REPUBLIC OF ESTONIA
POLICE AND BORDER GUARD BOARD

Estonian eID scheme: ID card

Technical specifications and procedures for assurance level high for electronic identification

27/02/2018

Table of contents

Table of figures

Introduction

The current document maps the characteristics of the Estonian eID token based on the Estonian ID card to the requirements of the eIDAS levels of assurance, defined in the Commission Implementing Regulation (EU) 2015/1502 pursuant to article 8 (3) of the eIDAS Regulation [1] (EU) 910/2014.
As follows, each requirement of the implementing regulation is considered, and it is explained how the Estonian ID card meets the requirements for the level of assurance high. Below is the caption of the specimen of the Estonian ID card.

Caption 1 – specimen of the Estonian ID card

Reliable and secure personal identification as well as physical and digital identity management are the basis for a credible process of issuing identity documents. Estonia has long-term experience in using electronic authentication and is a global leader in the context of e-government. Estonia issues the ID card as the primary and mandatory document for identifying its citizens and EU citizens living in Estonia. The owners of ID card have the right to have an additional digital identity carrier or eID token such as Digi-ID or Mobiil-ID. The chip card issued is a physical identification document and has advanced electronic functions that facilitate secure authentication and a qualified electronic signature. The first Estonian ID cards were issued on 28/01/2002. The card is meant to be universal, and its functions are to be used in any form of business, governmental, or private communications. The aim is to help people make everyday communications more convenient.

The Ministry of the Interior is responsible for the development of policies of identity management and for policies in connection with issuing identity documents to Estonian citizens and aliens.

General principles of the policy for identity management and personal identification documents [2]:

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

The Estonian Police and Border Guard Board is responsible for identity management and issuing personal identification documents (hereinafter referred to as *the issuing authority*). The issuing of identity documents is regulated by the Identity Documents Act [3].

Estonian eID scheme is based on using PKI with cryptography according to best practises and using SSCD/QSCD smartcards.

The issuer identifies physically the person during the issuance process.
The Estonian electronic ID card application specification (EstEID) fulfils ISO/IEC 7816 standard requirements for electronic identification and signing operations. The latest EstEID standards, certificate profiles, and specifications are publicly available [4]. The name of the Estonian ID card certificate is ESTEID. On the Estonian ID card chip, there are two private keys with corresponding public keys on the X.509-format certificates. The certificates are stored both on the chip and LDAP repository (available for e-services).

1) certificate for electronic authentication and encryption;
2) certificate for providing a qualified electronic signature.

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.

From a certificate, the following information can be read about the ID card holder's data without entering the PIN1 code:

- first name;
- surname;
- date of birth (part of the person's identification code);
- person's identification code;
- sex (part of the person's identification code);
- certificate issuer;
- serial number of the certificate;
- date of expiry of the certificate;
- date of issue of the certificate.

Definitions

1) *authoritative source* means any source irrespective of its form that can be relied upon to provide accurate data, information, and/or evidence that can be used to prove identity;
2) *CA* – Certificate Authority;
3) *CAB* – Conformity Assessment Body;
4) *CAR* – Conformity Assessment Report;
5) *CRL* – Certificate Revocation List;
6) *CSP* – Certificate Service Provider;
7) *eIDAS* or *eIDAS Regulation* [1] – Regulation (EU) no. 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market;
8) *Estonian eID tokens* means the Estonian ID card, Estonian residence permit card (RP card), Estonian Digi-ID, Estonian e-Residency Digi-ID, Estonian Mobiil-ID, and the Estonian diplomatic identity card;
9) *GDPR - General Data Protection Regulation* [5] - 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 and is applicable from 25 May 2018;
10) *ID Card Utility* – an end-user desktop application for personal maintenance (unlock/change the PIN codes, change the PUK code, renew certificates, configure official email, etc.) of smartcard-based eID;
11) *information security management system* means a set of processes and procedures designed to manage, to acceptable levels, risks related to information security;
12) *OCSP* – Online Certificate Status Protocol;
13) *QTS* – Qualified Trust Service;
14) *QTSP* – Qualified Trust Service Provider;
15) *TS* – Trust Service;
16) *URL* – Uniform Resource Locator, also known as web address;

2. Technical specifications and procedures

The elements of technical specifications and procedures outlined in this annex of the Commission Implementing Regulation (EU) 2015/1502 will be used to determine how the requirements and criteria of article 8 of Regulation (EU) no. 910/2014 will be applied for electronic identification means issued under an electronic identification scheme.

2.1. Enrolment

The Estonian ID card (ID card) is an identity document mandatory for Estonian citizens and the citizens of the EU 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 ID card and the obligations of the holder are regulated by the eIDAS Regulation [1], Identity Documents Act [3], Electronic Identification and Trust Services for Electronic Transactions Act [6], Certificate Policy for ID card [7] and Certificate, CRL and OCSP Profile for Personal Identification Documents of the Republic of Estonia [8].
According to section 11^4 of the Identity Documents Act [3], the initial ID card can be applied for only in person (or via a legal representative) in an office of the issuing authority or in the official foreign representation of the Republic of Estonia. In cases of expiry, loss, or theft, Estonian citizens and EU citizens can apply for a recurring ID card in one of the following methods:

- in an office of the issuing authority;
- in the official foreign representation of the Republic of Estonia;
- via post;
- via email;
- in an e-environment (currently available only for Estonian citizens who have been previously issued an ID card).

