REPUBLIC OF ESTONIA
POLICE AND BORDER GUARD BOARD

LoA Mapping of the Estonian diplomatic identity 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 Certificate Authority which issued the certificate.
diplomatic card	An identity card which is issued to a foreign national who is a diplomat accredited to Estonia and his or her family member, who is a foreign national. Categories A and B.
diplomatic identity card	There are two types of diplomatic identity cards: diplomatic card and service card.
diplomatic note	Formal, written communication between states, typically sent by an embassy to a host country's Foreign Ministry or vice versa for official business.
Diplomatic Portal	Secure online platform (website) managed by MFA to share information, procedures and communication for accredited foreign missions and other institutions. Handling accreditations, immunities, notifications and protocol guidelines.
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 mission	Diplomatic representation and consular post of a foreign state, mission of an international organisation and an international organisation or other institution accredited to Estonia.
foreign national	A person, who is not Estonian citizen.
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.

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 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 identity card, e-resident's digital ID, residence permit card and diplomatic identity card.
information security management system	A set of processes and procedures designed to manage, to acceptable levels, risks related to information security.
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.
revocation portal	Portal for revocation of certificates, available at https://revocation-portal.eidpki.ee/en/landing.
service card	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 or an international organisation or other institution established by an international agreement located in Estonia 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. Categories C, D, E, F, G, HC.
travel document	An official identity document (national passport, diplomatic passport, service or official passport, national ID card) that proves a person's identity and allows them to cross international borders and enter other countries.
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
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, suspended) 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
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
TS	Trust Service
VEIS	Database of foreign missions and representations of international organizations, international organizations and institutions established by international agreements, and their personnel

1. Introduction

The present document explain how the diplomatic identity card (*hereafter where necessary a/the 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).
There are two types of Estonian diplomatic identity cards: diplomatic card and service card (hereinafter used together as "the card").

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 the eIDAS Regulation [2} 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 post-issuance 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 optimizer: 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 card, meaning up to five years depending on the validity of the physical card.

2.1. Enrolment

The card grants the immunities and privileges outlined in the Vienna Convention on Diplomatic Relations [3] and other international conventions and treaties according to the relevant category.

Diplomatic and service cards are also the legal basis for residence in Estonia for the employees of a foreign mission and their family members and entitle the bearer, together with a passport, to enter and travel within the territory of the Schengen Area.

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 obligations of the document holder are regulated by

- eIDAS Regulation [2],
- Identity Documents Act (IDA) [4],
- Electronic Identification and Trust Services for Electronic Transactions Act [5],
- Subscriber Terms and Conditions for Certificates issued by Zetes Estonia OÜ for ID-1 format identity documents of the Republic of Estonia [6],
- Certificate Policy for ID-1 format identity documents of the Republic of Estonia (eID CP) [7],
- Certification Practice Statement for the Intermediate certificate for ID-1 Documents of the Republic of Estonia (eID CPS) [8] and
- Regulation 7 of the Minister of the Foreign Affairs [9].

The card can be applied for only through diplomatic note or official letter. A card is issued in person at the MFA's service point, except for the minor under the age of 15 or an adult with limited legal capacity, in these cases the card will be issued to his/her legal representative. For a person aged between 15 and 17 years the card may be collected by his/her legal representative. The applicant can complete the application form online by submitting required personal data and uploading applicant's photo via Diplomatic Portal [10]. The pre-filled notification must be printed, signed by the applicant and the head of mission, affixed with the foreign mission's seal, and submitted together with the necessary supporting documents to the issuing authority with a diplomatic note or official letter.

When applying for the card the applicant must agree to the terms and conditions of using certificates by signing the application form. The basic terms and conditions related to the use of the electronic identification means of the Estonian diplomatic identity card are listed on the paper carrier with a card and are introduced by the issuing authority during the issuance process. The paper carrier consists of two parts: firstly, the terms and conditions; secondly, the acknowledgement part. The recipient signs the

paper carrier physically, acknowledging and accepting the terms and conditions, after which the acknowledgement part is separated by an official. The signed acknowledgement on paper is archived by the issuing authority together with an application form. The recipient receives the part of the terms and conditions on paper. Furthermore, a detailed version of the terms and conditions for the use of certificates of personal identification documents is publicly available on the online notification form and on the id.ee website [11].

