

# Certificate Policy for ID-1 format identity documents of the Republic of Estonia (eID CP)

Version 1.1

OID: 1.3.6.1.4.1.51361.2 (PBGB) and 1.3.6.1.4.1.51455.2 (MFA)

Effective since: 15.10.2025

Version History		
Date	Version	Changes/Updates/Amendments
27.05.2025	1.1	<p>Added the term “Subject” and updated the terms “Subscriber” and “Subscriber Certificates” in 1.6.1. Amended the terms throughout the eID CP accordingly.</p> <p>Removed references to EUTS from 4.9 in regard to revocation of Subscriber Certificates. Removed word expired from 4.9.11 in regard to revocation status of Subscriber Certificates.</p> <p>Added an effective since date to the eID CP.</p>
21.02.2025	1.0	

## Table of Contents

1. Introduction .....	8
1.1. Overview .....	8
1.2. Document Name and Identification .....	9
1.3. PKI Participants .....	11
1.3.1. Certification Authorities .....	11
1.3.2. Registration Authorities .....	11
1.3.3. Subscribers .....	12
1.3.4. Relying Parties .....	12
1.3.5. Other Participants .....	12
1.4. Certificate Usage .....	12
1.4.1. Appropriate Certificate Uses .....	12
1.4.2. Prohibited Certificate Uses .....	13
1.5. Policy Administration .....	13
1.5.1. Organisation Administering the Document .....	13
1.5.2. Contact Person .....	13
1.5.3. Person Determining CPS Suitability for the Policy .....	13
1.5.4. CP Approval Procedures .....	13
1.6. Definitions and Acronyms .....	14
1.6.1. Terminology .....	14
1.6.2. Acronyms .....	16
2. Publication and Repository Responsibilities .....	16
2.1. Repositories .....	17
2.2. Publication of Certification Information .....	17
2.2.1. Publication and Notification Policies .....	17
2.2.2. Items not Published in the Certification Practice Statement .....	17
2.3. Time or Frequency of Publication .....	17
2.4. Access Controls on Repositories .....	17
3. Identification and Authentication .....	18
3.1. Naming .....	18
3.1.1. Types of Names .....	18
3.1.2. Need for Names to be Meaningful .....	18
3.1.3. Anonymity or Pseudonymity of Subscribers .....	18
3.1.4. Rules for Interpreting Various Name Forms .....	18
3.1.5. Uniqueness of Names .....	18
3.1.6. Recognition, Authentication, and Role of Trademarks .....	18
3.2. Initial Identity Validation .....	18
3.2.1. Method to Prove Possession of Private Key .....	18
3.2.2. Authentication of Organisation Identity .....	18
3.2.3. Authentication of Individual Identity .....	18
3.2.4. Non-Verified Subscriber Information .....	18
3.2.5. Validation of Authority .....	19
3.2.6. Criteria for Interoperation .....	19
3.3. Identification and Authentication for Re-Key Requests .....	19
3.3.1. Identification and Authentication for Routine Re-Key .....	19
3.3.2. Identification and Authentication for Re-Key After Revocation .....	19
3.4. Identification and Authentication for Revocation Request .....	19
4. Certificate Life-Cycle Operational Requirements .....	19