The basic terms and conditions related to the use of the electronic identification means of the Estonian ID card are listed on paper form with an ID card and are introduced by the issuing authority during the issuance process. The paper form consists of two parts: firstly, the terms and conditions; secondly, the acknowledgement part. The recipient signs the paper form physically, acknowledging and accepting the terms and conditions, after which the acknowledgement part is separated by an official of the issuing authority. The signed acknowledgement on paper is archived by the issuing authority. The recipient receives the part of the terms and conditions on paper together with an information brochure.
Additionally, on the website of the issuing authority, there is a reminder on safe usage of the ID card [9], which is also available on a paper brochure in the service point of the issuing authority.
Furthermore, a detailed version of the terms and conditions for the use of certificates of personal identification documents [10] is publicly available on the website of the certification service provider

(CSP), and a printout can be requested from the issuing authority or the official foreign representation of the Republic of Estonia.

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

The obligations of a holder and return of an ID card are stated in section 14 of the Identity Documents Act [3]. Additionally, recommended security precautions related to the electronic identification means are listed on the information brochure, on the reminder on safe usage of an ID card, and in the terms and conditions for the use of the certificates mentioned above in section 1; for example, not to hand over one's ID card, to keep the PIN codes of a card secret from others, to ensure the ID card is used only under the control of its holder, to promptly notify the issuing authority in order to suspend the certificates in case of lost, stolen, or forgotten 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 based on Regulation 77 of the Minister of the Interior, as of 18/12/2015 [11]. Collecting application and relevant identity data required for identity-proofing in the official foreign representation of the Republic of Estonia is additionally regulated by the Consular Act [12] and regulations of the minister responsible. Collected identity data is checked against the database of the Estonian population register and identity documents database.
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 representative, or electronically);
- 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]);
- paid state fees;
- the Minimum Data Set listed in section24 of Regulation 77 of the Minister of the Interior, as of 18/12/2015 [11], 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);
    4) place of issuance;
    5) reason for applying;
    6) date.

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 Estonian 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 Estonian 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 Estonian ID card, the identity of the applicant and the validity and authenticity of their document is always verified, not assumed.

SUBSTANTIAL

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 together with the Estonian eID token, referred to in this document as the Estonian ID card. The Estonian ID card is issued to both Estonian citizens and EU citizens. The ID card issued to European Union citizens is valid for using Estonian e-services, but is not recognised as a travel document. Data about every ID card application is recorded in the identity documents database. Aliens who have been issued an Estonian identity document under Identity Documents Act [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 and the identity documents database in accordance with the Identity Documents Act [3] and regulations issued on the basis of that act. The identity documents database ascertains whether an Estonian identity document is valid, but also provides information about the personal data of the document holder (including a facial image), 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.

When an EU citizen applies for an ID card, their data is also checked against the population register and the identity documents database 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. To verify the validity and authenticity of the presented identity document, the data of the document is checked against the Schengen Information System (SIS) and the INTERPOL database of lost and stolen documents. The authenticity of the presented identity document is verified in accordance with the sample documents presented by other Member States.

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 [14]; in case of a recurring ID card, the identification is done based on the previous ID card and the Estonian population register; in case of EU citizens, based on a valid identity document including biometric data, such as a photo.

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 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 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 valid identity document including biometric data is checked in accordance with the Identity Documents Act [3] and regulations issued on the basis of that act, as well as with the internal procedures and regulations of the issuing authority. The personnel of the issuing authority follows the routine procedure to check that the document is genuine and corresponds to the data provided in either national or international registers, whether the document provided is valid and not listed as lost, stolen, revoked, or expired. During application, a physical identity check is conducted, together with a system checks to the SIS and INTERPOL.

(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 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 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 an exceptional case where a valid document issued by Estonia is lost or stolen, the person is identified on the bases of the information entered previously into the identity documents database.

2.1.3. Identity proofing and verification (legal person)

The Estonian 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 Estonian 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 Estonian ID card eID: a chip ID card and PIN codes. The first factor of authentication is being in the possession of a chip ID card. The second factor of authentication are the PIN codes that are issued together with the ID card. The person receives three securely sealed codes: PIN1 for authentication purposes, PIN2 for a qualified electronic signature, and PUK for de-blocking the PIN codes after entering an incorrect PIN code three times.
The user 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 user.

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 user'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 smart card is a SSCD/QSCD 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 user has physical control over the authentication device. The user has the option to change the PIN codes at any time by using a(n offline) PC application. Certificate suspension service is available 24/7.

2.2.2. Issuance, delivery, and activation

The process of issuance, delivery, and activation is regulated by the Identity Documents Act [3] and the Consular Act [12].

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 an authorised representative assigned by the applicant at the time of applying for the document, and the ID card is issued at the issuing authority service point or in the foreign representation of the Republic of Estonia indicated in the application form. The choice of the receiver of an ID card and the place of receiving must be stated in the application. The choice of the receiver cannot be changed later in the process. This possibility can be applied only if the person has provided the application in person at the issuing authority service point or in the foreign representation of the Republic of Estonia, which means at least one face-to-face contact for physical identification to be carried out.
On receipt of an ID card, the applicant must provide a previously issued valid document of the same type, which, in current case, would be an ID card.
In case of an authorised representative, the authorised person provides one's valid identity document issued by the Republic of Estonia and a previously issued valid document of the same type which has been applied for by the applicant.

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 is that the ID card is issued only personally to the applicant or to an authorised representative (who has been appointed at the application) only after identity-proofing. The authenticity of the presented identity document is verified in accordance with the sample documents database. This

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.

