Police and Border Guard Board - Certificate Policy for identity card, digital identity card, residence permit card and diplomatic identity card

Version 1.2

OID: 1.3.6.1.4.1.51361.1 (PBGB) and 1.3.6.1.4.1.51455.1 (MFA).

Effective since 08.04.2021

Version History		
Date	**Version**	**Changes/Updates/Amendments**
05.03.2021	1.2	1.1. amendments; 1.2., 1.3.2. linguistic corrections; 1.5.3., 1.6.1. amendments; 3.1.4. linguistic corrections; 4.1.2., 4.2.1. amendments; 4.2.2., 4.3.2., 4.7. linguistic corrections; 4.7.1., 4.7.2., amendments; 4.7.3., 4.7.5. linguistic corrections; 4.9.1. amendments; 4.9.2., 4.9.3., 4.9.13., 4.9.14., 4.9.17. - 4.9.19. linguistic corrections; 6.1.2., 9.6.3. amendments.
18.03.2019	1.1	1.6.1 update; 3.2.1 clarification; 3.3.1 update; 4.7 linguistic corrections; 4.7.1-3 update; 4.9.7-8 update; 7.2 update;
26.09.2018	1.0	

Table of Contents

1. Introduction

1.1. Overview

The Republic of Estonia is the issuer of identity documents (pursuant to sections 9^4 (1) and 15 (4) of the Identity Documents Act, hereinafter as IDA) that include a certificate that enables digital authentication and a certificate that enables digital signing, both of which are issued by/from the EE-GovCA2018 root certificate and the intermediate certificate. The Republic of Estonia adheres to the following official certificate hierarchy (see Figure 1):

a. The root certificate of the Republic of Estonia is the EE-GovCA2018, which issues the ESTEID2018 intermediate certificate.
b. The ESTEID2018 intermediate certificate issues a certificate that enables digital authentication and a certificate that enables digital signing (end-user certificates) entered in ID-1 format identity documents of the Republic of Estonia.

c. The ESTEID2018 intermediate certificate issues the OCSP Responder certificate, which issues information on the validity of end-user certificates.

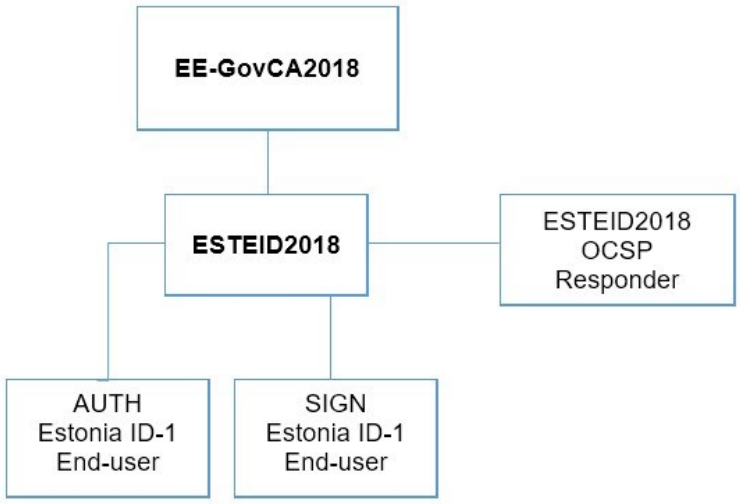

Figure 1. The official certificate hierarchy of the Republic of Estonia

This document, named "Police and Border Guard Board – Certificate Policy for identity card, digital identity card, residence permit card and diplomatic identity card" (hereinafter referred to as CP) defines procedural and operational requirements that Certification Authority adheres to and requires entities to adhere to when issuing and managing the Certificates for the following identity documents issued by the Republic of Estonia (hereinafter referred together as “Card”):

- identity card for Estonian citizen;
- identity card for European Union citizen;
- digital identity card for Estonian resident;
- digital identity card for e-resident;
- residence permit card for long-term resident;
- residence permit card for temporary residence citizen and NATO SOFA;
- residence permit card for family members of citizen of European Union;
- diplomatic identity card.

The general term “Card” SHALL be used when all the above mentioned identity documents are concerned. Any specific exceptions SHALL be described under each section separately according to the particular identity document type.

These Certificates facilitate electronic signatures and electronic identification of natural persons. The Certificates always come in pairs: each Card contains one Authentication Certificate and one Qualified Electronic Signature Certificate and their corresponding Private Keys. Each Private Key is protected by separate Activation Data (PIN code) and each Card has a single Unlock (PUK code). A single person can have only one valid Card per each Card type at any point in time. The Cards are physically shaped in ID-1 format and comply with the ISO/IEC 7816 [1] and Card Documentation [2].

According to IDA [3] Police and Board Guard Board (hereinafter PBGB) is the issuing authority of the identity documents hence is the owner of this CP. Issuing and managing Certificates for

the Card is based on the IDA [3] and Regulation (EU) N° 910/2014 [4] which establishes a legal framework for electronic signatures.

Certification Authority (hereinafter CA) is the Subcontractor of the Card Manufacturer.

This document describes only restrictions to the Policy for EU qualified Certificates issued to natural persons where the Private Key and the related Certificate reside on a QSCD (QCP-nqscd) from ETSI EN 319 411-2 [5] and Normalised Certificate Policy requiring a Secure Cryptographic Device (NCP+) from ETSI EN 319 411-1 [6].

The semantics of "no stipulation" in this document is that no additional restrictions are set and relevant provisions from QCP-n-qscd and NCP+ are applied directly.

Issuing and managing Qualified Electronic Signature Certificates for the Card is based on the requirements of the Policy QCP-n-qscd: Certificate Policy for EU qualified Certificates issued to natural persons with Private Key related to the certified Public Key in a QSCD.