4.1. Certificate Application.....	19
4.1.1. Who Can Submit a Certificate Application .....	19
4.1.2. Enrolment Process and Responsibilities .....	19
4.2. Certificate Application Processing.....	20
4.2.1. Performing Identification and Authentication Functions.....	20
4.2.2. Approval or Rejection of Certificate Applications .....	20
4.2.3. Time to Process Certificate Applications .....	20
4.3. Certificate Issuance.....	20
4.3.1. CA Actions During Certificate Issuance.....	20
4.3.2. Notifications to Subscriber by the CA of Issuance of Certificate.....	20
4.4. Certificate Acceptance.....	20
4.4.1. Conduct Constituting Certificate Acceptance.....	20
4.4.2. Publication of the Certificate by the CA .....	20
4.4.3. Notification of Certificate Issuance by the CA to Other Entities.....	20
4.5. Key Pair and Certificate Usage.....	21
4.5.1. Subscriber Private Key and Certificate Usage.....	21
4.5.2. Relying Party Public Key and Certificate Usage .....	21
4.6. Certificate Renewal .....	21
4.6.1. Circumstance for Certificate Renewal.....	21
4.6.2. Who May Request Renewal .....	21
4.6.3. Processing Certificate Renewal Requests .....	21
4.6.4. Notification of New Certificate Issuance to Subscriber .....	21
4.6.5. Conduct Constituting Acceptance of a Renewal Certificate .....	21
4.6.6. Publication of the Renewal Certificate by the CA .....	21
4.6.7. Notification of Certificate Issuance by the CA to Other Entities.....	21
4.7. Certificate Re-Key .....	22
4.7.1. Circumstance for Certificate Re-Key.....	22
4.7.2. Who May Request Certification of a New Public Key .....	22
4.7.3. Processing Certificate Re-Keying Requests .....	22
4.7.4. Notification of New Certificate Issuance to Subscriber.....	22
4.7.5. Conduct Constituting Acceptance of a Re-Keyed Certificate .....	22
4.7.6. Publication of the Re-Keyed Certificate by the CA.....	22
4.7.7. Notification of Certificate Issuance by the CA to Other Entities.....	22
4.8. Certificate Modification.....	22
4.8.1. Circumstance for Certificate Modification .....	22
4.8.2. Who May Request Certificate Modification.....	22
4.8.3. Processing Certificate Modification Requests .....	22
4.8.4. Notification of New Certificate Issuance to Subscriber.....	23
4.8.5. Conduct Constituting Acceptance of Modified Certificate.....	23
4.8.6. Publication of the Modified Certificate by the CA .....	23
4.8.7. Notification of Certificate Issuance by the CA to Other Entities.....	23
4.9. Certificate Revocation and Suspension .....	23
4.9.1. Circumstances for Revocation .....	23
4.9.2. Who Can Request Revocation .....	24
4.9.3. Procedure for Revocation Request.....	24
4.9.4. Revocation Request Grace Period .....	24
4.9.5. Time Within Which CA Must Process the Revocation Request.....	24
4.9.6. Revocation Checking Requirement for Relying Parties .....	24

4.9.7. CRL Issuance Frequency .....	24
4.9.8. Maximum Latency for CRLs .....	24
4.9.9. On-Line Revocation/Status Checking Availability.....	24
4.9.10. On-Line Revocation Checking Requirements .....	25
4.9.11. Other Forms of Revocation Advertisements Available .....	25
4.9.12. Special Requirements re Key Compromise .....	25
4.9.13. Circumstances for Suspension .....	25
4.9.14. Who Can Request Suspension .....	25
4.9.15. Procedure for Suspension Request.....	25
4.9.16. Limits on Suspension Period .....	25
4.9.17. Circumstances for Termination of Suspension.....	25
4.9.18. Who can Request Termination of Suspension .....	25
4.9.19. Procedure for Termination of Suspension .....	25
4.10. Certificate Status Services .....	25
4.10.1. Operational Characteristics.....	25
4.10.2. Service Availability .....	25
4.10.3. Optional Features.....	26
4.11. End of Subscription .....	26
4.12. Key Escrow and Recovery.....	26
4.12.1. Key Escrow and Recovery Policy and Practices .....	26
4.12.2. Session Key Encapsulation and Recovery Policy and Practices.....	26
5. Facility, Management, and Operational Controls.....	26
5.1. Physical Controls .....	26
5.1.1. Site Location and Construction .....	26
5.1.2. Physical Access .....	26
5.1.3. Power and Air Conditioning.....	26
5.1.4. Water Exposures.....	26
5.1.5. Fire Prevention and Protection .....	26
5.1.6. Media Storage.....	26
5.1.7. Waste Disposal .....	26
5.1.8. Off-Site Backup.....	26
5.2. Procedural Controls .....	27
5.2.1. Trusted Roles .....	27
5.2.2. Number of Persons Required per Task.....	27
5.2.3. Identification and Authentication for Each Role .....	27
5.2.4. Roles Requiring Separation of Duties .....	27
5.3. Personnel Controls.....	27
5.3.1. Qualifications, Experience, and Clearance Requirements.....	27
5.3.2. Background Check Procedures.....	27
5.3.3. Training Requirements .....	27
5.3.4. Retraining Frequency and Requirements .....	27
5.3.5. Job Rotation Frequency and Sequence.....	27
5.3.6. Sanctions for Unauthorized Actions.....	27
5.3.7. Independent Contractor Requirements .....	27
5.3.8. Documentation Supplied to Personnel .....	27
5.4. Audit Logging Procedures.....	27
5.4.1. Types of Events Recorded.....	28
5.4.2. Frequency of Processing Log .....	28

