The process of issuance, delivery, and activation is regulated by the IDA [3] and the Consular Act [11].

LOW

After issuance, the electronic identification means is delivered via a mechanism by which it can be assumed to reach only the intended person.

The ID card is issued in person. Additionally, there is a possibility to issue an ID card to a legal guardian or an authorised representative assigned by the applicant at the time of applying for the document. The ID card is issued at the issuing authority service point, at the external service provider's service

point or in the foreign representation indicated in the application form. The choice of the authorised representative to receive the ID card and the place of receiving must be stated in the application. The choice of the authorised representative cannot be changed later in the process. This option can be applied only if the person has provided the application in person at the issuing authority service point or in the foreign representation, in self-service or electronically signed via email.

In case of an authorised representative and legal guardian, the authorised person provides their own identity document.

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 ID card is issued only personally to the applicant, their legal guardian or to an authorised representative (who has been appointed at the application) after identity-proofing. This includes checking the person's document and identity checks into ITDAK and ABIS. The authenticity of the presented identity document is verified with ITDAK or register for authentic documents when necessary. This indicates that the eID means is delivered only into the possession of the person who applied for it and to whom it belongs.

HIGH

The activation process verifies that the electronic identification means was delivered only into the possession of the person to whom it belongs.

The documents are delivered to the service points (PBGB and external service provider's service point and foreign representation) in a secure document bag. The contents of the bags are checked by the authorised personnel and confirm the receipt of the delivery electronically.

ID cards are delivered to the issuing authority service point, external service provider's service point or the foreign representation in a suspended state (meaning that the eID functionality is not active). If an ID card is issued at the issuing authority service point or external service point to the applicant personally, to a legal guardian or to an authorised representative, the ID card is activated by the issuing authority after the identity-proofing of the receiver, who confirms with their handwritten signature that they have received the document in its entirety (the receiver confirms that the ID card was received, the envelope was intact and data correct).

If the ID card is handed over at a foreign representation, the physical ID cards are delivered there by diplomatic mail in an electronically suspended state. Once the foreign representation has proven the identity of the applicant and handed over the document, the necessary actions are carried out via the MFA's information systems, and a request to activate the document is sent to the ITDAK. If the document is handed out by an honorary consul, they inform the relevant foreign representation of the issuance, and the foreign representation performs the required actions.

Once the document is handed over by a external service provider, the necessary actions are carried out in the service provider information system, and a request to activate the document is sent to the ITDAK.

2.2.3 Suspension, revocation and reactivation

After issuance of ID card, the certificates cannot be suspended and reactivated by the certificate owner. Only revocation is allowed.

The legal framework of revocation of the electronic identification means is set by the eIDAS Regulation [2], with its implementing acts, and is regulated at the national level by the IDA [3] and eID CP [6]. 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.

LOW
1. It is possible to suspend and/or revoke an electronic identification means in a timely and effective manner.

Suspension of certificates after activating the certificate is not possible.

The certificates of an ID card can be revoked in the issuing authority service point in person and in the revocation portal. A certificate owner may request revocation of their own certificates or for another person over which they have legal custody. E-services cannot be used/accessed if the certificates are revoked.

At the service point, the certificate owner is identified by the service point official, and the revocation request must be signed by the certificate owner. The service point official verifies the person filing for revocation in accordance with the PBGB identity verification procedures and checks the legality to request revocation.

In the online revocation portal, the certificate owner is authenticated electronically with an alternative state approved eID means or an OTP, and revocation requests are forwarded to the CA via the X-tee secure authenticated channel. The CA authenticates and executes the request automatically and immediately. If the request is accepted, it is executed without delay.

After revocation is completed, the certificate status in the CA interface is set as *revoked* and the certificates cannot be used; therefore, e-services cannot also be used. The physical document remains valid until the expiry of the document. To regain access to e-services after revocation has been completed, a new ID card must be issued (with new certificates); therefore, the enrolment procedure is applied as described in section 2.1.1.

2. The existence of measures taken to prevent unauthorised suspension, revocation and/or reactivation.

Suspension of certificates after activating the certificate is not possible.

Revocation can be performed in the service point of the issuing authority after physical identification or in revocation portal and cannot be reversed.

3. Reactivation shall take place only if the same assurance requirements as established before the suspension or revocation continue to be met.

Since suspension of certificates after activating the certificate is not possible, then reactivation is not applicable. Certificates in the status *revoked* cannot be reactivated. Revocation of the ID card or the certificates can be done only in a service point of the issuing authority or in revocation portal.

SUBSTANTIAL

Same as level low.

HIGH

Same as level low.

2.2.4. Renewal and replacement

LOW

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 is based on a valid electronic identification means of the same, or higher, assurance level.

According to the IDA [3], a person is obliged to notify the issuing authority if the personal identification data (in case of name change or other) has been changed within one month's time and apply for a new ID card as described in section 2.1.1. Therefore, it is the responsibility of the document holder to keep the person's identification data up to date.

For renewal of the ID card in case of expiry, loss, theft or damage, the person must fill in the application, providing personal data (including biometric data), and the enrolment procedure is applied as described in section 2.1.1.

The re-key of certificates is required, for example, in case of security vulnerabilities or cryptographic updates that might have an impact on the security of already issued ID cards or to remain QSCD certified. Certificate re-key can be carried out after the identity-proofing procedure (either physical or electronic authentication), where the data provided is checked against the ITDAK and the Estonian population register.

If an ID card malfunction falls under warranty (for example, ID card cannot be used electronically), then the new ID card and certificates are issued for the same period of validity without a charge to the document holder.

SUBSTANTIAL

Same as level low.

HIGH

Level low, plus: Where renewal or replacement is based on a valid electronic identification means, the identity data is verified with an authoritative source.

Certificate re-key can be performed in the service point of the issuing authority or remotely via ID card administration portal.

Prerequisites for the certificate re-key:

- ID card is whitelisted for the re-key by the issuing authority,
- ID card is valid and electronically functional,
- ID card certificates are valid,
- person knows PIN1 of the ID card.