Issuing and managing Authentication Certificates for the Card is based on the requirements of the Policy NCP+: Normalised Certificate Policy requiring a Secure Cryptographic Device.

The Certification Service for Qualified Electronic Signature Certificates for the Card described in this CP SHALL be qualified trust service according to the Trusted List of Estonia.

Data structures and communication protocols in use SHALL be as described in the Card Documentation [2] where applicable.

In case of conflicts, the following documents SHALL be considered in the following order (prevailing ones first):

- ETSI EN 319 411-2 [5],
- ETSI EN 319 411-1 [6],
- this CP,
- SK ID Solutions AS - ESTEID2018 Certification Practice Statement.

To preserve IETF RFC 3647 [7] outline, this CP is divided into nine parts, section headings that do not apply, are designated as **"Not applicable"**. Each top-level chapter includes references to the relevant sections in ETSI EN 319 411-1 [6] and ETSI EN 319 411-2 [5].

In this CP modal verbs in capital letters are to be interpreted as described in Clause 3.2 of the ETSI Drafting Rules [8] (Verbal forms for the expression of provisions).

Terms and acronyms listed in Clause 1.6 of this CP are written starting with a capital letter in this CP.

1.2. Document Name and Identification

Refer to Clause 5.3 of ETSI EN 319 411-1 [6] and ETSI EN 319 411-2 [5].

This document is named “Police and Border Guard Board – Certificate Policy for the identity card, digital identity card, residence permit card and diplomatic identity card". This CP is identified by two OIDs: 1.3.6.1.4.1.51361.1 and 1.3.6.1.4.1.51455.1.

OID is composed according to the contents of the following table:

Parameter	**OID reference**
Internet attribute	1.3.6.1
Private entity attribute	4
Registered business attribute given by private business manager IANA	1
PBGB attribute in IANA register	51361
MFA attribute in IANA register	51455
Certification Service attribute	1.1

The division of sub-OIDs according to the card type issued are composed according to the contents of the following table:

Card Type	**General PBGB OID**	**Sub-OID: Type (identity document = 1)**	**Sub-OID: document type**
Identity card of Estonian citizen	51361	1	1
Identity card of European Union citizen	51361	1	2
Digital identity card	51361	1	3
Digital identity card of e-resident	51361	1	4
Residence card of long term resident	51361	1	5
Residence card of temporary residence citizen	51361	1	6
Residence card of family members of citizen of European Union	51361	1	7
Diplomatic identity card	51455	1	1

Example of sub-OIDs according to the card type issued under this CP:

- Digital identity card: 1.3.6.1.4.1.51361.1.1.3
- Diplomatic identity card: 1.3.6.1.4.1.51455.1.1.1

Qualified Electronic Signature Certificate for the Card issued to Subscribers SHALL include OID's of the following policies:

- ETSI EN 319 411-2 [5] clause 5.3 c) for QCP-n-qscd: 0.4.0.194112.1.2

Itu-t(0) identified-organization(4) etsi(0) qualified-certificate-policies(194112) policy-identifiers(1) qcp-natural-qscd (2)

- OID of the certificate issuer.

Authentication Certificates for the Card issued to Subscribers SHALL include OID's of the following policies:

- ETSI EN 319 411-1 [6] clause 5.3 b) for NCP+: 0.4.0.2042.1.2

  itu-t(0) identified-organization(4) etsi(0) other-certificate-policies(2042) policyidentifiers(1) ncpplus (2)

- OID of the certificate issuer.

1.3. PKI Participants

Refer to Clause 5.4 of ETSI EN 319 411-1 [6] and ETSI EN 319 411-2 [5].

1.3.1. Certification Authorities

SK ID Solutions AS issues Certificates under this CP.

1.3.2. Registration Authorities

Pursuant to the IDA [3] the Registration Authorities (RA-s) and their responsibilities are laid down in Chapter 3 of the IDA [3]. Transfer of functions listed under IDA section 3^1 may be applied.
NOTE: The PBGB and the Ministry of Foreign Affairs (hereinafter MFA) CAN appear in multiple roles throughout the process. Throughout the rest of this CP a following distinction is made based on the role:

- both institutions are referred as RA when they are performing technical actions such as face to face authentication or delivery of the Cards (in terms of technical actions such as face to face authentication or delivery of diplomatic identity card, the MFA is solely responsible);
- they are referred to as PBGB or MFA when they are representing Republic of Estonia in the role of the Issuer of the Document according to IDA [3], during initial identification of persons or making decisions about their eligibility to apply for a Card.

1.3.3. Subscribers

Subscriber is the Subject of the Certificate issued under this CP.

Subscriber can be only a natural person entitled by IDA [3]. The IDA [3] refers to the Subscriber as “the holder of the Document”.

1.3.4. Relying Parties

Relying Parties are legal or natural persons who are making decisions based on the Certificate.

1.3.5. Other Participants

The Card Manufacturer is the Contractor of the PBGB. The Card Manufacturer manufactures and personalises the Cards only when ordered by the PBGB or the MFA, and provides the technical environment for personalisation in the RA offices.

1.4. Certificate Usage

Refer to Clause 5.5 of ETSI EN 319 411-1 [6] and ETSI EN 319 411-2 [5].

1.4.1. Appropriate Certificate Uses

Subscriber Certificates are intended for the following purposes.

Qualified Electronic Signature Certificate is intended for:

- creating Qualified Electronic Signatures compliant with eIDAS [4].

Authentication Certificate is intended for:

- Authentication,
- Encryption,
- secure e-mail.

CA Private Keys SHALL NOT be used to sign other types of Certificates except for the following:

- Subscriber Certificates compliant with QCP-n-qscd or NCP+,
- OCSP response verification Certificates,
- Internal Certificates for technical needs.