ID cards are delivered to the issuing authority service point or the foreign representation of the Republic of Estonia in an electronically deactivated form (meaning that the eID functionality is not active). If an ID card is issued at the issuing authority service point to the applicant personally or to an authorised representative, the ID card is activated by the issuing authority after the identity-proofing of the receiver (or an authorised representative), who signs physically the terms and conditions related to the use of the electronic identification means of the Estonian ID card on paper with the ID card. 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. After identity-proofing, the eID functionality is activated by the official of the issuing authority.

If the ID card is issued at the foreign representation of the Republic of Estonia, then the physical ID cards are delivered by diplomatic post. An official of the issuing authority activates the electronic identification means of the ID card manually in the system within one working day after receiving an email notification from an employee of the foreign representation of the Republic of Estonia stating that the eID token has been issued after identity-proofing.

2.2.3. Suspension, revocation, and reactivation

The legal framework of suspension, revocation, and reactivation of the electronic identification means are set by the eIDAS Regulation [1], with its implementing acts, and is regulated at the national level by the Identity Documents Act [3], the Electronic Identification and Trust Services for Electronic Transactions Act [6], the certificate policy for the ID card [7], and the issuing authority's internal order for servicing of certificates, which includes certificate suspension service, termination of suspension, renewal, certificate revocation service, and validity confirmation service. The card holder is obliged to notify the issuing authority within 24 hours in case of the theft or loss of the ID card, so the following processes could be triggered:

1) Suspending the certificates – can be done via calling the 24/7 helpline (or the international number +372 677 3377) for operative reasons. The person must identify themselves by stating one's name and personal identification code. The calls are recorded for the purpose of later control. Suspending of the certificates can be also done in the service point in person. Suspending the certificates means that electronic functionality cannot be used (i.e., e-services cannot be used), the physical document remains enact. For ending the suspension, the person must appear in person in a service point of the issuing authority and file the corresponding application.
2) Revocation of an ID card (including the certificates) – can be done only in person by appearing in a service point of the issuing authority and filing the corresponding application. Revocation

of the ID card means that the certificates are revoked; therefore, electronic functionality cannot be used and the physical document itself is no longer valid.

LOW

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

Suspension and restoration is regulated under section 9^5 of the Identity Documents Act [3].

The certificates of an ID card can be suspended in the issuing authority service point in person or via calling the 24/7 helpline 1777 (or the international number +372 677 3377), or in the SEB and Swedbank offices in Estonia. E-services cannot be used/accessed if the certificates are suspended, not activated or revoked as stated above.
For suspension of certificates in a service point of the issuing authority, an official identifies the person according to the issuing authority's internal processes, marks the requested certificate status as *suspended* in the CSP interface, enters the reason for suspension, and confirms the certificate status suspension. The certificate suspension form is printed out and signed physically by the card holder of the certificates and the official. The official also performs a check to verify that the certificates are in the status *suspended*.
For suspension of certificates via calling the 24/7 helpline 1777 (or the international number +372 677 3377), the person is identified by name and personal identification code while the call is recorded for the purpose of later control and evidence.
The revocation procedure is process-wise similar to suspension, as described above, with the difference that it can only be done in the offices of the issuing authority and the certificate status is set as *revoked*. After revocation is completed, 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. above.

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

The suspension process can be performed only by the authorised staff of the issuing authority or by the authorised staff of the helpline, and the minimum information for suspension is the person's first name, last name, and date of birth or personal identification code.
The certificates can be reactivated upon the request of the certificate user or upon the request of an administrative official stated by law. Reactivation can only be done in the office of the issuing authority after physical identification. Reactivation cannot be done via phone or email.
Revocation can be performed only in the offices of the issuing authority 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.**

Once the certificates are suspended, they can be reactivated only in the issuing authority service point. For reactivating the certificates in suspended status, an official of the issuing authority identifies the

person according to the issuing authority's internal processes, after which the former chooses the requested certificates' status as *end suspension* in the CSP interface and confirms the change of the certificate status. The form of ending certificate suspension is printed out and signed physically by the user of the certificates and the official. The official also performs a check to verify that the certificates are in the *active* status.

The legal basis for revocation of certificates is stated in section 9^6 of the Identity Documents Act [3].

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.

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 Identity Documents Act [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. Therefore, it is the responsibility of the ID card holder to keep the person's identification data up to date. For renewal of the ID card, the person must fill in the application, providing personal data (including a photo), which is checked against existing information, provided previously.

In exceptional cases, certificate renewal might be needed if an issue is detected with the certificate(s), upgrading the cryptography is needed, certificate(s) are suspended or blocked, or remote certificate renewal has failed. In all cases, certificate renewal can be carried out at the offices of the issuing authority after the identity-proofing procedure, where the data provided is checked against the identity documents database and the Estonian population register. In cases where an issue is detected with the certificate(s), or while upgrading the cryptography, there is an additional option of remote certificate renewal via the user's personal computer (PC).
If an ID card malfunction falls under warranty or guarantee, then the new ID card and certificates are issued for the same period of validity without a charge to the ID card user.
The ID card warranty cases include:

- usage of electronic functionality being problematic;
- the ID card reader not recognising the ID 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.

Remote certificate renewal on the user's PC can be performed with the latest version of ID Card Utility only if the software provides the option of remote renewal for the particular ID card inserted into the reader. Renewal can be initiated after using the electronic authentication based on certificate with corresponding private key (which functional access is protected with PIN1), after which a response on the certificate status is received from the CA.