If PIN1 is not known, the document holder can set new PIN code in the ID software by entering PUK.

The document holder can log in to ID card administration portal via State Authentication Service TARA. Document holder must insert ID card to a smart card reader, agree with the terms and conditions for the use of certificates and initiate the process by inserting PIN1.

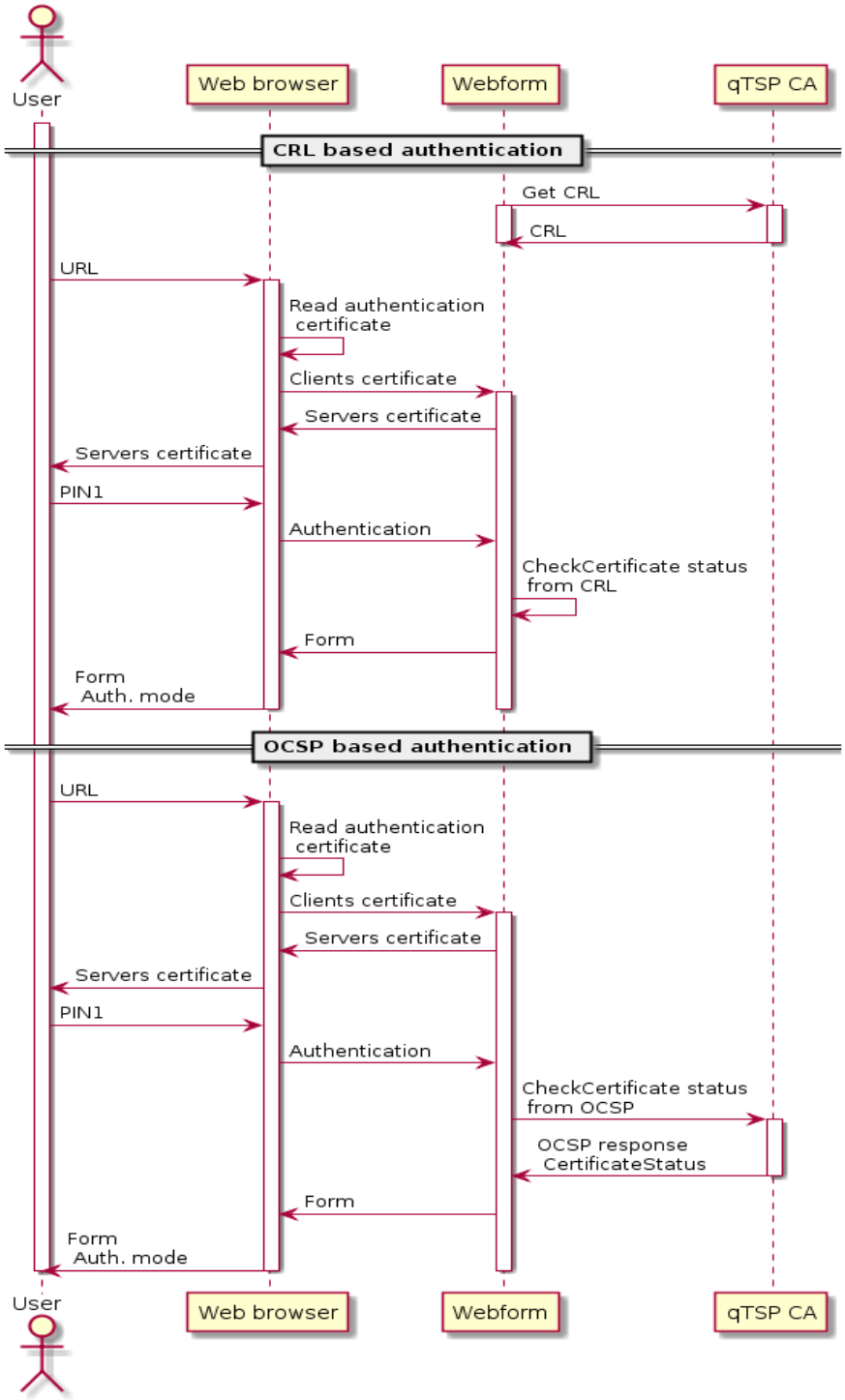
Certificate re-key at a service point of the issuing authority is done after the physical identification procedure, where the data provided is checked against the ITDAK and the Estonian population register. Document holder will sign an application for re-key, insert their ID card to the smart card reader and enter PIN1.

During the process of re-key, the new keys and certificates are generated and will be in active state, previous certificates will be revoked automatically by the CA. Document holder will receive a notification from the issuing authority about the revocation and issuance of new certificates to their official personalidentificationcode@eesti.ee email address.

The warranty application can be submitted in the offices of the issuing authority after the physical identification procedure or in cases of the document holder's request (via helpline and email) where the data provided is checked against the ITDAK. A new ID card is issued in a service point of the issuing authority, external service provider or the foreign representation after the physical identification procedure (authorisation is permitted, when the applicant appoints the representative during application).