5.4.3. Retention Period for Audit Log .....	28
5.4.4. Protection of Audit Log .....	28
5.4.5. Audit Log Backup Procedures .....	28
5.4.6. Audit Collection System (Internal vs. External) .....	28
5.4.7. Notification to Event-Causing Subject .....	28
5.4.8. Vulnerability Assessments .....	28
5.5. Records Archival .....	28
5.5.1. Types of Records Archived .....	28
5.5.2. Retention Period for Archive .....	28
5.5.3. Protection of Archive .....	28
5.5.4. Archive Backup Procedures .....	28
5.5.5. Requirements for Time-Stamping of Records .....	28
5.5.6. Archive Collection System (Internal or External) .....	28
5.5.7. Procedures to Obtain and Verify Archive Information .....	29
5.6. Key Changeover .....	29
5.7. Compromise and Disaster Recovery .....	29
5.7.1. Incident and Compromise Handling Procedures .....	29
5.7.2. Computing Resources, Software, and/or Data Are Corrupted .....	29
5.7.3. Entity Private Key Compromise Procedures .....	29
5.7.4. Business Continuity Capabilities After a Disaster .....	29
5.8. CA or RA Termination .....	29
6. Technical Security Controls .....	29
6.1. Key Pair Generation and Installation .....	29
6.1.1. Key Pair Generation .....	29
6.1.2. Private Key Delivery to Subscriber .....	29
6.1.3. Public Key Delivery to Certificate Issuer .....	29
6.1.4. CA Public Key Delivery to Relying Parties .....	29
6.1.5. Key Sizes .....	30
6.1.6. Public Key Parameters Generation and Quality Checking .....	30
6.1.7. Key Usage Purposes (as per X.509 v3 Key Usage Field) .....	30
6.2. Private Key Protection and Cryptographic Module Engineering Controls .....	30
6.2.1. Cryptographic Module Standards and Controls .....	30
6.2.2. Private Key (n out of m) Multi-Person Control .....	30
6.2.3. Private Key Escrow .....	30
6.2.4. Private Key Backup .....	30
6.2.5. Private Key Archival .....	30
6.2.6. Private Key Transfer Into or From a Cryptographic Module .....	30
6.2.7. Private Key Storage on Cryptographic Module .....	30
6.2.8. Method of Activating Private Key .....	30
6.2.9. Method of Deactivating Private Key .....	30
6.2.10. Method of Destroying Private Key .....	31
6.2.11. Cryptographic Module Rating .....	31
6.3. Other Aspects of Key Pair Management .....	31
6.3.1. Public Key Archival .....	31
6.3.2. Certificate Operational Periods and Key Pair Usage Periods .....	31
6.4. Activation Data .....	31
6.4.1. Activation Data Generation and Installation .....	31
6.4.2. Activation Data Protection .....	31