Remote certificate renewal functionality in the user's PC can only be completed if the person has a valid and functional ID card, knows the PIN codes, the ID card certificates are valid or suspended, and the PC has the latest version of ID Card Utility. The requirement is fulfilled as the person can start remote certificate renewal only after electronic authentication based on certificate with corresponding private key (which functional access is protected with PIN1) after which a response on the certificate status is received from CA.

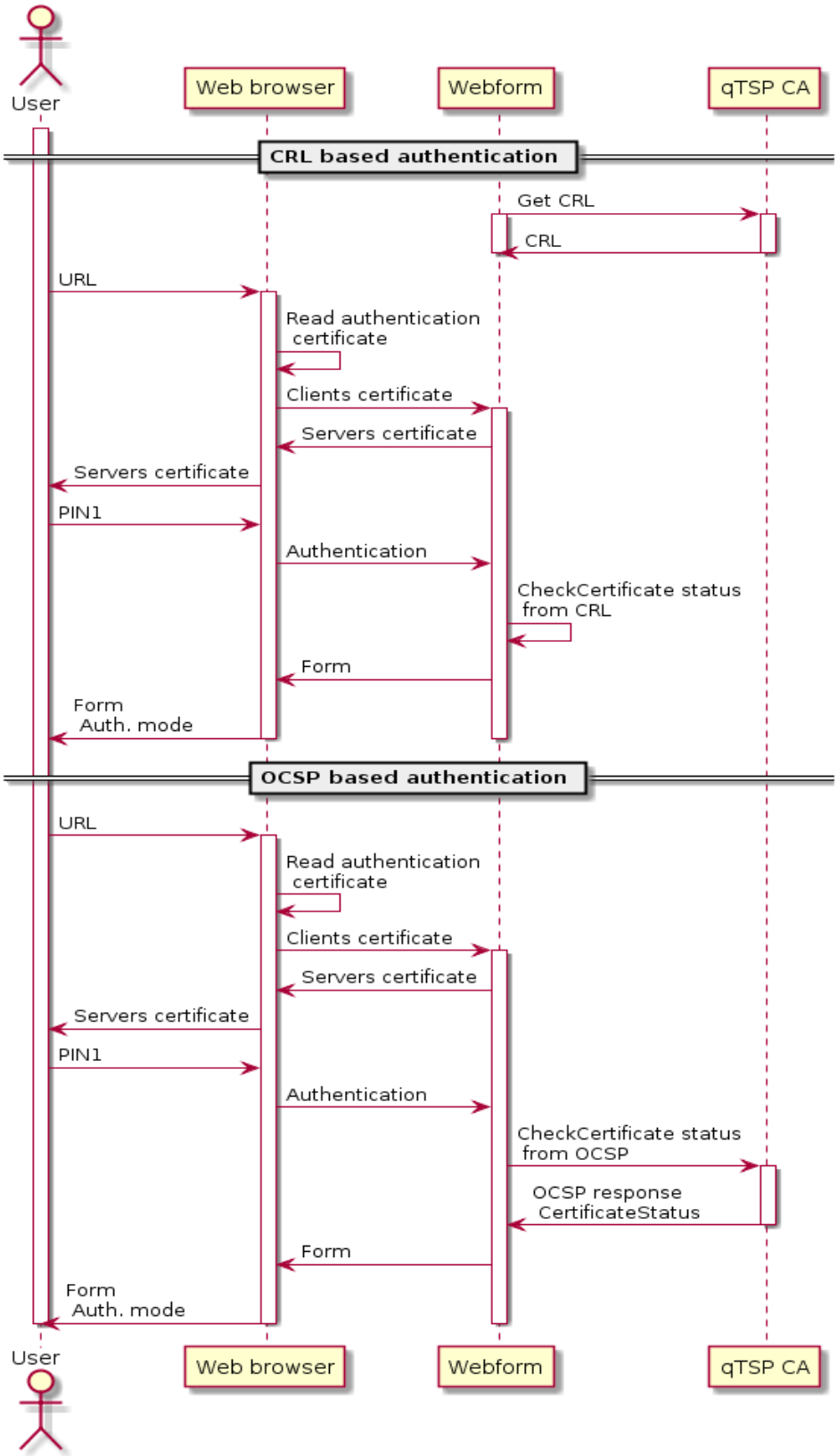
Certificate renewal at a service point of the issuing authority is done after the physical identification procedure, where the data provided is checked against the identity documents database and the Estonian population register. Certificates can be renewed in a service point only in person (authorisation is not permitted for certificate renewal).

The warranty form can be submitted in the offices of the issuing authority after the physical identification procedure or in cases of the user's request (via helpline and email) where the data provided is checked against the identity documents database. A new ID card is issued in a service point of the issuing authority or the official foreign representation after the physical identification procedure (authorisation is not permitted).

2.3. Authentication

2.3.1. Authentication mechanism

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



Caption 2 – authentication of the Estonian ID card

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 service or by using current CRL. 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 SSL/TLS is used. Data in 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 user, 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 SSL/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 user, 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 user, 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 Estonian Police and Border Guard Board is responsible for identity management, for issuing personal identification documents, and performs the functions of a point of single contact under eIDAS Regulation [1] article 9. 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: public and private. Both public and private parties must comply with requirements that come from European and national legislation.

1) Public authorities

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

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 [15] and the Statutes of the Police and Border Guard Board [16].

According to the Identity Documents Act [3], the PBGB exercises supervision over compliance with the contract under public law and has the competence of making a decision on the issue, suspension of validity, and revocation of an identity document (including the ID card).