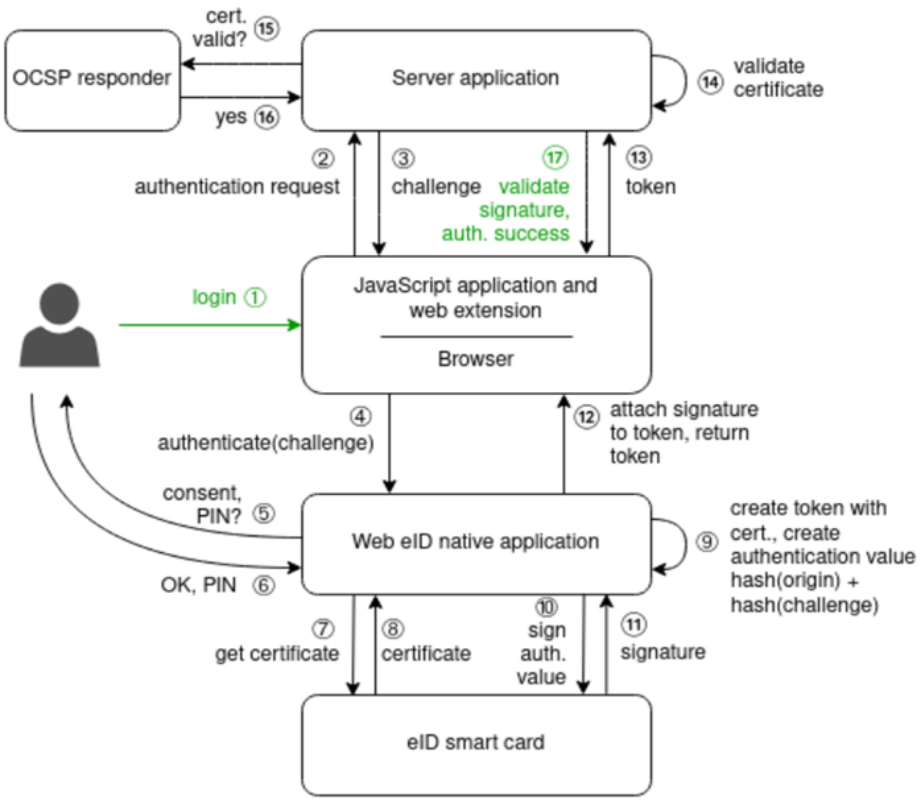
2.3. Authentication

The authentication mechanism of the ID card in case of Transport Layer Security (TLS) Client Certificate Authentication (CCA) is described on the following caption.



Caption 1 Authentication of the Estonian ID card

Since autumn 2022, it has also been possible to use Web eID for authentication. Web eID authentication uses the same mechanism, but it is implemented in the application layer, not in the transport layer like TLS CCA. Web eID authentication is described on the following caption 2.



Caption 2 Web eID authentication diagram

2.3.1. Authentication mechanism

LOW
1. The release of person identification data is preceded by reliable verification of the electronic identification means and its validity.

At the beginning of authentication, the certificate validity can be checked by the OCSP (Online Certificate Status Protocol) service or by using current CRL (Certificate Revocation List). Certificate validity checks are made by the website/-service.

2. 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.

For secure transaction and authentication, the TLS is used. Data on the ID card certificates are considered as public data.

3. 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.

With the correct implementation and usage of PKI technology, where a private key is under the sole control of the document holder, guessing, eavesdropping, replay, or manipulation of communication is not possible.

SUBSTANTIAL

Level low, plus:

1. The release of person identification data is preceded by reliable verification of the electronic identification means and its validity through a dynamic authentication.

On TLS authentication, the person's certificate validity can be checked with the OCSP or with the CRL.

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.

With the correct implementation and usage of PKI technology, where a private key is under the sole control of the document holder, guessing, eavesdropping, replay, or manipulation of communication is not possible.

HIGH

Level substantial, plus: 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.

With the correct implementation and usage of PKI technology, where a private key is under the sole control of the document holder, guessing, eavesdropping, replay, or manipulation of communication is not possible.

2.4. Management and organisation

The Estonian eID scheme is based on nationally issued identity documents. In the Republic of Estonia, the Ministry of the Interior is responsible for identity management policy.

Two types of parties can be distinguished within the Estonian eID scheme: public and private. Both public and private parties must comply with requirements that come from European and national legislation.

Public authorities

Public authorities act in the public interest according to laws and regulations and are subject to special obligations of due diligence.

The Ministry of the Interior

The Ministry of the Interior is tasked with developing the policy of identity management and the policy of issuing the personal identification documents for Estonian citizens and foreigners and coordinating the activities of government authorities.

Estonian Police and Border Guard Board (PBGB)

The PBGB is the issuing authority. This is the institution of executive power within the area of government of the Estonian Ministry of the Interior and, among the main functions, ensures protection of public order, organisation of matters of border management, citizenship, and migration by carrying out national legislation, state supervision, and applying enforcement powers of the state on the basis, the extent, and condition. The functions, rights, and organisation of the police and the legal bases of the police service are provided in the Police and Border Guard Act [17] and the Statutes of the Police and Border Guard Board [18].

According to the IDA [3], the PBGB has the competence of making a decision on issuance and revocation of an identity document. The IDA allows the PBGB to transfer duties for the hand-over of documents to an external service provider. Additionally, the IDA [3] allows the PBGB to transfer the duties for the issuance of certificates. Certificates are generated during the personalisation process by the qualified trust service provider (QTSP), who is managing the whole life cycle of the qualified certificates.

Development, preparation of tenders and contracts, implementation, objectively certain and secure identification and management (including procedures concerning complaints) for identity documents (including the national ID card) are the main responsibilities of the Identity and Status Bureau of PBGB.

Personalisation site of PBGB is responsible for the distribution of all types of identity documents (including the ID card) to the issuing locations.

IT and Development Centre, Ministry of the Interior (SMIT)

SMIT is responsible for ensuring the information and communication technology service development and management within the ministry governing area. The functions, rights, and organisation are provided in the Statutes of SMIT [19].

Information System Authority (RIA)

RIA is a government body responsible for:

- eID technical architecture,
- development of client/end-user software,
- chip technical specification,
- application for eID middleware,
- Estonian Information Security Standard [20],
- collecting, analysing, solving security incidents and informing them to ENISA (CERT, E-ITS [20]),
- creating and ensuring technical solutions/platform for both domestic and cross-border accessing of e-services and
- performing the functions of a point of single contact under eIDAS Regulation [2].

RIA is also the Supervisory Body, who is responsible for supervisory tasks that are set out in eIDAS Regulation [2]:

- 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,
- supervising of notified trust services providers in meeting the established requirements.

The functions, rights, and organisation are provided in the Statutes of the RIA [21].