1.4.2. Prohibited Certificate Uses

Subscriber Certificates issued under this CP SHALL NOT be used for any of the following purposes:

- unlawful activity (including cyber attacks and attempt to infringe the Certificate or the Card),

- issuance of new Certificates and information regarding Certificate validity,
- enabling other parties to use the Subscriber's Private Key,
- enabling the Certificate issued for electronic signing to be used in an automated way,
- using the Certificate issued for electronic signing for any other purposes than creating a Qualified Electronic Signature, including for signing documents which can bring about unwanted consequences or signing such documents for testing purposes.

The Subscriber Authentication Certificate SHALL NOT be used to create Electronic Signatures.

1.5. Policy Administration

1.5.1. Organisation Administering the Document

This CP is administered by the PBGB.

Registry code 70008747

Pärnu mnt 139, 15060 Tallinn

Tel +372 612 3000

Email: ppa@politsei.ee

https://www.politsei.ee/en/

1.5.2. Contact Person

Service planner for identification.

Email: eid@list.politsei.ee

1.5.3. Person Determining CPS Suitability for the Policy

Policy Administrator validates and determines CPS conformity to this CP.

1.5.4. CP Approval Procedures

CP shall be reviewed annually or if significant changes occur to ensure the continuing suitability, adequacy and effectiveness of applicable standards to current policy.

Amendments which do not change the meaning of this CP, such as spelling corrections, translation activities and contact details updates, SHALL be documented in the Versions and Changes section of the present document. In this case the fractional part of the document version number SHALL be incremented.

In the case of substantial changes, the new CP version SHALL be clearly distinguishable from the previous ones, and the serial number SHALL be incremented by one. The amended CP along with the enforcement date, which cannot be earlier than 30 days after publication, SHALL be published electronically on www.id.ee website.

All amendments to this CP SHALL be coordinated with the Information System Authority (RIA), CA, MFA and the Card Manufacturer.

All amendments SHALL be approved by the service planner for identification and the head of eID Department of RIA. Amended CP SHALL be enforced by the Deputy Director of the PBGB.

1.6. Definitions and Acronyms

1.6.1. Terminology

In this CP the following terms have the following meaning.

Term	**Definition**
Authentication	Unique identification of a person by checking his/her alleged identity.
Card Manufacturer	Contractor of the PBGB who manufactures and personalises identity cards, resident permit cards and e-resident's digital identity cards as ordered by the PBGB, diplomatic identity cards as ordered by the MFA, and manufactures blank digital identity cards and provides the technical environment for the personalisation of digital identity cards in the RA offices.
Certificate	Public Key, together with additional information, laid down in the Certificate Profile [9], rendered unforgeable via encipherment using the Private Key of the Certificate Authority which issued it.
Certificate Authority	A part of the trust service provider's structure responsible for issuing and verifying electronic Certificates. SK ID Solutions AS issues Certificates under this CP.
Certificate Pair	A pair of Certificates consisting of one Authentication Certificate and one Qualified Electronic Signature Certificate.
Certificate Policy	A set of rules that indicates applicability of a specific Certificate to a particular community and/or PKI implementation with common security requirements.
Certification Practice Statement	One of the several documents that all together form the governance framework in which Certificates are created, issued, managed, and used.

Term	Definition
Certificate Profile	Document that determines the information contained within a Certificate as well as the minimal requirements towards the Certificate.
Certificate Revocation List	A list of invalid (revoked, suspended) Certificates. CRL contains suspended and revoked Certificates during their validity period, i.e. until they expire.
Certification Service	Trust service related to issuing Certificates, managing suspension, termination of suspension, revocation, modification and re-key of the Certificates.
Directory Service	Trust service related to publication of Certificate validity information.
Distinguished name	Unique Subject name in the infrastructure of Certificates.
Encrypting	Information treatment method changing the information unreadable for those who do not have necessary rights.
Card	Personal identity document in ID-1 format and issued on the basis of IDA. Cards include Estonian citizen identity cards, European Union citizen identity cards, digital identity cards for residents, digital identity cards for e-residents, residence permit cards and diplomatic identity cards.
ID-1	Format which defines physical characteristics of identification cards according to the standard ISO/IEC 7816 [1].
Integrity	A characteristic of an array: information has not been changed after the array was created.
Object Identifier	An identifier used to uniquely name an object (OID).
Personal Data File	File on Card that includes the Subscriber's personal data.
PIN code	Activation code for the Authentication Certificate and for the Qualified Electronic Signature Certificate.
Private Key	The key of a key pair that is assumed to be kept in secret by the holder of the key pair, and that is used to create electronic signatures and/or to decrypt electronic 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 holder of the corresponding Private Key and that is used by Relying Parties to verify electronic signatures created with the holder’s corresponding Private Key and/or to encrypt messages so that they can be decrypted only with the holder’s corresponding Private Key.

Term	Definition
PUK code	The code for unblocking the PIN codes when they have been blocked after number of allowed consecutive incorrect entries.
Qualified Certificate	A certificate for electronic signatures, that is issued by the qualified trust service provider and meets the requirements laid down in Annex I of the eIDAS [4] Regulation.
Qualified Electronic Signature	Advanced electronic signature that is created by a qualified electronic signature creation device, and which is based on a Qualified Certificate for electronic signatures.
Qualified Electronic Signature Creation Device	A Secure Signature Creation Device that meets the requirements laid down in eIDAS [4] Regulation.
Relying Party	Entity that relies on the information contained within a Certificate.
Registration Authority	Entity that is responsible for identification and Authentication of Subjects of Certificates. Additionally, the Registration Authority may accept Certificate applications, check the applications and/or forward the applications to the Certificate Authority.
Secure Cryptographic Device	Device, which holds the Private Key of the user, protects this key against compromise and performs signing or decryption functions on behalf of the user.
Subscriber	A natural person to whom the Certificates of the Card are issued as a public service provided that the person has a statutory right to it and has requested it.
Subject	In this document, the Subject is the same as the Subscriber.
Terms and Conditions	Document that describes obligations and responsibilities of the Subscriber with respect to using Certificates. The Subscriber has to be familiar with the document and accept the Terms and Conditions [10] upon submitting an application for a Card.