Development, preparation of tenders and contracts, implementation, and management (including procedures concerning complaints) for identity documents (including the national ID card) are the main responsibilities of the Identity and Status Bureau (ISB). In personal identity document development, the requirements of the International Civil Aviation Organization [17] (ICAO) are followed.

- Documents Printing Centre – its responsibilities are personalisation of Estonian travel documents and serving as the logistic centre for the distribution of all types of identity documents (including the ID card) to the issuing offices and to the official foreign representation of the Republic of Estonia.
- Client information contact +372 612 3000 – provides general information about the services provided by the PBGB.

IT and Development Centre, Ministry of the Interior

The IT and Development Centre, Ministry of the Interior, 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 the IT and Development Centre, Ministry of the Interior [18].

Information System Authority (EISA)

The EISA is responsible for technical architecture, development of client/end-user software and chip technical specification, and software application for eID; ISKE [19]; cyber security incident management by the CERT-EE and supervision of vital services (incl. the trust service provider). The functions, rights, and organisation are provided in the Statutes of the Information System Authority [20].

In the Estonian public sector, all information systems, including the eID scheme, must comply with the three-level IT baseline security system ISKE. The goal of implementing ISKE is to ensure a security level sufficient for the data processed in IT systems. The necessary security level is achieved by implementing the standard organisational, infrastructural/physical, and technical security measures in availability (K), integrity (T), and security (S). It is an information security standard that is developed for the Estonian public sector. According to Government Regulation no. 273 of 12 August 2004, ISKE is compulsory for state and local government organisations who handle databases/registers. The preparation and development of ISKE is based on a German information security standard: IT Baseline Protection Manual (*IT-Grundschutz* in German), which has been adapted to suit the Estonian situation. A three-level baseline system means three different sets of security measures for three different security requirements. Ministries, agencies, plus registers connected to the state IS are obligated to perform IT audit according to their level: level high (H) every 2 years, level medium (M) every 3 years, and level low (L) every 4 years.

Technical Regulatory Authority (ETRA)

The Estonian Technical Regulatory Authority (ETRA) is the supervisory body who is responsible for supervisory tasks that are established in eIDAS [1] article 17. The ETRA manages and issues activity licences of Estonian trust service providers, maintains Estonian trusted list [21], and supervises trust service providers in meeting the specifications. The functions, rights, and organisation are provided in the Statutes of the Technical Regulatory Authority [22].

Ministry of Foreign Affairs

The Ministry of Foreign Affairs is responsible for forwarding collected applications to the PBGB for issuing Estonian ID cards and giving out issued ID cards in the official foreign representation of the Republic of Estonia.

2) 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 bodies.

Identity document manufacture and personalisation contractor

- The Estonian Police and Border Guard Board has a contract with Gemalto AG for manufacturing and personalisation of ID cards. The personalisation of ID cards is done by Gemalto AG subsidiary Trüb Baltic AS, located in Estonia.
- Gemalto AG has provided the following certificates:
    - Common Criteria Site Certification 2016–2018;
    - ISO9001 Gemalto AA+UE 2016–2019;
    - ISO14001 Gemalto AA+UE 2016–2019;
    - ISO14298 Gemalto AA 2015–2017;
    - ISO14298 Gemalto UE 2015–2017;
    - ISO/IEC 15408-1:2005 Information technology — Security techniques — Evaluation criteria for IT security — Part 1-3;
    - ISO27001 Gemalto AA+UE 2015–2016;
    - Known-Consignor AA 2015–2020;
    - Known-Consignor UE 2015–2020;
    - MasterCard PCI CP AA 2016–2017;
    - MasterCard PCI CP UE 2016–2017;
    - VISA PCI CP Gemalto AA 2015;
    - VISA PCI CP Gemalto UE 2015.

Certification Service Provider (CSP or CA): SK ID Solutions

CA is a partner of the Estonian state in issuing certificates for national identity documents (ID card, Mobiil-ID, Digi-ID, residence permit card, e-Residency Digi-ID, and diplomatic identity card). CA is the subcontractor of Gemalto AG for issuing certificates, providing the LDAP, the OCSP, CRL, and time-stamping services and is responsible for serving the certificates for their whole validity period (including verification, suspension, revocation, and activation of certificates; receipt of a replacement PIN envelope). CA is included in the European Trust List as qualified trust service provider and fulfils the eIDAS Regulation [1] requirements for qualified certificates for electronic signatures [23]. The offices of the issuing authority receive the data of a card applicant and verify its validity; CA provides electronic certificates for the ID card.

Helpline

ID card helpline international phone no +372 677 377 or no 1777 available 24/7.

I level support for the end-user at abi@id.ee provides information on the following matters:	**II level support for organisations and developers at** support@sk.ee provides information on the following matters:
certificate status information and suspension; • ID card-related activities (change of PIN or PUK codes, etc.); • eID usage and issues (authentication, e-signature); • eID middleware install, usage, and issues; • eID usage and e-service support.	• PBGB service point issues with certificates; • I level technical support for organisations and developers.

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 Identity Documents Act [3] and the Statutes of the Police and Border Guard Board [16] 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.**

The service provider (Gemalto AG) should have a valid bank guarantee during the whole contract period as the warranty of their obligations arising from the contract. In addition, during the validity period of the contract, the service provider should have a sufficient insurance policy. According to the Electronic Identification and Trust Services for Electronic Transactions Act [6], the certification service provider must have a liability insurance contract [24], 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.