In the Estonian public sector, all information systems, including the eID scheme must comply with the Estonian Information Security Standard (E-ITS) [20].

The objective of E-ITS is to develop and promote the level of information security in both the Estonian public and private sectors by presenting a basis for information security in Estonia, compliant with the Estonian legal system, which is also aligned with the internationally recognised information security management standard ISO/IEC 27001. The development process of the E-ITS [20] is based on the German BSI IT-Grundschutz baseline security system [22].

The Ministry of Foreign Affairs (MFA)
The MFA is responsible for accepting ID card applications, forwarding collected applications to the PBGB for issuing ID cards, and for handing over ID cards in the foreign representations.

Private parties

Private parties take over tasks as contractors of public authorities or carry out market roles within the Estonian eID scheme that are not executed by public authorities. The exact role and responsibilities of the private parties will be agreed upon in the concluded contracts in accordance with the IDA [3].

Card manufacturer
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.

The card manufacturer 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.

Certification Authority (CA)
The PBGB has a contract with Zetes SA for the provision of certification and qualified trust services.
The duties of the CA 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 OCSP responder service,
- provision of CRL service,
- provision of LDAP directory service,
- provision of test services.

External Service Provider

According to § 3^1 of the IDA [3], at the request of the applicant, the issuing authority may deliver the document through a secure service provider. The secure service provider shall be determined by the issuing authority.

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 issuing authority and foreign representations. Requirements for the external service provider are set out in the contract.

Helpline

ID software user support for electronic use of ID cards and ID software is available workdays 8.30-17.00 by phone +372 666 8888 or email help@ria.ee, additionally www.id.ee is available for user support.

2.4.1. General provisions

LOW
1. Providers delivering any operational service covered by this Regulation are a public authority or a legal entity recognised as such by national law of a Member State, with an established organisation and fully operational in all parts relevant for the provision of the services.

The IDA [3] and the Statutes of the PBGB [18] apply to any operational service covered in the Estonian eID scheme; hence, the requirement is fulfilled.

2. Providers comply with any legal requirements incumbent on them in connection with operation and delivery of the service, including the types of information that may be sought, how identity proofing is conducted, what information may be retained and for how long.

Operations of all entities involved in the Estonian eID scheme are directly governed by national legislation and subordinate regulations. The legislation and enforcement of procedures about identity-proofing are described previously under section 2.1.2.; hence, the requirement is fulfilled.

3. Providers are able to demonstrate their ability to assume the risk of liability for damages, as well as their having sufficient financial resources for continued operations and providing of the services.

According to the Electronic Identification and Trust Services for Electronic Transactions Act [5], the CA shall have a liability insurance contract with the sum insured at least in the amount of one million euros annually per each single insured event and at least one million euros per all events in total.

The CA and card manufacturer shall have a valid performance warranty for the duration of the contract. During the term of the contract, the private party shall hold a non-life insurance contract with an insurer authorised in Estonia, the EU or another Member State of the European Economic Area to which the PBGB is a beneficiary.

PBGB has established fines for external service providers for breach of contract.

4. Providers are responsible for the fulfilment of any of the commitments outsourced to another entity, and compliance with the scheme policy, as if the providers themselves had performed the duties.

Private parties are responsible for the fulfilment of all commitments outsourced to another entity and compliance with the policies as stated (including an obligation to notify about the subcontractors) in the contract with the PBGB.

5. Electronic identification schemes not constituted by national law shall have in place an effective termination plan. Such a plan shall include orderly discontinuations of service or continuation by another provider, the way in which relevant authorities and end users are informed, as well as details on how records are to be protected, retained and destroyed in compliance with the scheme policy.

Estonian eID scheme is constituted by national law; therefore, a termination plan is not applicable. Subcontractors have contractual obligations to the continuation of service throughout the validity period of the issued certificates. As of 01.07.2017, electronic authentication is listed as a vital service in the Emergency Act [23] and is considered as a provider of a service of general interest; therefore, the General Part of the Economic Activities Code Act [24] applies. Termination of CA is stipulated in eID CPS [7].

SUBSTANTIAL

Same as level low.

HIGH

Same as level low.

2.4.2. Published notices and user information

LOW

1. The existence of a published service definition that includes all applicable terms, conditions, and fees, including any limitations of its usage. The service definition shall include a privacy policy.

The service of issuing identity documents ensures the issuance of national identity documents under the conditions and timeframe set out in national legislation (IDA [3] and Regulation 20 of the Minister of the Interior, as of 01.08.2025 [10]), accepting the application for procedures during which the decision to issue, or not to issue, the document is made, and the issuance of the document. Quality control includes “four eyes” principle, where two different officials are involved in the issuance of the document. The IDA also sets the rules for revocation of the document and/or certificates.

Applicable terms and conditions (including any limitations of usage and privacy policy) are defined and explained under section 2.1.1. The fees for ID card are regulated by the Statutory Fees Act [26]. Usage of personal data and privacy is regulated by the GDPR [27], the Personal Data Protection Act [28], which provides the conditions and procedure for processing of personal data, the procedure for the exercise of state supervision and administrative supervision upon processing of personal data, and liability for a violation of the requirements for processing of personal data. The statutes of ITDAK [25] and ABIS statute [14] provide the specifics of what data is collected, the preservation period of collected data etc.

2. Appropriate policy and procedures are to be put in place in order to ensure that users of the service are informed in a timely and reliable fashion of any changes to the service definition and to any applicable terms, conditions, and privacy policy for the specified service.

PBGB is fully responsible for coordinating change management and communication of all aspects of ID card issuance in a timely and reliable fashion, without undue delay. PBGB is responsible for putting appropriate policies and procedures in place, ensuring that users of the service are informed in a timely and reliable fashion of any changes to the service definition, any applicable terms, conditions, and privacy policy.

3. Appropriate policies and procedures are to be put in place that provide for full and correct responses to requests for information.