1.6.2. Acronyms

Acronym	Definition
CA	Certificate Authority
CP	Certificate Policy
CPS	Certification Practice Statement

Acronym	Definition
CRL	Certificate Revocation List
eIDAS	Regulation (EU) No 910/2014 [4] of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.
IDA	Identity Documents Act [3]
MFA	Ministry of Foreign Affairs
NCP+	Normalised Certificate Policy requiring a Secure Cryptographic Device from ETSI EN 319 411-1 [6]
OCSP	Online Certificate Status Protocol
OID	Object Identifier, a unique object identification code
PBGB	Police and Border Guard Board
PKI	Public Key Infrastructure
QSCD	Qualified Electronic Signature Creation Device
QCP-nqscd	Policy for EU qualified certificate issued to a natural person where the private key and the related certificate reside on a QSCD from ETSI EN 319 411-2 [5]
RA	Registration Authority
RIA	Information System Authority
SK	SK ID Solutions AS
SMIT	IT and development centre of the Ministry of the Interior

2. Publication and Repository Responsibilities

Refer to Clause 6.1 of ETSI EN 319 411-1 [6] and ETSI EN 319 411-2 [5].

2.1. Repositories

CA SHALL ensure that its repository is available 24 hours a day, 7 days a week with a minimum of 99% availability overall per year with a scheduled down-time that does not exceed 0,5% annually.

2.2. Publication of Certification Information

2.2.1. Publication and Notification Policies

This CP SHALL be published on the www.id.ee website and the reference SHALL be added to the CA website repository no less than 30 days prior to taking effect.

The Certification Practice Statement [11], the Certificate Profile [9], as well as the Terms and Conditions [10] with the enforcement dates SHALL be published on the CA website repository no less than 30 days prior to taking effect.

2.2.2. Items not Published in the Certification Practice Statement

Information about service levels, fees and technical details laid out in mutual agreements between the CA, PBGB and Card Manufacturer MAY be left out of CPS.

The CPS MAY not cover internal procedures of the PBGB and Card Manufacturer.

2.3. Time or Frequency of Publication

No stipulation.

2.4. Access Controls on Repositories

No stipulation.

3. Identification and Authentication

Refer to Clause 6.2 of ETSI EN 319 411-1 [6] and ETSI EN 319 411-2 [5].

3.1. Naming

The Distinguished Name of the Subscriber SHALL comply with the conventions set in the Certificate Profile [9].

3.1.1. Types of Names

No stipulation.

3.1.2. Need for Names to be Meaningful

All the values in the Subscriber information section of a Certificate SHALL be meaningful.

3.1.3. Anonymity or Pseudonymity of Subscribers

Not applicable.

3.1.4. Rules for Interpreting Various Name Forms

Pursuant to IDA [3], international letters SHALL be encoded according to ICAO transliteration rules where necessary.

3.1.5. Uniqueness of Names

PBGB and MFA SHALL ensure that Certificates with matching Common Name (CN), SerialNumber and e-mail addresses in Subject Alternative Name (SAN) fields are not issued to different Subscribers.

3.1.6. Recognition, Authentication, and Role of Trademarks

Not applicable.

3.2. Initial Identity Validation

3.2.1. Method to Prove Possession of Private Key

Private Keys SHALL be generated on the QSCD during personalisation by the Card Manufacturer. In case of digital identity card Private Keys SHALL be generated on the QSCD during personalisation by PBGB.

3.2.2. Authentication of Organisation Identity

Not applicable.

3.2.3. Authentication of Individual Identity

Authentication SHALL be carried out by RA in accordance with Chapter 3 of IDA [3], in case of e-resident's digital identity card in accordance with Chapter 5^2 of IDA [3] and in case of diplomatic identity card in accordance with Chapter 5^3 IDA [3].

3.2.4. Non-Verified Subscriber Information

Non-verified Subscriber information SHALL NOT be allowed in a Certificate.

3.2.5. Validation of Authority

Validation SHALL be carried out by RA in accordance with IDA [3].

3.2.6. Criteria for Interoperation

No stipulation.

3.3. Identification and Authentication for Re-Key Requests

3.3.1. Identification and Authentication for Routine Re-Key

Private Keys SHALL be generated and authentication SHALL be carried out according to 3.2.3.

3.3.2. Identification and Authentication for Re-Key After Revocation

No stipulation.

3.4. Identification and Authentication for Revocation Request

No stipulation.

4. Certificate Life-Cycle Operational Requirements

Refer to Clause 6.3 of ETSI EN 319 411-1 [6] and ETSI EN 319 411-2 [5].

4.1. Certificate Application

4.1.1. Who Can Submit a Certificate Application

The eligibility for persons to request a Card is defined in IDA [3]. CA SHALL accept Certificate requests only from the Card Manufacturer. The Certificate request from the Card Manufacturer SHALL include signed file as a confirmation that the request to personalise the Card is originated by either PBGB or MFA.

4.1.2. Enrolment Process and Responsibilities

The responsibilities and process for making decisions about eligibility to apply for a Certificate are laid out in IDA [3].

Upon a positive decision the PBGB or in case of the diplomatic identity card the MFA SHALL send an order to the Card Manufacturer to produce a new Card.