PBGB contractors (and subcontractors/partners)

Contractual partners of the PBGB must adhere, during procurement procedures, to bank guarantee, insurance, and confidentiality requirements. The bank guarantee must be valid during the whole validity period of the contract. During the validity period of the contract, the partner should have a sufficient insurance policy, which covers the replacement price, which includes the risks of theft or damage upon production, transportation, and/or personalisation, also in case of fire, damage of generating installations, or risks of theft or interruption of work. Additionally, partners must present a copy of an insurance certificate as evidence of a valid insurance policy required from a certification service provider by the legislation of the Republic of Estonia.

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 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 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 [25], and is considered as a provider of a service of general interest; therefore, the General Part of the Economic Activities Code Act [26] applies.

Termination of CA is stipulated in Trust Services Practice Statement [27].

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, 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. Furthermore, it deals with service after issuing, repeal of the document, and organising the working environment and quality control.
Applicable terms and conditions (including any limitations of usage and privacy policy) are defined and explained under section 2.1.1. The fees for identification documents (including the ID card) are regulated by the State Fees Act [28]. Usage of personal data and privacy is regulated by the GDPR [5] (applicable from 25 May 2018) and the Personal Data Protection Act [29], 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 the Identity Documents Database [30] provides the data protection principles.

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 PBGB is fully responsible for coordinating change management and communication of all aspects of document (including the ID card) issuance 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.

The PBGB internal process provides the guidelines for issuance and services related to identity documents after their issuance (i.e., PIN replacement, certificate renewal, etc.).

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.

The three-level IT baseline security system ISKE [19] 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 ISKE security levels and classes. ISKE is a tool for risk and security management; hence, the requirement is fulfilled. State supervision for ISKE compliance is conducted by the EISA.
Contractors adhere to and provide certificates of audits 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 [1], GDPR [5]) 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 [31] 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 [29] 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 77 of the Minister of the Interior of 18/12/2015 [11] provides, in section 33, that submitted applications, with all additional documents presented, are kept according to the Archives Act [32] and its subordinate acts.

Regulation 78 of the Minister of the Interior of 18/12/2015 [33], the Statutes of the Identity Documents Database (ITDAK) [30], provides, in section 5, that, for ensuring availability, integrity, and confidentiality of data protection in databases, the organisational, physical, and information technology security measures must be implemented. Section 18 provides that data records are kept 50 years, as stated in the Archives Act [32]. According to section 20, the decision of liquidation of the state database can be made by the Government of the Republic and in accordance with the Archives

Act. The ITDAK has a service-level agreement between the service owner (PBGB) and the ICT service provider (SMIT), in which are stated quality parameters, ISKE [19] security classes, and highest data loss tolerance.

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 [32] 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 [34], 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 [35] and the statutes of particular responsible administrative authorities or agencies.

Additionally, ISKE [19] facilitates requirements for both facilities and staff.

The requirements for the security facilities and staff come from the tender documentation (annexes 2 and 3) and paragraph 7 and annexes 5 and 6 of the contract. The tender documentation is for use only inside the issuing authority (according to clause 35 (1) 10) of the Public Information Act [31]), and the contract requirements are confidential according to the contract. Gemalto AG operates under the PCI standards that cover the physical security part and personnel requirements.

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. 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 ISKE [19] 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 [1] (QTSP requirements), the Electronic Identification and Trust Services for Electronic Transactions Act [6], the tender documents, and the contract. All specific standards and requirements set out in the previously mentioned contract with Gemalto AG are applicable to the subcontractor(s) of Gemalto AG depending on their role.

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 ISKE [19] 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 [1] (QTSP requirements), the Electronic Identification and Trust Services for Electronic Transactions Act [6], the tender documents and the contract. The certificate policy for the ID card [7] (applies for the diplomatic identity card likewise) of the Republic of Estonia can be found on the website of the CSP.

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

Implementing ISKE [19] 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 [1] (QTSP requirements), the Electronic Identification and Trust Services for Electronic Transactions Act [6], the tender documents, and the contract. The contractor has an insurance policy to provide the security of the service.

Physical security requirements for manufacturing are based on the ISO and ICAO standards. Personalisation process and physical security requirements for the personalisation site come from the PCI standards. The physical and information systems security of the Ministry of Foreign Affairs 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 ISKE [19] 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 [1] (QTSP requirements), the Electronic Identification and Trust Services for Electronic Transactions Act [6], the tender documents, and the contract; also from the Certificate Policy for ID card of the Republic of Estonia [7] and the ESTEID-SK Certification Practice Statement [36]. Gemalto AG operates 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) – SK ID Solutions AS. Conformity assessment reports and certificates are available at https://sk.ee/en/repository/audit/.

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, the tender documents, and the contract. Data exchange interfaces between the PBGB, Gemalto AG, and CA must be encrypted (the parties are verified by conformity certification).
PKI-based solution (SSL authentication), in which:

a) Confidentiality – only the user's name, unique personal identification code, and state-issued email address is available for consumer service. Furthermore, encrypted data exchange is supported (usage depends on integration on the consumer service side).
b) Integrity – proper use of PKI technology assures integrity requirements.
c) Availability – granted with SLA requirements for trusted services (available 24/7).

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, the tender documents, and the contract. Data exchange interfaces between the PBGB, Gemalto AG, and CA must be encrypted (the parties are verified by conformity certification).

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 [1] (QTSP requirements), the Electronic Identification and Trust Services for Electronic Transactions Act [6], the tender documents, and the contract.

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) The user can check the history of use of one's certificate through a self-service portal if the OCSP service is used (available 24/7).
b) Middleware software (including card drivers) are maintained by the state and is frequently updated.
c) For emergency patches, there is a separate, secure procedure which requires the involvement of independent parties (CA, card producer, RA, middleware software management).
d) All certificates can be centrally revoked immediately in case of a large scale security breach.