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

Returning a card is detailed in section 9 of the Regulation 7 of the Minister of the Foreign Affairs [9] Additionally, recommended security precautions related to the electronic identification means, the reminder of safe usage of a card, and the terms and conditions for the use of certificates are listed, as mentioned above, in section 1; for example, not to hand over one's card, to keep the codes of a card secret from others, to ensure the card is used only under the control of the document holder, to promptly inform the issuing authority in order to revoke the certificates in case of lost, stolen, or forgotten or blocked PIN codes.

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 by section 3 of the Regulation 7 of the Minister of the Foreign Affairs [9]. Collected identity data is checked against the database of Estonian population register.

The official of the issuing authority identifies physically the person at least once during the issuance process, taking into account the exceptions described in this document.

For identity-proofing, the staff of a foreign mission provides the following information to the issuing authority:

- a diplomatic note or official letter,
- a copy of a valid travel document,
- a photo taken 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 [12]),
- the Minimum Data Set listed in section 3 of the Regulation 7 of the Minister of Foreign Affairs, as of 09.03.2017 [9], to collect the relevant identity data required to verify the identity of a person beyond doubt at the time of application, including the following:
    1) the name of the foreign mission or other institution submitting the application,
    2) personal data (first name(s), last name(s), date of birth, gender, country of birth, citizenship),
    3) contact information (address, telephone number, and email address),
    4) the signature of the Head of Mission,
    5) the date of submission,
    6) the seal of the foreign mission submitting the application,
    7) the document holder's signature to confirm that he or she has examined and approve the

conditions of use of the certificates.

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 card, the identity of the applicant and the validity and authenticity of their document is always verified. 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 Estonian diplomatic identity card, the identity of the applicant and the validity and authenticity of their document is always verified. Please see the description in the following paragraphs for substantial and high.

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 Estonian diplomatic identity card, the identity of the applicant and the validity and authenticity of their document is always verified. Please see the description in the following paragraphs for substantial and high.

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 means is always issued as a part of the diplomatic identity card issuance, referred to in this document as the card.

The card is for using Estonian provided e-services. It grants the immunities and privileges outlined in the Vienna Convention on Diplomatic Relations [3] and other international conventions and treaties according to the relevant category. It is also the legal basis for residence in Estonia for the employees of a foreign mission and other institution and their family members and entitles the bearer, together with a travel document, to enter and travel within the territory of the Schengen states.

The data about every card application is recorded in the statutes of the database of foreign missions and representations of international organisations, international organisations and institutions established by international agreements, and their personnel (*hereafter database of VEIS*) [13]. All foreigners who have been issued the card have a personal identification code and are recorded centrally in the Estonian population register. Personal identification code is used as unique identifier.

When applying for a card, applicant's data in the notification form is checked by the official of issuing authority for previous data against the population register and the database of VEIS [13] in accordance with the IDA [4] and the Foreign Relations Act [14] and regulations issued on the basis of these acts.

The database of VEIS [13] provides information about the personal data of the document holder (including a facial image and signature sample), as well as about the status of the previously issued identity document, including information about whether the document has been lost, stolen, revoked, expired, destroyed and whether the card has been physically returned to the issuing authority. Applicant needs to present a copy of the valid travel document issued by the country of their citizenship when applying for the card.

A notification for a card needs to be accompanied by a diplomatic note or official letter of the foreign mission or other institution submitting the application, including the signature of the Head of foreign mission and the seal of mission.

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.

N/A

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 [15] of the European Parliament and of the Council 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 [15] 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.

A copy of a valid identity document including biometric data is checked in accordance with the IDA [4] and regulations issued on the basis of that act, as well as with the internal procedures and regulations of the issuing authority.

(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 [15] 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 [15] 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.

N/A

2.1.3. Identity proofing and verification (legal person)

The 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 card is used only for the 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.

Two-factor authentication is required when using the Estonian eID. The two factors are the chip of the card and the PIN codes. The first factor of authentication is possession of the card. The second factor is the set of PIN codes issued together with the 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 smart card. The smart card with the secure module is a physical device under the document holder's control.

The eID means are part of the card, issued as defined under section 2.1.1.

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 smart card is a QSCD (Qualified Electronic 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 (available at: https://revocation-portal.eidpki.ee/en/landing) using OTP (one-time password) or alternative state approved eID means 24/7, and in service point during operating hours.