It is the responsibility of the Card Manufacturer to manufacture the blank Card, imprint visual elements to it, personalise the Card with the Subscriber's personal data, create the Personal Data File on the Card, generate the keypairs for Authentication and Qualified Electronic Signature on the Card and submit a pair of Certificate requests to the CA.

In case of the digital identity card for Estonian resident, the PBGB will personalise the card itself by using the technical environment and blank documents provided by the Card Manufacturer. PBGB SHALL personalise the Card with the Subscriber's personal data, create the Personal Data File on the Card, generate the keypairs for Authentication and Qualified Electronic Signature on the Card and submit a pair of Certificate requests to the Card Manufacturer.

PBGB and MFA will ensure the submitting of correct identification data (names, personal codes, dates, photo etc) to the Card Manufacturer. The Card Manufacturer and the CA will rely upon the values provided by the PBGB or MFA, no alteration of the data provided by PBGB or MFA is allowed.

SMIT is responsible for assigning the correct e-mail address in the eesti.ee domain to the Certificate for Authentication:

- re-use the previous one if the Subscriber already has an address assigned;
- generate a previously unused address according to data provided by RA.

SMIT is responsible for keeping track of e-mail address assignments.

MFA is responsible for assigning the correct e-mail address in the eesti.ee domain and keeping track of e-mail address assignments for diplomatic identity card.

4.2. Certificate Application Processing

4.2.1. Performing Identification and Authentication Functions

The Subscriber's identity SHALL be validated by the RA as described in Chapter 3 of IDA [3] and in case of e-resident's digital identity card as described in Chapter 5^2 of IDA [3].

PBGB or MFA SHALL send a Certificate application to the Card Manufacturer, who shall submit an applicable Certificate request to the CA.

CA SHALL accept Certificate requests only from the Card Manufacturer. The Certificate request submitted by the Card Manufacturer to the CA SHALL include a confirmation that the request to personalise the Card is originated by either PBGB or MFA. CA and the Card Manufacturer SHALL rely upon identification data provided by PBGB or MFA.

4.2.2. Approval or Rejection of Certificate Applications

CA SHALL refuse to issue a Certificate if the Certificate request does not comply with the following technical requirements:

- Certificate application SHALL be signed by PBGB or in case of the diplomatic identity card by MFA.
- Certificate request SHALL be sent in an encrypted form.
- Certificate request data file and data in the signed application SHALL match exactly.

If the data contained in a Certificate application needs to be modified, the corresponding amendment SHALL be coordinated with PBGB or in case of the diplomatic identity card with the MFA.

4.2.3. Time to Process Certificate Applications

In accordance with the applicable laws and agreements.

4.3. Certificate Issuance

4.3.1. CA Actions During Certificate Issuance

SMIT SHALL allocate correct and unique e-mail address in the eesti.ee domain to the Subscriber. At this stage, OCSP service SHALL NOT return response "GOOD" and the Certificate SHALL NOT be made available via the Directory Service.

4.3.2. Notifications to Subscriber by the CA of Issuance of Certificate

No stipulation.

4.4. Certificate Acceptance

4.4.1. Conduct Constituting Certificate Acceptance

No stipulation.

4.4.2. Publication of the Certificate by the CA

Certificate SHALL be published by the CA using the Directory Service immediately after the Subscriber has accepted it, OCSP SHALL start responding with "GOOD".

4.4.3. Notification of Certificate Issuance by the CA to Other Entities

No stipulation.

4.5. Key Pair and Certificate Usage

4.5.1. Subscriber Private Key and Certificate Usage

No stipulation.

4.5.2. Relying Party Public Key and Certificate Usage

No stipulation.

4.6. Certificate Renewal

Not allowed.

4.7. Certificate Re-Key

Certificate Re-Key SHALL be allowed only upon successful personal identification of the Subscriber via physical identity checks or digital Authentication methods.

During Certificate Re-Key the Certificates to be replaced SHALL be revoked.

Certificate Re-Key MAY be done upon initial application in the case of the Card manufacturing errors before acceptance of the Certificates or to replace a defective Card. In either case only the last Certificates SHALL be written to the Card and remain valid. All the erroneous or unusable Certificates SHALL be revoked immediately.

4.7.1. Circumstances for Certificate Re-Key

This CP treats recurring Certificate application the same way as initial Card application. The Subscriber’s application for a recurring Certificate SHALL be processed as an application for a new Card and either physical or digital Authentication SHALL be conducted.

Certificate Re-Key is allowed:

- to replace an expired or defective Card;
- to fix production errors that are discovered during quality checks;

- when applying for a recurring Card.

In case the Subscriber claims the card is defective then the person is requested to submit a warranty claim and Certificate Re-Key is done upon initial Certificate application.

4.7.2. Who May Request Certification of a New Public Key

Re-Key MAY be requested by Subscriber, PBGB, MFA (in case of diplomatic identity card) or Card Manufacturer.

Subscriber MAY request Re-Key in case of initial Certificate application or to replace a defective Card.

PBGB MAY request Re-Key of all the Cards (except diplomatic identity card) to replace a defective Card and in case of the digital identity cards for residents if the need to replace the Certificate is discovered during quality checks before delivery of the Card to the Subscriber.

MFA MAY request Re-Key of diplomatic identity card to replace a defective Card.

Card Manufacturer MAY request Re-Key of all the Cards except the digital identity cards for residents, if the need to replace the Certificate is discovered during quality checks before delivery of the Card to the PBGB or MFA.

CA SHALL NOT accept Re-Key requests from any other party than the Card Manufacturer following a Certificate application signed by either PBGB or MFA.

4.7.3. Processing Certificate Re-Key Requests

If the Re-Key is to replace an expired or defective Card or to apply for a recurring Card, the process is similar to initial issuance.