Requirements for contractors come from the eIDAS Regulation [1] (QTSP requirements), the Electronic Identification and Trust Services for Electronic Transactions Act [6], the tender documents, and the contract. The issuing authority has the right to revoke the certificates if there is reason to believe that it is possible to use the private key corresponding to the public key contained in the certificate without

the consent of the certificate holder or the document is no longer in compliance with the requirements needed for the secure use thereof [3].

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 [1] (QTSP requirements), the Electronic Identification and Trust Services for Electronic Transactions Act [6] and other applicable national legislative acts, the tender documents, and the contract; 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.

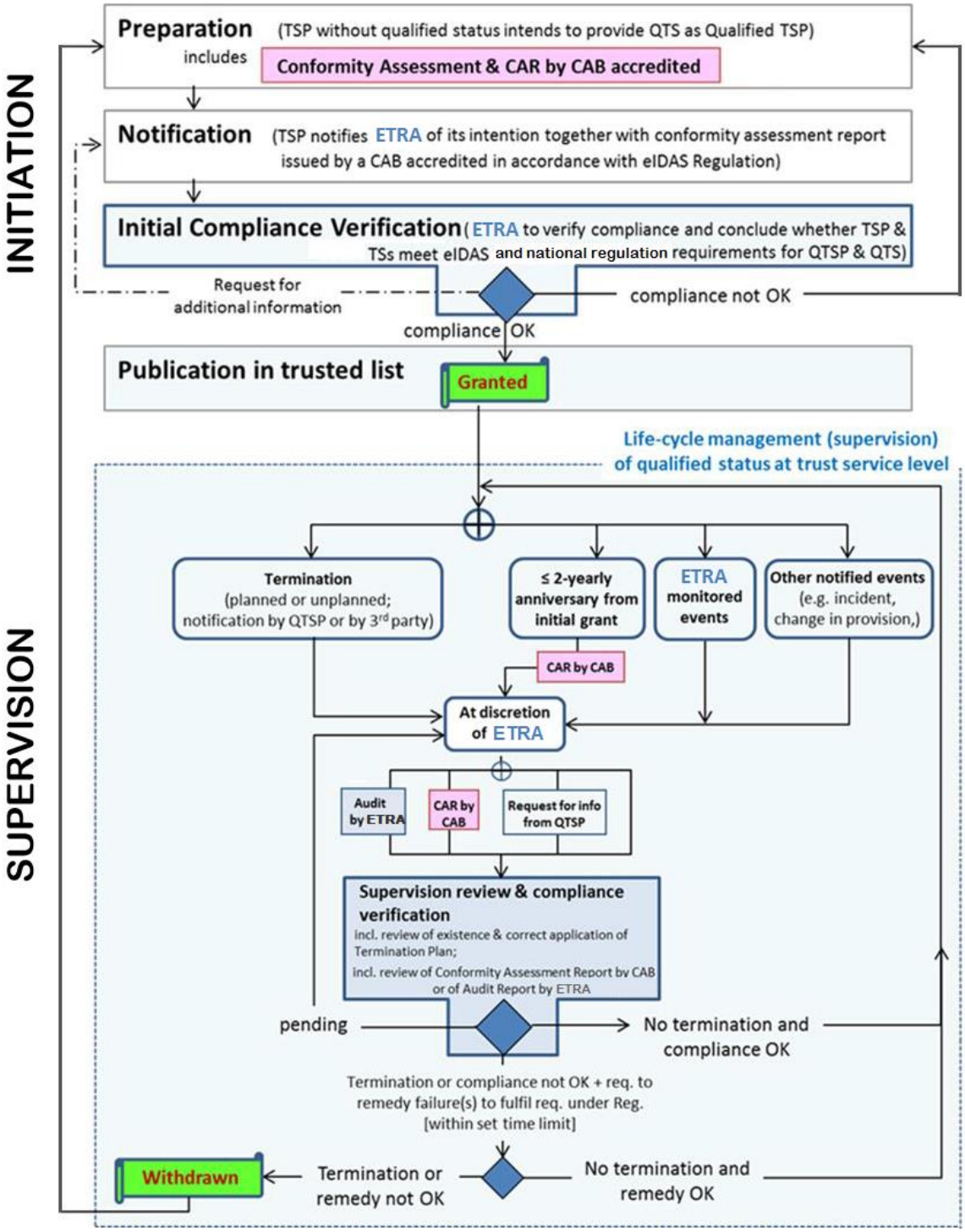
Requirements for contractors come from the eIDAS Regulation [1] (QTSP requirements), the Electronic Identification and Trust Services for Electronic Transactions Act [6] and other applicable national legislative acts, the tender documents, and the contract.

HIGH

Same as level substantial.

2.4.7. Compliance and audit

The qualified certification service provider SK ID Solutions AS is subject to the eIDAS Regulation [1], with its implementing acts, and, at the national level, is regulated by the Electronic Identification and Trust Services for Electronic Transactions Act [6].
CA has been audited by the certification body of TÜV Informationstechnik GmbH (accredited by DAkkS Deutsche Akkreditierungsstelle GmbH) and confirmed as a qualified trust service provider according to point (20) of article 3 of eIDAS by the ETRA. The initiation and supervisory activities of CA and its QTS 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 the ETRA 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://sk.ee/en/repository/.