PBGB’s internal process provides the guidelines for issuance and services related to identity documents after their issuance (e.g. revocation of certificates).
Additionally, the terms and conditions are referred to under section 2.1.1.

SUBSTANTIAL

Same as level low.

HIGH

Same as level low.

2.4.3. Information security management

LOW
There is an effective information security management system for the management and control of information security risks.

Please see the description below under substantial.

SUBSTANTIAL
Level low, plus: The information security management system adheres to proven standards or principles for the management and control of information security risks.

E-ITS [20] is compulsory for all state and local government organisations who handle databases/registers. Therefore, all internal procedures for development and maintenance are created and managed based on E-ITS security levels and classes. E-ITS [20} is a tool for risk and security management; hence, the requirement is fulfilled. State supervision for E-ITS [20] compliance is conducted by RIA.

Private parties adhere to and provide certificates of audits (eIDAS and ISO) which demonstrate following proven standards and principles for the management and control of information security risks, as previously stated under 2.4.

HIGH

Same as level substantial.

2.4.4. Record keeping

Collecting data and records, maintenance, archiving, and protection of all relevant records and data is required and regulated by European (eIDAS Regulation [2], GDPR [27]) and national legislation, subordinate regulations, and internal procedures.

LOW
1. Record and maintain relevant information using an effective record-management system, taking into account applicable legislation and good practice in relation to data protection and data retention.

The Public Information Act [29] provides the conditions of, procedure for, and methods of access to and reuse of public information and the bases for refusal to grant access to information, restricted public information, and the procedure for granting access thereto to the extent not regulated by other acts, the bases for establishment and administration of databases, and supervision over the administration of databases, the procedure for the exercise of state supervision, and administrative supervision over the organisation of access to information.

The Personal Data Protection Act [28] provides for the conditions and procedure for the processing of personal data, the procedure for the exercise of state supervision and administrative supervision upon the processing of personal data, and liability for a violation of the requirements for the processing of personal data.

The Statutes of ITDAK [25] and ABIS [14] provide that for ensuring availability, integrity, and confidentiality of data protection in databases, the organisational, physical, and information technology security measures must be implemented. Article 18 of ITDAK Statutes provides that data records are kept 75 years, except for initial documents, which are kept permanently. The ITDAK has a service-level agreement between the PBGB and the ICT service provider (SMIT), in which are stated quality parameters, data confidentiality, integrity, availability, and highest data loss tolerance.

The Statutes of ABIS [12] provides that data records are kept actively for 15 years, after that for 60 years.

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.

Please see description in 2.4.4/1.

SUBSTANTIAL

Same as level low.

HIGH

Same as level low.

2.4.5. Facilities and staff

Estonian eID is managed by an Estonian government body (PBGB); therefore, all human resource decisions are laid down in official administrative procedures according to the national legislation; in particular, based on the Civil Service Act [30] and Police and Border Guard Board Act [17].

Additionally, E-ITS [20] facilitates requirements for both facilities and staff.

The manufacturing site of the card manufacturer is certified throughout the contract period according to the following standards:

- Intergraf's ISO 14298 – level Governmental,
- ISO 9001 Quality Management System – requirements,
- ISO/IEC 27001 Information technology – Security techniques – Information security management systems – Requirements,
- PCI CPP Physical Security Requirements and Test Procedures for the transportation of documents from the manufacturing site to the personalisation site via secure transportation.

The personalisation site and processes of the card manufacturer are compliant with the following regulations and standards:

- 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 (always referred together as eIDAS regulation),
- ISO 9001 Quality Management System – requirements,
- ISO/IEC 27001 Information technology – Security techniques - Information security management systems – Requirements,
- PCI CPP - Logical Security Requirements and Test Procedures,
- PCI CPP - Physical Security Requirements and Test Procedures,
- ISO 9001 Quality Management System – requirements,
- ISO/IEC 27001 Information technology – Security techniques – Information security management systems – Requirements,
- PCI CPP - Logical Security Requirements and Test Procedures,
- PCI CPP - Physical Security Requirements and Test Procedures,
- PCI Data Security Standard.

The card manufacturer ensures compliance with all relevant EU, Estonian and international legal acts, standards and recommendations as well as the relevant electronic identification and CA rules at all times throughout the contract and in case any amendments or updates are introduced, card manufacturer shall ensure compliance with all amended and updated requirements without any delay.

LOW
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.

In public authorities, staff are employed and trained according to dedicated job profiles (general framework and qualification requirements) and job descriptions (detailed work characteristics and responsibilities). Both originate from state development plans, work plans, cooperation agreements, and the needs specified by the service owner of PBGB. Where relevant, additional dedicated training programmes for staff members also exist (e.g., identity-proofing and fraud). This ensures that procedures are performed by trained, qualified, and experienced staff. Background checks are implemented during recruitment and employment as a routine precautionary measure in accordance with Police and Border Guard Act [17]. Duties are performed according to formalised processes, and special obligations of due diligence exist. Job profiles, training programmes, procedures, and processes are monitored and updated on a regular basis as part of the state public service.

Implementing E-ITS [20] or ISO 27001 [31] requirements facilitate 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.

The requirements for private parties come from the eIDAS Regulation [2], the Electronic Identification and Trust Services for Electronic Transactions Act [5], and the contract. All specific standards and requirements set out in the previously mentioned under contractors are applicable to the

subcontractor(s) depending on their role. The CPs for the ID-1 format identity documents are publicly available electronically on CA webpage [6] and www.id.ee webpage [8], CPSs are available on CA webpage [6].

2. The existence of sufficient staff and subcontractors to adequately operate and resource the service according to its policies and procedures.

Public authorities have been provided with resources and staff according to the administrative effort of the corresponding services as part of legislative procedures, which are reassessed on a yearly basis as part of yearly estimations and analysis. Additionally, implementing E-ITS [20] or ISO [31] requirements facilitate the existence of sufficient staff and subcontractors to adequately operate and resource the service according to its policies and procedures.