If the Card needs to be replaced because it is defective then the warranty claim is treated as the Certificate application and Certificate Re-Key is done upon initial Certificate application. With the warranty claim the person MUST agree to the Terms and Conditions [10] applicable at the moment of the claim in a written format.

4.7.4. Notification of New Certificate Issuance to Subscriber

No stipulation.

4.7.5. Conduct Constituting Acceptance of a Re-Keyed Certificate

No stipulation.

4.7.6. Publication of the Re-Keyed Certificate by the CA

Refer to Clause 4.4.2 of this CP.

4.7.7. Notification of Certificate Issuance by the CA to Other Entities

No stipulation.

4.8. Certificate Modification

Not allowed.

4.8.1. Circumstances for Certificate Modification

Not allowed.

4.8.2. Who May Request Certificate Modification

Not allowed.

4.8.3. Processing Certificate Modification Requests

Not allowed.

4.8.4. Notification of New Certificate Issuance to Subscriber

Not allowed.

4.8.5. Conduct Constituting Acceptance of Modified Certificate

Not allowed.

4.8.6. Publication of the Modified Certificate by the CA

Not allowed.

4.8.7. Notification of Certificate Issuance by the CA to Other Entities

Not allowed.

4.9. Certificate Revocation and Suspension

4.9.1. Circumstances for Revocation

Circumstances for Certificate revocation SHALL be as laid down in IDA [3] and section 19 of the Electronic Identification and Trust Services for Electronic Transactions Act [12].

In case the Card does not pass the quality check and a new card is personalised to replace the Card, the Manufacturer or PBGB SHALL be allowed to request the revocation of the Certificates of the Card that has not passed the quality check.

4.9.2. Who Can Request Revocation

Entities eligible to request Certificate revocation SHALL be as laid down in IDA [3] and section 19 of the Electronic Identification and Trust Services for Electronic Transactions Act [12].

In case the Card does not pass the quality check and a new card is manufactured to replace the Card the Manufacturer or PBGB SHALL be allowed to request the revocation of the Certificates of the Card that has not passed the quality check.

4.9.3. Procedure for Revocation Request

The procedure for revocation request for issued Cards SHALL be as laid down in IDA [3] and section 20 of the Electronic Identification and Trust Services for Electronic Transactions Act [12].

If the new Certificate request is sent to CA and the Card has not been issued then CA SHALL revoke the previously generated certificate.

4.9.4. Revocation Request Grace Period

No stipulation.

4.9.5. Time within Which CA Must Process the Revocation Request

No stipulation.

4.9.6. Revocation Checking Requirements for Relying Parties

No stipulation.

4.9.7. CRL Issuance Frequency

No stipulation.

4.9.8. Maximum Latency for CRLs

No stipulation.

4.9.9. On-Line Revocation/Status Checking Availability

No stipulation.

4.9.10. On-Line Revocation Checking Requirements

No stipulation.

4.9.11. Other Forms of Revocation Advertisements Available

No stipulation.

4.9.12. Special Requirements Related to Key Compromise

No stipulation.

4.9.13. Circumstances for Suspension

Circumstances for Certificate suspension SHALL be as laid down in IDA [3] and section 17 of the Electronic Identification and Trust Services for Electronic Transactions Act [12].

4.9.14. Who Can Request Suspension

Entities eligible to request Certificate suspension SHALL be as laid down in IDA [3] and section 17 of the Electronic Identification and Trust Services for Electronic Transactions Act [12].

4.9.15. Procedure for Suspension Request

It SHALL be possible to request Certificate suspension via phone 24 hours a day, 7 days a week. Certificate suspension SHALL leave a uniquely identifiable trace.

4.9.16. Limits on Suspension Period

No limits.

4.9.17. Circumstances for Termination of Suspension

Circumstances for termination of Certificate suspension SHALL be as laid down in IDA [3] and section 18 of the Electronic Identification and Trust Services for Electronic Transactions Act [12].

4.9.18. Who can request Termination of Suspension

Entities who can request termination of Certificate suspension SHALL be as laid down in IDA [3] and section 18 of the Electronic Identification and Trust Services for Electronic Transactions Act [12].

4.9.19. Procedure for Termination of Suspension

The procedure for termination of Certificate suspension SHALL be as laid down in IDA [3] and section 18 of the Electronic Identification and Trust Services for Electronic Transactions Act [12].

4.10. Certificate Status Services

4.10.1. Operational Characteristics

No stipulation.

4.10.2. Service Availability

CA SHALL ensure that the Certificate Status Services are available 24 hours a day, 7 days a week with a minimum of 99% availability overall per year with a scheduled down-time that does not exceed 0,5% annually.

4.10.3. Operational Features

No stipulation.

4.11. End of Subscription

No stipulation.

4.12. Key Escrow and Recovery

4.12.1. Key Escrow and Recovery Policy and Practices

Not allowed.

4.12.2. Session Key Encapsulation and Recovery Policy and Practices

Not applicable.

5. Facility, Management, and Operational Controls

Refer to Clause 6.4 of ETSI EN 319 411-1 [6] and ETSI EN 319 411-2 [5].

6. Technical Security Controls

Refer to Clause 6.5 of ETSI EN 319 411-1 [6] and ETSI EN 319 411-2 [5].

6.1. Key Pair Generation and Installation

6.1.1. Key Pair Generation

The Subscriber Certificate keys SHALL be generated using the QSCD by one of the following roles:

- Card Manufacturer,
- PBGB.

6.1.2. Private Key Delivery to Subscriber

Private keys SHALL be delivered on a QSCD inside a sealed envelope that SHALL be handed over to the RA by the Card Manufacturer.