2.2.2. Issuance, delivery and activation

The process of issuance, delivery, and activation is regulated by the IDA [4], and of the Regulation 7 of the Minister of the Foreign Affairs [9].

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 card is issued in person. If the applicant has previously been issued a card, the applicant must return it upon the receipt of a new card.

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 fact that the card is issued only personally to the applicant after identity-proofing indicates that the electronic identification 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 MFA's service point in a secure document bag. The contents of the bags are checked by the authorised personnel and confirm the receipt of the delivery electronically.

The cards are delivered to the issuing authority in an electronically suspended form (meaning that the eID functionality is not active). A card is handed over to the applicant personally and the card is activated by the issuing authority after identity-proofing of the receiver. The recipient signs the paper form physically, acknowledging and accepting the terms and conditions, after which an official of the issuing authority activates the electronic identification means in the system.

2.2.3. Suspension, revocation and reactivation

After issuance of the 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 [4] and eID CP [7]. The document holder is obliged to notify the MFA in case of theft or loss of the card, so revocation can be implemented.

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.

Upon termination or suspension of the card user's service relationship with the foreign mission, the card shall be declared invalid by the issuing authority no later than one month after the relevant diplomatic note or notification letter from the mission has been received by the MFA [9].

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

The certificates of the card can be revoked in the issuing authority service point in person and in the revocation portal. E-services cannot be used/accessed if the certificates are revoked.

For revocation of certificates an officer identifies the person according to the issuing authority's internal processes. The physical document remains valid until the expiry of the document.

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 be used either. The physical document remains valid until the expiry of the document. To regain access to e-services after revocation has been completed, a new card must be issued (with new certificates); therefore, the enrolment procedure is applied as described in section 2.1.1 above.

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 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 [4], a person is obliged to notify the issuing authority if the personal identification data (in case of a name or other change) has been changed within one month's time and apply for a new card. Therefore, it is the responsibility of the card holder to keep the person's identification data up to date. For renewal of the card, the applicant must fill in the application and foreign mission must provide a diplomatic note or official letter, providing personal data (including a photo), which is checked against existing information, provided previously.

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 cards or to remain QSCD certified. Certificate renewal can be carried out after the identity-proofing procedure (either physical or electronic authentication), where the data provided is checked against the database of VEIS [13] and the Estonian population register.

If a card malfunction falls under warranty or guarantee, then the new card is replaced, and new certificates are issued for the same period of validity.
The card warranty cases include:

- usage of electronic functionality being problematic,
- the card reader not recognising the card chip,
- the issuing authority revoking the certificates before the end of the certificate validity period.

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:

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

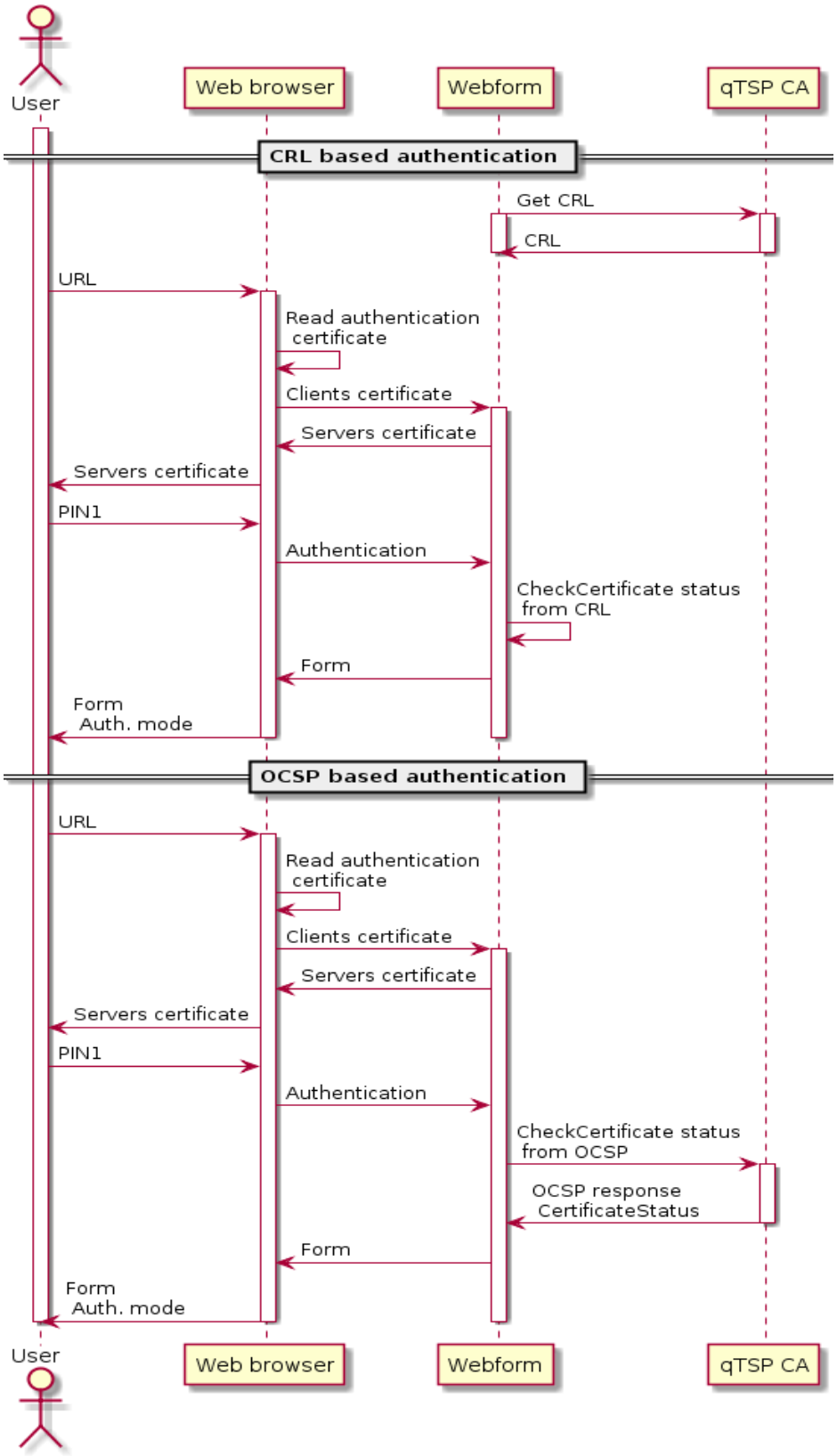
During the process of re-key, the new keys and certificates are generated and will be in active state, previous certificates will be revoked automatically by the CA. Document holder will receive a notification

from the issuing authority about the revocation and issuance of new certificates to their official personalidentificationcode@eesti.ee email address.

A request for renewal or replacement of a card can be submitted through a diplomatic note or official letter. A new card is issued in a service point of the issuing authority after the physical identification procedure (authorisation is not permitted).