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 ID card) must be audited accordingly and/or comply with requirements of standard(s) (QTSP, PCI and/or ISO) until the expiry of the contract or until the expiry of the last certificate pair issued and/or renewed according to the specifics of particular standard or audit. CA is audited at least every 2 years by ETRA 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 ISKE [19] audit has been conducted for the PBGB information system (including the identity documents database) as of 4 December 2017, and the next planned audit will be conducted in accordance with the stated ISKE security level.

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

Estonian eID 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.

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 EISA and the ETRA is done by the Ministry of Economic Affairs and Communications.
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 2012). 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.

References

[1] “eIDAS Regulation,” http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2014.257.01.0073.01.ENG .

[2] “Internal Safety Development Plan 2015–2020,” (in Estonian only), https://www.valitsus.ee/sites/default/files/content-editors/arengukavad/taiendatud_siseturvalisuse_arengukava_2015-2020.pdf.

[3] “Identity Documents Act,” https://www.riigiteataja.ee/en/eli/521062017003/consolide.

[4] “EstEID v. 3.5 Estonian electronic ID card application specification,” http://id.ee/public/TB-SPEC-EstEID-Chip-App-v3.5-20170314.pdf.

[5] “GDPR,” http://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32016R0679 .

[6] “Electronic Identification and Trust Services for Electronic Transactions Act,” https://www.riigiteataja.ee/en/eli/527102016001/consolide.

[7] “Certificate policy for the ID card,” https://sk.ee/upload/files/SK-CP-ID%20CARD-EN-v6_0_20161101.pdf .

[8] “Certificate, CRL and OCSP Profile for Personal Identification Documents of the Republic of Estonia,” https://sk.ee/upload/files/SK-CPR-ESTEID-EN_v8_1_20171104.pdf .

[9] “The safe use of an identity card (ID card), residence card, and Digi-ID,” https://www.politsei.ee/en/nouanded/isikut-toendavad-dokumendid/index.dot.

[10] “Terms and conditions for the use of certificates of personal identification documents of the Republic of Estonia,” https://www.sk.ee/upload/files/SK-TCU-ESTEID-EN-CURRENT.pdf.

[11] “Regulation 77 of the Minister of the Interior,” (in Estonian only), https://www.riigiteataja.ee/akt/102022018002.

[12] “Consular Act,” https://www.riigiteataja.ee/en/eli/527012016004/consolide.

[13] “Regulation 62 of the Minister of the Interior, as of 01/12/2015,” (in Estonian only), https://www.riigiteataja.ee/akt/118112016005 .

[14] “Citizenship Act,” https://www.riigiteataja.ee/en/eli/513012017001/consolide.

[15] “Police and Border Guard Act,” https://www.riigiteataja.ee/en/eli/515092017001/consolide.

[16] “Statutes of the Police and Border Guard Board,” (in Estonian only), https://www.riigiteataja.ee/akt/128062017043.

[17] “International Civil Aviation Organization,” https://www.icao.int/ .

[18] “Statutes of the IT and Development Centre, Ministry of the Interior,” (in Estonian only), https://www.smit.ee/pdf/pohimaarus.pdf.

[19] “ISKE,” https://www.ria.ee/en/iske-en.html.

[20] “Statutes of the Information System Authority,” (in Estonian only), https://www.riigiteataja.ee/akt/129122016014.

[21] “Estonian Trusted List,” https://sr.riik.ee/en/tl.html.

[22] “Statutes of the Technical Regulatory Authority,” (in Estonian only), https://www.riigiteataja.ee/akt/106012017003.

[23] “ESTEID-SK qualified certificates for electronic signatures,” https://www.sk.ee/upload/files/9734UE_s_2017.pdf.

[24] “SK insurance certificate,” https://www.sk.ee/upload/files/PI%20Certificate%20-%20SK%20ID%20Solutions%20AS%20-%20signed_nimega.pdf.

[25] “Emergency Act,” https://www.riigiteataja.ee/en/eli/505012018004/consolide.

[26] “General Part of the Economic Activities Code Act,” https://www.riigiteataja.ee/en/eli/504012018003/consolide.

[27] “Trust Services Practice Statement,” https://sk.ee/upload/files/SK-PS-EN-v3_0_20170101.pdf .

[28] “State Fees Act,” https://www.riigiteataja.ee/en/eli/502012018002/consolide.

[29] “Personal Data Protection Act,” https://www.riigiteataja.ee/en/eli/507032016001/consolide.

[30] “Statutes of the Identity Documents Database,” (in Estonian only), https://www.riigiteataja.ee/akt/102022018003.

[31] “Public Information Act,” https://www.riigiteataja.ee/en/eli/516102017007/consolide .

[32] “Archives Act,” https://www.riigiteataja.ee/en/eli/504032016002/consolide .

[33] “Regulation 78 of the Minister of the Interior,” (in Estonian only), https://www.riigiteataja.ee/akt/114012017016.

[34] “Regulation 181 of the Government of the Republic as of 22/12/2011,” (in Estonian only), https://www.riigiteataja.ee/akt/113012015021?leiaKehtiv.

[35] “Civil Service Act,” https://www.riigiteataja.ee/en/eli/502012018003/consolide.

[36] “ESTEID-SK Certification Practice,” https://sk.ee/upload/files/SK-CPS-ESTEID-EN-v3_0_20171101.pdf.

[37] “Government of the Republic Act,” https://www.riigiteataja.ee/en/eli/516102017008/consolide.

[38] “Certificate Policy for Mobile ID of the Republic of Estonia,” https://sk.ee/upload/files/SK-CP-MOBILE%20ID-EN-v6_0-20171024.pdf.