The requirements for private parties come from the eIDAS Regulation [2], the Electronic Identification and Trust Services for Electronic Transactions Act [5], and the contract. The CPs for the ID-1 format identity documents are publicly available electronically on CA webpage [6] and www.id.ee webpage [8], CPSs are available on CA webpage [8].

3. Facilities used for providing the service are continuously monitored for, and protect against, damage caused by environmental events, unauthorised access and other factors that may impact the security of the service.

Implementing E-ITS [20] or ISO [31] requirements facilitate continuous monitoring for, and protection against, damage caused by environmental events, unauthorised access, and other factors that may impact the security of the service of facilities used for providing services.

The requirements for private parties come from the eIDAS Regulation [2], the Electronic Identification and Trust Services for Electronic Transactions Act [5], and the contracts. The private parties have an insurance policy to provide the security of the service.

The bases of continuity of vital services are regulated in the Emergency Act [23].

Physical security requirements for manufacturing and personalisation process and physical security requirements for the personalisation site come from the PCI standards (as described in 2.4.5). The physical and information systems security of the MFA is regulated with different internal organisational documents.

4. Facilities used for providing the service ensure that access to areas holding or processing personal, cryptographic or other sensitive information is limited to authorised staff or subcontractors.

Implementing E-ITS [20] requirements ensure that access to areas holding or processing personal, cryptographic, or other sensitive information is limited to authorised staff or subcontractors.
The archival rules referred to in 2.4.4 regulate and specify the requirements for assessment and safekeeping of the records at public institutions or persons until their handover to the public archive

and the rules of handover, preservation, protection in the public archive, access management, including issuance of the archival notice of the archive records.

Additionally, why and how data is gathered, kept, and handled and who has access to the data are defined in the statutes of a particular database. This includes information system access control, which is monitored in terms of who has which access rights, for how long, and given by whom. This ensures that access rights are backwards traceable, should there be a need to identify who, when, why, and where has granted access.

The requirements for private parties come from the eIDAS Regulation [2], the Electronic Identification and Trust Services for Electronic Transactions Act [5], and the contracts; also, from the eID CP [6]. The private party for manufacturing and personalisation of the ID cards operate under the PCI standards that cover the physical security part and personnel requirements.

SUBSTANTIAL

Same as level low.

HIGH

Same as level low.

2.4.6. Technical controls

LOW

The service system is hosted by a qualified trust service provider, published in the national trusted list: https://sr.riik.ee/en/trusted-list/ and in the EU trusted list: https://eidas.ec.europa.eu/efda/trust-services/browse/eidas/tls.

eID CPS, eID CP, terms and conditions are available at https://repository.eidpki.ee/repository/. Conformity assessments reports are provided upon request and under nondisclosure agreement.

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.

Requirements for the existence of proportionate technical controls to manage the risks posed to the security of services, protecting the confidentiality, integrity, and availability of the information processed for contractors, come from European and national legislation, and the contracts. Data between the PBGB, the card manufacturer, and CA transfers through secure PBGB exchange interface HUB.

The data exchange takes place as a transmission of messages over the X-tee data exchange layer, ensuring secure, standardised, and auditable message-based communication. Generic information on X-tee can be found at https://www.ria.ee/en/state-information-system/x-tee.html.

As part of the Estonian eID scheme, a new intermediary service called HUB has been introduced to support and standardise data exchange related to the issuance of ID-1 format identity documents. HUB is a gateway-type service that mediates communication between the parties involved in the ID card issuance process - the issuing authorities, the document manufacturer, and the QTSP. All data exchange through HUB takes place over the X-tee data exchange layer, ensuring secure, auditable, and standardised communication.

The primary role of HUB is to manage and mediate:

- requests for personalisation orders of ID-1 format identity documents sent from issuing authorities to the manufacturer,
- notifications of personalisation order and delivery package status changes back to the corresponding issuing authority systems, and
- requests for certificate generation, activation, revocation, and related status queries sent to the QTSP.

HUB enables the transmission of trust service responses both to the issuing authorities' systems and to the card manufacturer(s). By acting as a single intermediary, HUB reduces direct system-to-system integrations and ensures consistent handling of processes and data.
The introduction of HUB aims to:

- standardise communication between all parties involved in document issuance,
- provide auditable and traceable data exchange,
- increase resilience and efficiency by supporting the parallel or alternative use of different QTSPs when requesting certificates.

2. Electronic communication channels used to exchange personal or sensitive information are protected against eavesdropping, manipulation and replay.

Requirements for the existence of proportionate technical controls to manage the risks posed to the security of services, protecting the confidentiality, integrity, and availability of the information processed for private parties, come from European and national legislation, and the contracts. Data between the PBGB, the card manufacturer, and CA transfers through secure PBGB exchange interface HUB.

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.

Requirements for access restrictions for private parties come from the eIDAS Regulation [2], the Electronic Identification and Trust Services for Electronic Transactions Act [5], and the contracts.

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.

Security and risk management:

a) Middleware software (including card drivers) is maintained by the state and is frequently updated.
b) In case of security vulnerabilities or cryptographic updates that might have an impact on the security of already issued ID cards or to remain QSCD certified, the re-key of the certificates shall be possible via ID card administration portal.
c) To prevent the potential digital misuse, the certificates can be revoked using revocation portal which is accessible 24/7 to all ID card holders.

Requirements for private parties come from the eIDAS Regulation [2], the Electronic Identification and Trust Services for Electronic Transactions Act [5], and the contracts. IDA [3] allows the issuing authority to revoke the certificates, when necessary.

5. All media containing personal, cryptographic or other sensitive information are stored, transported and disposed of in a safe and secure manner.

Requirements for private parties come from the eIDAS Regulation [2], the Electronic Identification and Trust Services for Electronic Transactions Act [5] and other applicable national legislative Acts, and the contracts.

SUBSTANTIAL

Same as level low, plus:
Sensitive cryptographic material, if used for issuing electronic identification means and authentication is protected from tampering

Requirements for private parties come from the eIDAS Regulation [2], and other applicable national legislative acts, and the contracts.