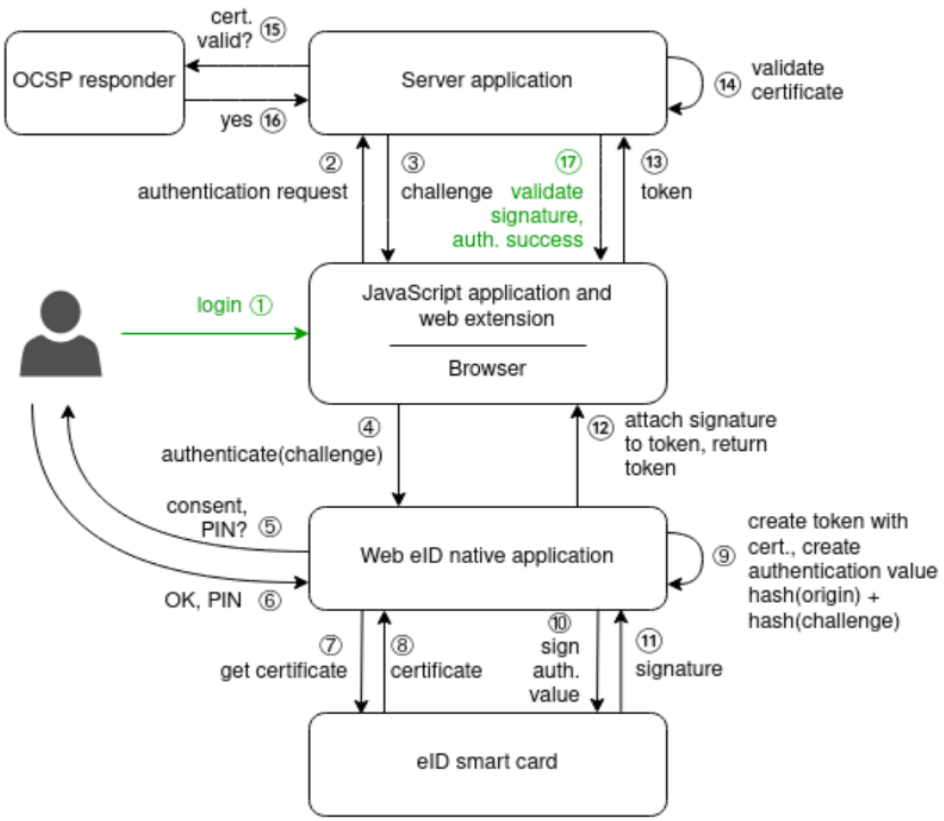
2.3. Authentication

The authentication mechanism of the Estonian diplomatic identity card is described on the following caption.



Caption 1 Authentication of the Estonian diplomatic and service 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.



Caption 2 Web eID identification 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 with the help of 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 Transport Layer Security (TLS) is used. Data on the Estonian eID 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 official documents. The MFA is responsible for identity management and for issuing diplomatic identity card. Therefore, all requirements are defined under national legislation, subordinate guidelines, orders, and procedures.

Two types of parties can be distinguished within the Estonian eID scheme: 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.

Ministry of Foreign Affairs (MFA)

The MFA is the issuing authority. MFA is a government agency in charge of conducting and designing Estonian Foreign policy. MFA's competence in foreign relations is provided for in the Foreign Relations Act [14] and in a Statute of the MFA [16]. According to the Foreign Relations Act [14] the MFA accredits diplomats and consular representatives of foreign states and international organisations, issues cards to the members of staff of diplomatic missions and consular posts of foreign states and representations of international organisations. Development, implementation, and management for the cards are the responsibility of the MFA's State Protocol Department, which operates on the basis of the department's statute.

Estonian Police and Border Guard Board (PBGB)

The PBGB 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].

PBGB is operating under the authorisation of the Estonian Government to represent MFA for procurement of card blanks, personalisation and certificates.[19]

Development, preparation of tenders and contracts, implementation, and management (including procedures concerning complaints) for identity documents are the main responsibilities of the Identity and Status Bureau of PBGB.

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 [20].

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 [21],
- collecting, analysing, solving security incidents and informing them to ENISA (CERT, E-ITS [21]),
- 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 [22].

In the Estonian public sector, all information systems, including the eID scheme must comply with the Estonian Information Security Standard (E-ITS) [21].

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 [21] is based on the German BSI IT-Grundschutz baseline security system. [23]

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 [4].

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.

Helpline

ID software user support for electronic use of the 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.

Diplomatic identity cards are issued by the MFA; 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 certification service provider 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 Contractor shall hold a non-life insurance contract with an insurer authorised in Estonia, the European Union (EU) or another Member State of the European Economic Area to which the Contracting Authority 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.

Contracting partners are responsible for the fulfilment of all commitments outsourced to another entity and compliance with the policies as stated (including an obligation to notify of 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 for 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 [24] and is considered as a provider of a service of general interest; therefore, the General Part of the Economic Activities Code Act [25] applies.

Termination of CA is stipulated in eID CPS [8].

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.

Applicable terms and conditions (including any limitations of usage and privacy policy) are defined and explained under section 2.1.1. The terms and conditions, the procedure for the issue and revocation of a diplomatic identity card, the format and technical specification of a card, the list of information entered on a card, and the registration procedure of non-residents exempt from income tax is listed in the Protocol Guide [26]. Usage of personal data and privacy is regulated by the GDPR [27] and 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.

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.

The MFA is fully responsible, according to the internal procedures and regulations, for coordinating change management and communication of all aspects of issuing the cards in a timely and reliable fashion, without undue delay. Service planners are 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.

Internal process of the MFA provides the guidelines for issuance of the cards and for services necessary after issuance (i.e. revoking the certificates).

Additionally, the Terms and Conditions for Use of Certificates of Personal Identification Documents of the Republic of Estonia 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 and high.

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 [21] 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 [21} is a tool for risk and security management; hence, the requirement is fulfilled. State supervision for E-ITS [21] 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.