RA, in turn, SHALL deliver it unopened to the Subscriber.

6.1.3. Public Key Delivery to Certificate Issuer

The Card Manufacturer SHALL deliver the Public Key to the CA using a secure communication channel.

6.1.4. CA Public Key Delivery to Relying Parties

No stipulation.

6.1.5. Key Sizes

Allowed key sizes SHALL be as described in the Certificate Profile [9].

6.1.6. Public Key Parameters Generation and Quality Checking

No stipulation.

6.1.7. Key Usage Purposes (as per X.509 v3 Key Usage Field)

Allowed key usage flags SHALL be set as described in the Certificate Profile [9].

6.2. Private Key Protection and Cryptographic Module Engineering Controls

6.2.1. Cryptographic Module Standards and Controls

Private Key SHALL be generated on a QSCD.

6.2.2. Private Key (n out of m) Multi-Person Control

No stipulation.

6.2.3. Private Key Escrow

No stipulation.

6.2.4. Private Key Backup

No stipulation.

6.2.5. Private Key Archival

No stipulation.

6.2.6. Private Key Transfer Into or From a Cryptographic Module

No stipulation.

6.2.7. Private Key Storage on Cryptographic Module

No stipulation.

6.2.8. Method of Activating Private Key

The Subscriber SHALL be prompted to enter the PIN code of the Authentication Certificate at least once after the Card has been inserted into the card reader device.

The Subscriber SHALL be prompted to enter the PIN code of the Qualified Electronic Signature Certificate before every single operation done with the corresponding Private Key.

It SHALL be possible to create different PIN codes for different keys of the Subscriber.

The length of the PIN codes SHALL be at least:

- for the Authentication Key 4 numbers,
- for the signature Key 5 numbers,
- The PUK code SHALL be at least 8 numbers.

6.2.9. Method of Deactivating Private Key

No stipulation.

6.2.10. Method of Destroying Private Key

No stipulation.

6.2.11. Cryptographic Module Rating

No stipulation.

6.3. Other Aspects of Key Pair Management

6.3.1. Public Key Archival

No stipulation.

6.3.2. Certificate Operational Periods and Key Pair Usage Periods

Validity period of the Subscriber Certificate SHALL NOT exceed the validity period of the corresponding Card for which it was issued.

6.4. Activation Data

6.4.1. Activation Data Generation and Installation

The initial activation PIN codes SHALL be generated by the Card Manufacturer and SHALL be included in a separate sealed envelope for delivery to the Subscriber. Copies of the PIN codes SHALL NOT be stored by the Card Manufacturer or any other entity involved in the process.

The Card Manufacturer SHALL produce replacement PIN codes and PUK code and SHALL hand them over to RA in sealed envelopes. The mechanism for replacing the PIN codes and PUK code SHALL ensure by technical means the impossibility to view or store the replacement PIN codes and PUK code by the RA employee during the whole process.

RA SHALL issue replacement PIN codes and PUK code to the Subscriber when the PIN codes and PUK code need to be replaced or updated.

All PIN codes and PUK code of a single Card SHALL be replaced at once.

Prior to issuing replacement PIN codes and PUK code the RA SHALL Authenticate the Subscriber.

6.4.2. Activation Data Protection

PIN codes and PUK code SHALL be handed over personally to the Subscriber by the RA.

Copies of the PIN codes and PUK code SHALL NOT be stored by the RA.

6.4.3. Other Aspects of Activation Data

No stipulation.

6.5. Computer Security Controls

6.5.1. Specific Computer Security Technical Requirements

No stipulation.

6.5.2. Computer Security Rating

No stipulation.

6.6. Life Cycle Technical Controls

6.6.1. System Development Controls

No stipulation.

6.6.2. Security Management Controls

No stipulation.

6.6.3. Life Cycle Security Controls

No stipulation.

6.7. Network Security Controls

No stipulation.

6.8. Time-Stamping

No stipulation.

7. Certificate, CRL, and OCSP Profiles

Refer to Clause 6.6 of ETSI EN 319 411-1 [6] and ETSI EN 319 411-2 [5].

7.1. Certificate Profile

The Certificate SHALL comply with the profile described in the Certificate Profile [9].

7.2. CRL Profile

The CRL SHALL comply with the profile described in the Certificate Profile [9].

7.3. OCSP Profile

The OCSP responses SHALL comply with the profile described in the Certificate Profile [9].

8. Compliance Audit and Other Assessments

Refer to Clause 6.7 of ETSI EN 319 411-1 [6] and ETSI EN 319 411-2 [5].

9. Other Business and Legal Matters

Refer to Clause 6.8 of ETSI EN 319 411-1 [6] and ETSI EN 319 411-2 [5].

9.1. Fees

9.1.1. Certificate Issuance or Renewal Fees

No stipulation.

9.1.2. Certificate Access Fees

No stipulation.

9.1.3. Revocation or Status Information Access Fees

No stipulation.

9.1.4. Fees for Other Services

No stipulation.

9.1.5. Refund Policy

No stipulation.

9.2. Financial Responsibility

9.2.1. Insurance Coverage

No stipulation.

9.2.2. Other Assets

No stipulation.

9.2.3. Insurance or Warranty Coverage for End-Entities

No stipulation.

9.3. Confidentiality of Business Information

No stipulation.

9.4. Privacy of Personal Information

9.4.1. Privacy Plan

No stipulation.

9.4.2. Information Treated as Private

No stipulation.

9.4.3. Information Not Deemed Private

No stipulation.

9.4.4. Responsibility to Protect Private Information

No stipulation.

9.4.5. Notice and Consent to Use Private Information

No stipulation.

9.4.6. Disclosure Pursuant to Judicial or Administrative Process

No stipulation.