HIGH

Same as level substantial.

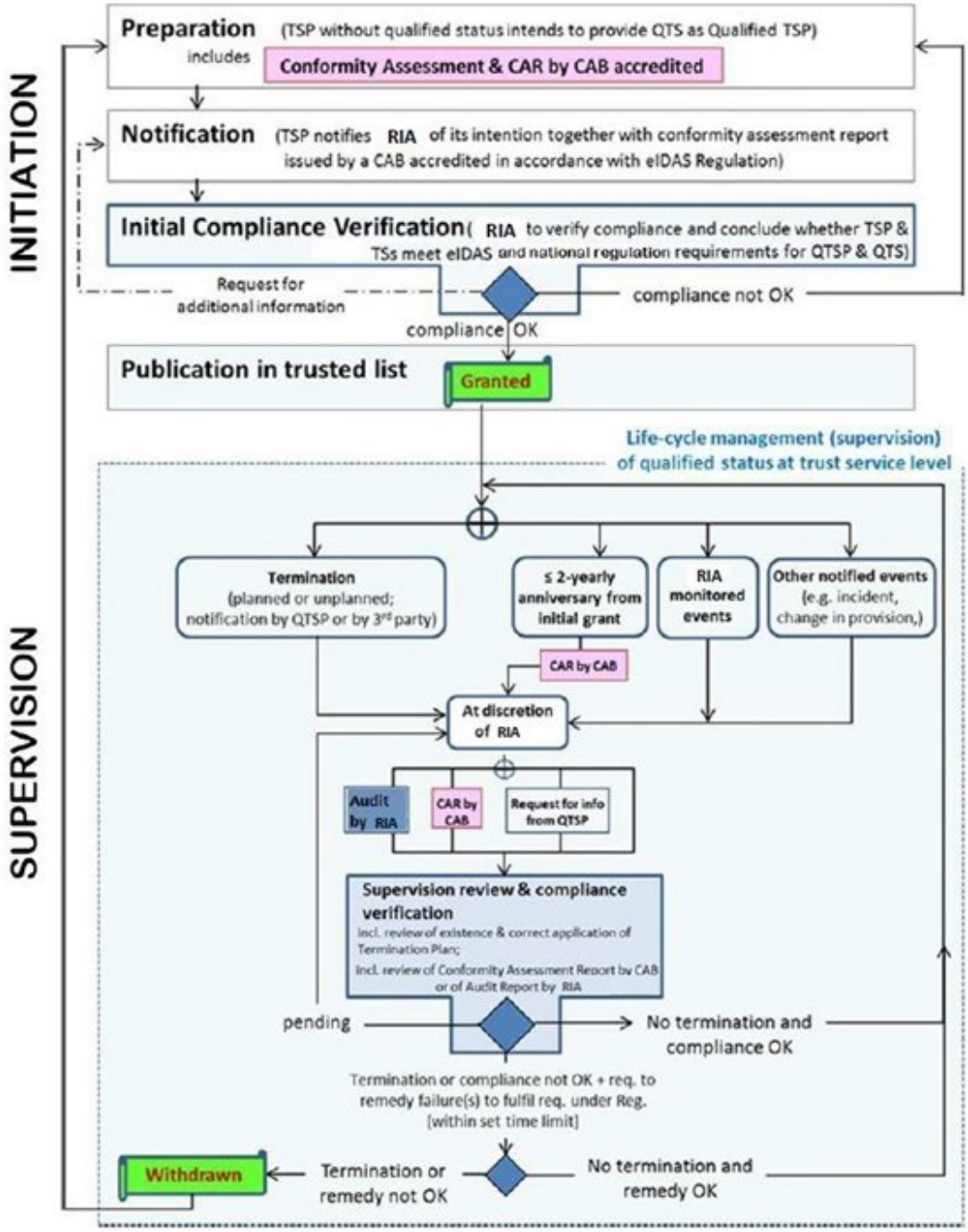
2.4.7. Compliance and audit

CA is subject to the eIDAS Regulation [2], with its implementing acts, and, at the national level, is regulated by the Electronic Identification and Trust Services for Electronic Transactions Act [5].

CA has been audited by the certification body LSTI-Apave SAS (Conformity Assessment Body is accredited for the certification of trust services according to ISO/IEC27001 and ETSI EN 319 403 [32]) and confirmed as a QTSP according to article 3 (20) of eIDAS by RIA. The initiation and supervisory activities of the CA and its qualified trust service provided, and lifecycle management of the related qualified status are carried out according to the figure below. The CA activities are under regular supervision throughout the lifecycle of such services, from their commencement to their termination. The CA has an obligation to communicate with RIA regarding any changes in the provision of its qualified trust services, data set out in a notification according to paragraph 1 of article 21 of eIDAS [2}, and any incidents concerning a breach of security or loss of integrity. The qualified trust services provided by CA are in accordance with the requirements laid down in eIDAS [2], the ETSI European

Standard (ETSI EN), and national regulations. Information related to the CA and provided services have been entered into the national trusted list by the validity of the relevant conformity assessment report, in general, for 2 years. Detailed information regarding the CA, provided services, certificates, certification practice statements, policies, and conformity assessment reports are available at the website https://repository.eidpki.ee/repository/.

Activities for QTSP/QTS initiation and lifecycle management of the related qualified status of trust service level is described on the following caption 3.



Caption 3 Activities for QTSP/QTS initiation and lifecycle management of the related qualified status of trust service level

LOW

The existence of periodical internal audits scoped to include all parts relevant to the supply of the provided services to ensure compliance with relevant policy.

Please see the detailed description in the following section high.

SUBSTANTIAL

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.

Please see the detailed description in the following section high.

HIGH

1. The existence of periodical independent external audits scoped to include all parts relevant to the supply of the provided services to ensure compliance with relevant policy.