Regulation 3 of the Minister of Foreign Affairs of 23.05.2016 [13] provides, in section 11, that submitted applications, with all additional documents presented, are kept according to the Archives Act [30] and its subordinate acts.

Section 11 provides that all data in the database will be archived after the accreditation, and other processes related to it, of the member of the foreign mission staff and her/his family member, private servant, and honorary consul, is finished. The archived data is preserved for seven years. The following data about the applicant of the card will be permanently preserved: the name of the foreign mission, surname and family name, rank, presumed starting and ending time of the posting, name of the position in both Estonian and English, the time of leaving the posting, and, in case of an ambassador, the date of presenting the credentials.

Activity record log files are saved and stored for ten years after creating the records in a saved CSV file on the hard drive.

Regulation 3 of the Minister of Foreign Affairs of 23.05.2016 [13] provides, in section 12, that the security class for data in the database of VEIS and the database security level. According to section 18, the decision of liquidation of the database can be made by the Minister of Foreign Affairs.

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.

The Archives Act [30] provides for the appraisal of records, acquisition and preservation of archival records, grant of access thereto, organisation of the use thereof, and liability for rendering records and archival records unusable and destruction thereof, establishment of the bases for records management of agencies and persons performing public duties, and bases for the activities of the National Archives and local government archives.

Regulation 181 of the Government of the Republic of 22.12.2011 [31], the archival rules, regulates and specifies the requirements for the 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 public archive, and access management, including issuance of the archival notice of the archive records.

SUBSTANTIAL

Same as level low.

HIGH

Same as level low.

2.4.5. Facilities and staff

Estonian eID is managed by the Estonian government; 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 [32], Foreign Service Act [33] and Employment Contracts Act [34].

Additionally, E-ITS [21] 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 planner/owner. 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. 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 [21] or ISO 27001 [35] 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 contractors come from the eIDAS Regulation [2], the Electronic Identification and Trust Services for Electronic Transactions Act [5], and the contracts. 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 [7] and www.id.ee webpage, CPSs are available on CA webpage [8].

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 [21] or ISO [35] 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 contractors come from the eIDAS Regulation [2], the Electronic Identification and Trust Services for Electronic Transactions Act [5], and the contracts. The certificate policies and certification practice statements for the ID-1 format identity documents (which apply for the diplomatic identity card likewise) are publicly available electronically respectively on CA webpage [8] or www.id.ee webpage [11].

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 [21] or ISO [35] 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 contractors come from the eIDAS Regulation [2], the Electronic Identification and Trust Services for Electronic Transactions Act [5], and the contracts. The contractors have an insurance policy to provide the security of the service.

The bases of continuity of vital services are regulated in the Emergency Act [24].

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.

Internal document of information management procedure establishes general principles for requesting access rights and obligations at the end of the employment. In addition, there are internal rules that regulate security and fire safety, e.g. general ATS system, in archive and for servers' automatic gas extinguishing system.

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 [21] 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 contractors come from the eIDAS Regulation [2], the Electronic Identification and Trust Services for Electronic Transactions Act [5], and the contracts; also, from the CP [7]. The contractors for manufacturing and personalisation of the 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 private parties, come from European and national legislation, and the contracts. Data between the MFA, the card manufacturer, and CA transfers through secure PBGB exchange interface HUB.

MFA accesses the environment via X-tee data change.

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 ID1-format identity documents. HUB is a gateway-type service that mediates communication between the parties involved in the ID card (applies for diplomatic cards also) 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 ID1 HUB is to manage and mediate:

- requests for personalisation orders of ID-1 format identity documents 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 ID1 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 contractors, come from European and national legislation, and the contract.
Data between the MFA, the card manufacturer, and CA transfers through secure PBGB exchange interface HUB.

MFA accesses the environment via X-tee data change.

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 contractors 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 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 card holders.

Requirements for contractors come from the eIDAS Regulation [2], the Electronic Identification and Trust Services for Electronic Transactions Act [5], and the contracts. IDA [4] 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 contractors 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. for example, data must be physically stored only in the Estonian territory.

SUBSTANTIAL

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

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

HIGH

Same as level substantial.