9.4.7. Other Information Disclosure Circumstances

No stipulation.

9.5. Intellectual Property rights

PBGB obtains intellectual property rights to this CP.

9.6. Representations and Warranties

9.6.1. CA Representations and Warranties

An employee of CA SHALL NOT have been convicted for an intentional crime.

9.6.2. RA Representations and Warranties

An employee of RA SHALL NOT have been convicted for an intentional crime.

9.6.3. Subscriber Representations and Warranties

The Subscriber warrants to complying with the Terms and Conditions [10] agreed to upon submitting an application for a Card.

9.6.4. Relying Party Representations and Warranties

Relying Party SHALL verify the validity of the Certificate using validation services offered by CA prior to relying on the Certificate.

Relying Party SHALL consider the limitations stated in the Certificate and SHALL ensure that the transaction to be accepted corresponds to this CP.

9.6.5. Representations and Warranties of Other Participants

An employee of the Card Manufacturer SHALL NOT have been punished for an intentional crime.

9.7. Disclaimers of Warranties

No stipulation.

9.8. Limitations of Liability

No stipulation.

9.9. Indemnities

No stipulation.

9.10. Term and Termination

9.10.1. Term

Refer to Clause 2.2.1 Publication and Notification Policies of this CP.

9.10.2. Termination

This CP SHALL remain in force until it is replaced by the new version or when the service is terminated upon the request of the RA and all the Certificates therefore become invalid.

9.10.3. Effect of Termination and Survival

PBGB SHALL communicate the conditions and effect of termination of this CP.

9.11. Individual Notices and Communications with Participants

No stipulation.

9.12. Amendments

9.12.1. Procedure for Amendment

Refer to Clause 1.5.4 of this CP.

9.12.2. Notification Mechanism and Period

Refer to Clause 1.5.4 of this CP.

9.13. Dispute Resolution Provisions

No stipulation.

9.14. Governing Law

This CP is governed by the jurisdictions of the European Union and Estonia.

9.15. Compliance with Applicable Law

CA SHALL ensure compliance with the following requirements:

- eIDAS [4] - Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC,
- GDPR [13] - 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 repealing Directive 95/46/EC,
- Electronic Identification and Trust Services for Electronic Transactions Act [12],
- Identity Documents Act [3],
- State Fees Act [14],
- Personal Data Protection Act [15],
- Emergency Act [16],
- Consular Act [17],
- Cybersecurity Act [18].

- related European Standards:
- ETSI EN 319 401 Electronic Signatures and Infrastructures (ESI); General Policy Requirements for trust service providers [19],
- ETSI EN 319 411-1 Electronic Signatures and Infrastructures (ESI); Policy and Security requirements for trust service providers issuing certificates; Part 1: General requirements [6],
- ETSI EN 319 411-2 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers issuing certificates; Part 2: Policy requirements for certification authorities issuing qualified certificates [5],
- EN 419 211 Protection profiles for secure signature creation device [20].

9.16. Miscellaneous Provisions

9.16.1. Entire Agreement

No stipulation.

9.16.2. Assignment

No stipulation.

9.16.3. Severability

No stipulation.

9.16.4. Enforcement (Attorney's Fees and Waiver of Rights)

No stipulation.

9.16.5. Force Majeure

No stipulation.

9.17. Other Provisions

Not allowed.

10. References

[1] “ISO/IEC 7816, Parts 1-4, published:,” http://iso.org;.

[2] “Card Documentation, published: www.id.ee”.

[3] “Identity Documents Act, RT I 1999, 25, 365, published:” https://www.riigiteataja.ee/en/eli/521062017003/consolide.

[4] “eIDAS - Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, published:,” http://eurlex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2014.257.01.0073.01.ENG.

[5] “ETSI EN 319 411-2 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates”.

[6] “ETSI EN 319 411-1 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements”.

[7] “RFC 3647 – Request For Comments 3647, Internet X.509 Public Key Infrastructure, Certificate Policy and Certification Practices Framework, published: https://www.ietf.org/rfc/rfc3647.txt;”.

[8] “ETSI Drafting Rules (Verbal forms for the expression of provisions);”.

[9] “Certificate, CRL and OCSP Profile for ID-1 format identity documents issued by the Republic of Estonia, published: https://sk.ee/en/repository/profiles/;”.

[10] “Terms and Conditions for ID-1 Format Identity Documents of the Republic of Estonia,,” published: https://sk.ee/en/repository/conditions-for-use-of-certificates/;.

[11] “SK ID Solutions AS - ESTEID2018 Certification Practice Statement, published: https://sk.ee/en/repository/CPS/”.

[12] “Electronic Identification and Trust Services for Electronic Transactions Act, 26.10.2016, published: https://www.riigiteataja.ee/en/eli/527102016001/consolide/current;”.

[13] “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 repealing Directive 95/46/EC,,” published: http://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32016R0679.

[14] “State Fees Act, published: https://www.riigiteataja.ee/en/eli/ee/519022016005/consolide/current;”.

[15] “Personal Data Protection Act, 16.01.2016, published: https://www.riigiteataja.ee/en/eli/507032016001/consolide/current;”.

[16] “Emergency Act, RT I, 03.03.2017, 1 published: https://www.riigiteataja.ee/en/eli/505012018004/consolide;”. [17] “Consular Act, RT I 2009, 29, 175, published: https://www.riigiteataja.ee/en/eli/527012016004/consolide;”.

[18] “Cybersecurity Act,” https://www.riigiteataja.ee/en/eli/523052018003/consolide.

[19] “ETSI EN 319 401 Electronic Signatures and Infrastructures (ESI); General Policy Requirements for trust service providers;”.

[20] “ETSI EN 419 211 Protection profiles for secure signature creation device;”.