The contractors of the PBGB and their subcontractors in connection with the issuance of documents (including the ID card) must be audited accordingly and/or comply with requirements of standard(s) (ETSI, PCI and/or ISO) until the expiry of the contracts or until the expiry of the last certificate pair issued and/or renewed according to the specifics of particular standard or audit. The CA is audited every year by a conformity assessment body, and RIA, as the Supervisory Body, confirms that the CA fulfils the requirements laid down in eIDAS [2] and national laws for a QTSP. CA is audited at least every 2 years to confirm that the CA and the qualified trust services provided by them fulfil the requirements laid down in eIDAS [2] and national law. E-ITS [20] preliminary audit was conducted in March 2025, main audit begun in the beginning of September 2025.

2. Where a scheme is directly managed by a government body, it is audited in accordance with the national law.

Estonian eID scheme is subject to national law, therefore, it is under supervisory control of the state. 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. Supervisory control of Estonian governmental authorities and agencies is regulated by chapter 7 of the Government of the Republic Act [33]; hence, this requirement is fulfilled.

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

The PBGB has an internal audit bureau which provides independent, objective, and consulting activities to create value and fulfilling organisational activities. Internal audits help to fulfil the organisational objectives by using a systematic approach for evaluating and improving risk management, control, and efficiency in organisation management culture processes. The activities of the Internal Audit Bureau are based on the international standards of the Institute of Internal Auditors (external conformity

assessment conducted in 2025). The work of the Internal Audit Bureau is regulated by the PBGB internal regulation. Risk management in the PBGB is regulated by the PBGB risk management framework.

List of References

[1]	Commission Implementing Regulation (EU) 2015/1502 of 8 September 2015 on Published: https://eur-lex.europa.eu/eli/reg_impl/2015/1502/oj/eng
[2]	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 (always referred together as eIDAS regulation) Reference: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02015R1502-20220711
[3]	Identity Documents Act https://www.riigiteataja.ee/en/eli/ee/505012026002/consolide/current
[4]	Subscriber Terms and Conditions for Certificates issued by Zetes Estonia OÜ for ID-1 format identity documents of the Republic of Estonia Published: https://repository.eidpki.ee/repository/
[5]	Electronic Identification and Trust Services for Electronic Transactions Act (in English) Published: https://www.riigiteataja.ee/en/eli/ee/529122024007/consolide/current
[6]	Certificate Policy for ID-1 format identity documents of the Republic of Estonia" (eID CP) Published: https://www.id.ee
[7]	Zetes Estonia OÜ - Certification Practice Statement for the Intermediate CA for ID-1 documents of the Republic of Estonia (eID CPS) Published: https://repository.eidpki.ee/repository/
[8]	www.id.ee webpage https://www.id.ee/ , in English: https://www.id.ee/en/
[9]	Important points to remember for document users https://www.politsei.ee/en/important-points-to-remember-for-document-users
[10]	Regulation No 20 of the Minister of the Interior, as of 01.08.2025 (only in Estonian) Published: https://www.riigiteataja.ee/akt/129072025001
[11]	Consular Act Published: https://www.riigiteataja.ee/en/eli/ee/516122025001/consolide/current
[12]	ABIS Database information Published: https://www.siseministeerium.ee/en/abis
[13]	Regulation No. 62 of the Minister of the Interior "Requirements for a photograph when applying for an identity document" (only in Estonian) Published: https://www.riigiteataja.ee/akt/108122015004?leiaKehtiv
[14]	ABIS Database Statute (only in Estonian) Published: https://www.riigiteataja.ee/akt/103102023017?leiaKehtiv
[15]	Citizenship Act Published: https://www.riigiteataja.ee/en/eli/528072025002/consolide
[16]	Regulation (EC) No 765/2008 of the European Parliament and of the Council of 9 July 2008 setting out the requirements for accreditation and repealing Regulation (EEC) No 339/93. Published: http://data.europa.eu/eli/reg/2008/765/2021-07-16
[17]	Police and Border Guard Act Published: https://www.riigiteataja.ee/en/eli/ee/527102025003/consolide/current
[18]	Police and Border Guard Statute (only in Estonian) Published: https://www.riigiteataja.ee/akt/128062025002?leiaKehtiv
[19]	SMIT Statute (only in Estonian) Published: https://www.riigiteataja.ee/akt/109072024006?leiaKehtiv

[20]	Estonian Information Security Standard (E-ITS, website in Estonian, some documents also in English) Published: https://eits.ria.ee
[21]	RIA Statute (only in Estonian) Published: https://www.riigiteataja.ee/akt/127122024010?leiaKehtiv
[22]	German BSI IT-Grundschutz baseline security system https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/it-grundschutz_node
[23]	Emergency Act Published: https://www.riigiteataja.ee/en/eli/ee/527102025001/consolide/current
[24]	General Part of the Economic Activities Code Act Published: https://www.riigiteataja.ee/en/eli/ee/511092025011/consolide/current
[25]	ITDAK Database Statute (only in Estonian) Published: https://www.riigiteataja.ee/akt/102072025011?leiaKehtiv
[26]	Statutory Fees Act Published: https://www.riigiteataja.ee/en/eli/ee/525112025005/consolide/current
[27]	Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 Published: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679&qid=1765634765358
[28]	Personal Data Protection Act Published: https://www.riigiteataja.ee/en/eli/522092025009/consolide
[29]	Public Information Act (in English) Published: https://www.riigiteataja.ee/en/eli/ee/514112013001/consolide/current
[30]	Civil Service Act (in English) Published: https://www.riigiteataja.ee/en/eli/ee/502012018003/consolide/current
[31]	ISO standards Published: https://www.iso.org/standards.html
[32]	ETSI EN 319 403 https://www.etsi.org/deliver/etsi_en/319400_319499/31940301/02.03.01_60/en_31940301v020301p.pdf
[33]	Government of the Republic Act Published https://www.riigiteataja.ee/en/eli/ee/504092025010/consolide/current