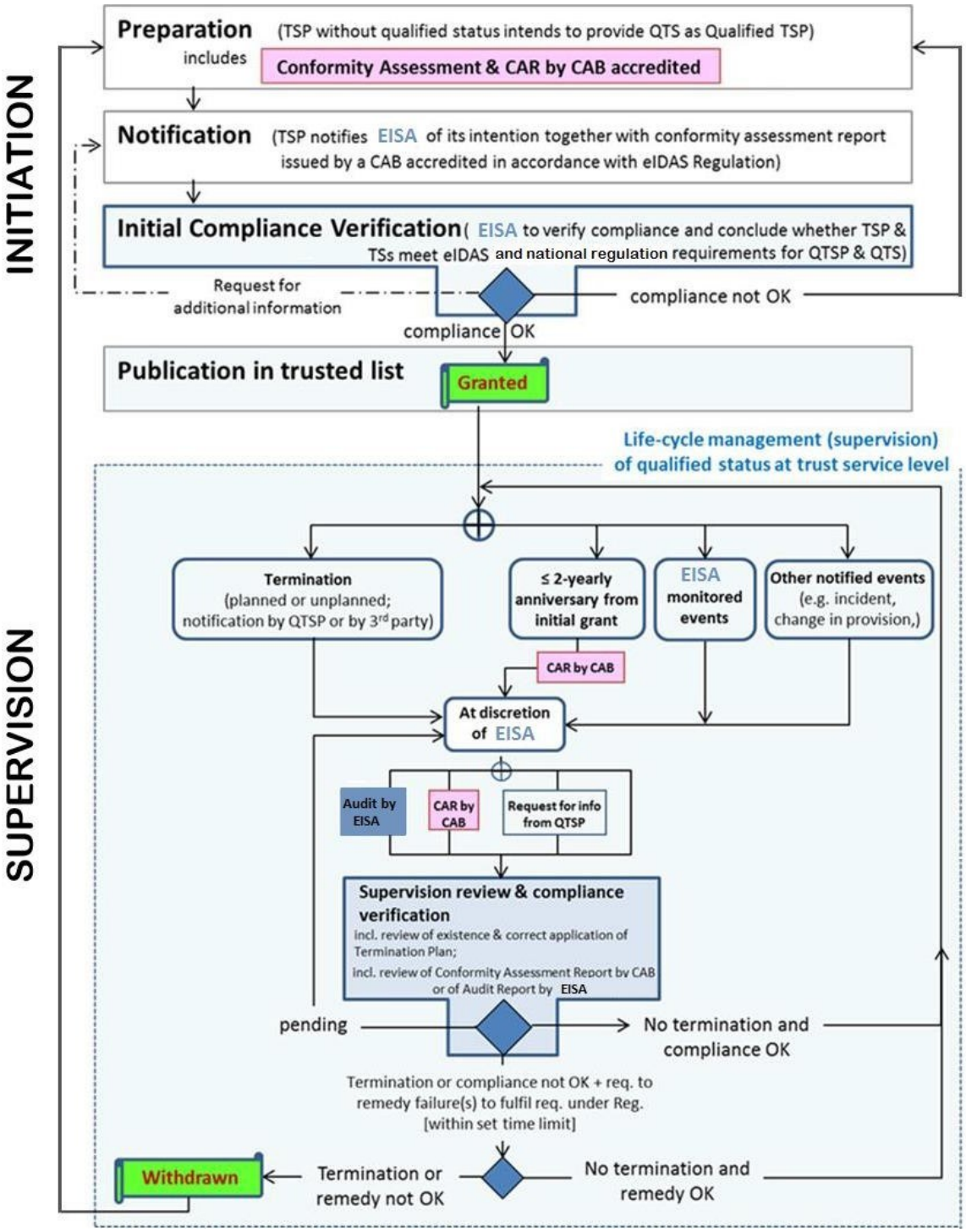
2.4.7. Compliance and audit

The qualified trust service provider Zetes SA 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 of LSTI SAS (CAB is accredited for the certification of trust services according to ISO/IEC27001 and ETSI EN 319 403 [36]) and confirmed as a QTSP according to

article 3 (20) of eIDAS by RIA. The initiation and supervisory activities of CA and its qualified trust service provided, and lifecycle management of the related qualified status are carried out according to the figure below. CA activities are under regular supervision throughout the lifecycle of such services, from their commencement to their termination. 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, 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, the ETSI European Standard (ETSI EN), and national regulations. Information related to 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 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 at 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 diplomatic identity card issued by the MFA) 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 and national law. An external E-ITS [21] audit has been conducted for the MFA information system (including the database of VEIS [13]) as of 26.062017, and the next planned audit will be conducted in accordance with the stated E-ITS security level.

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 [37]; hence, this requirement is fulfilled.

List of References

[1]	Commission Implementing Regulation (EU) 2015/1502 of 8 September 2015 on Published: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02015R1502-20220711
[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%3A02014R0910-20241018
[3]	Vienna Convention on Diplomatic Relations Published: https://treaties.un.org/pages/viewdetails.aspx?src=treaty&mtdsg_no=iii-3&chapter=3&clang=_en
[4]	Identity Documents Act (IDA) https://www.riigiteataja.ee/en/eli/ee/505012026002/consolide/current
[5]	Electronic Identification and Trust Services for Electronic Transactions Act Published: https://www.riigiteataja.ee/en/eli/ee/529122024007/consolide/current
[6]	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/
[7]	Certificate Policy for ID-1 format identity documents of the Republic of Estonia" (eID CP) Published: https://www.id.ee
[8]	Zetes Estonia OÜ - Certification Practice Statement for the Intermediate CA for ID-1 documents of the Republic of Estonia; Trust Service Practice Statement (eID CPS) Published: https://repository.eidpki.ee/repository/
[9]	Regulation 7 of the Minister of the Foreign Affairs, as of 09.03.2017 (in Estonian only) Published: https://www.riigiteataja.ee/akt/126082025005?leiaKehtiv
[10]	Diplomatic Portal Published: https://dipid.mfa.ee/
[11]	www.id.ee webpage Published: https://www.id.ee/
[12]	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
[13]	Regulation 3 of the Minister of Foreign Affairs, as of 23.05.2016," (in Estonian only) Published: https://www.riigiteataja.ee/akt/126092025004?leiaKehtiv
[14]	Foreign Relations Act Published: https://www.riigiteataja.ee/en/eli/ee/530092025011/consolide/current
[15]	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
[16]	Statute of MFA (in Estonian only Published: https://www.riigiteataja.ee/akt/101112011004?leiaKehtiv
[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]	Authorisation of the Estonian Government (only in Estonian) Published: https://www.riigiteataja.ee/akt/303122022004
[20]	SMIT Statute (only in Estonian)

	Published: https://www.riigiteataja.ee/akt/109072024006?leiaKehtiv
[21]	Estonian Information Security Standard (E-ITS, website in Estonian, some documents also in English) Published: https://eits.ria.ee
[22]	RIA Statute (only in Estonian) Published: https://www.riigiteataja.ee/akt/127122024010?leiaKehtiv
[23]	German BSI IT-Grundschutz baseline security system Published: https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/it-grundschutz_node
[24]	Emergency Act Published: https://www.riigiteataja.ee/en/eli/ee/527102025001/consolide/current
[25]	General Part of the Economic Activities Code Act Published: https://www.riigiteataja.ee/en/eli/ee/504012018003/consolide/current
[26]	Protocol Guide Published: https://vm.ee/en/ministry-news-and-contacts/state-protocol/protocol-guide
[27]	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 Published: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679&qid=1765634765358
[28]	Personal Data Protection Act Published: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02016R0679-20160504
[29]	Public Information Act Published: https://www.riigiteataja.ee/en/eli/ee/514112013001/consolide/current
[30]	Archives Act Published: https://www.riigiteataja.ee/en/eli/ee/521032019019/consolide/current
[31]	Regulation 181 of the Government of the Republic of 22.12.2011 (in Estonian only) Published: https://www.riigiteataja.ee/akt/114072023005?leiaKehtiv
[32]	Civil Service Act Published: https://www.riigiteataja.ee/en/eli/ee/503022026003/consolide/current
[33]	Foreign Service Act Published: https://www.riigiteataja.ee/en/eli/ee/515092025004/consolide/current
[34]	Employment Contracts Act Published: https://www.riigiteataja.ee/en/eli/ee/501092025001/consolide/current
[35]	ISO standards https://www.iso.org/standards.html
[36]	ETSI EN 319 403 Published: https://www.etsi.org/deliver/etsi_en/319400_319499/31940301/02.03.01_60/en_31940301v020301p.pdf
[37]	Government of the Republic Act Published https://www.riigiteataja.ee/en/eli/ee/504092025010/consolide/current