6.4.3. Other Aspects of Activation Data.....	31
6.5. Computer Security Controls.....	31
6.5.1. Specific Computer Security Technical Requirements .....	32
6.5.2. Computer Security Rating .....	32
6.6. Life Cycle Technical Controls.....	32
6.6.1. System Development Controls .....	32
6.6.2. Security Management Controls .....	32
6.6.3. Life Cycle Security Controls .....	32
6.7. Network Security Controls.....	32
6.8. Time-Stamping .....	32
7. Certificate, CRL, and OCSP Profiles.....	32
7.1. Certificate Profile.....	32
7.1.1. Version Number(s) .....	32
7.1.2. Certificate Extensions.....	32
7.1.3. Algorithm Object Identifiers .....	32
7.1.4. Name Forms .....	33
7.1.5. Name Constraints .....	33
7.1.6. Certificate Policy Object Identifier .....	33
7.1.7. Usage of Policy Constraints Extension .....	33
7.1.8. Policy Qualifiers Syntax and Semantics.....	33
7.1.9. Processing Semantics for the Critical Certificate Policies Extension .....	33
7.2. CRL Profile.....	33
7.2.1. Version Number(s) .....	33
7.2.2. CRL and CRL Entry Extensions .....	33
7.3. OCSP Profile .....	33
7.3.1. Version Number(s) .....	33
7.3.2. OCSP Extensions.....	33
8. Compliance Audit and Other Assessments .....	33
8.1. Frequency or Circumstances of Assessment .....	33
8.2. Identity/Qualifications of Assessor .....	33
8.3. Assessor's Relationship to Assessed Entity.....	34
8.4. Topics Covered by Assessment.....	34
8.5. Actions Taken as a Result of Deficiency .....	34
8.6. Communication of Results .....	34
9. Other Business and Legal Matters .....	34
9.1. Fees.....	34
9.1.1. Certificate Issuance or Renewal Fees .....	34
9.1.2. Certificate Access Fees .....	34
9.1.3. Revocation or Status Information Access Fees.....	34
9.1.4. Fees for Other Services.....	34
9.1.5. Refund Policy .....	35
9.2. Financial Responsibility .....	35
9.2.1. Insurance Coverage .....	35
9.2.2. Other Assets.....	35
9.2.3. Insurance or Warranty Coverage for End-Entities.....	35
9.3. Confidentiality of Business Information.....	35
9.3.1. Scope of Confidential Information.....	35
9.3.2. Information Not Within the Scope of Confidential Information.....	35

9.3.3. Responsibility to Protect Confidential Information .....	35
9.4. Privacy of Personal Information .....	35
9.4.1. Privacy Plan .....	35
9.4.2. Information Treated as Private.....	35
9.4.3. Information Not Deemed Private.....	35
9.4.4. Responsibility to Protect Private Information.....	36
9.4.5. Notice and Consent to Use Private Information .....	36
9.4.6. Disclosure Pursuant to Judicial or Administrative Process.....	36
9.4.7. Other Information Disclosure Circumstances.....	36
9.5. Intellectual Property rights.....	36
9.6. Representations and Warranties .....	36
9.6.1. CA Representations and Warranties .....	36
9.6.2. RA Representations and Warranties .....	36
9.6.3. Subscriber Representations and Warranties.....	36
9.6.4. Relying Party Representations and Warranties.....	36
9.6.5. Representations and Warranties of Other Participants.....	36
9.7. Disclaimers of Warranties .....	36
9.8. Limitations of Liability.....	36
9.9. Indemnities .....	36
9.10. Term and Termination .....	37
9.10.1. Term .....	37
9.10.2. Termination .....	37
9.10.3. Effect of Termination and Survival .....	37
9.11. Individual Notices and Communications with Participants.....	37
9.12. Amendments.....	37
9.12.1. Procedure for Amendment.....	37
9.12.2. Notification Mechanism and Period .....	37
9.12.3. Circumstances Under Which OID Must be Changed.....	37
9.13. Dispute Resolution Provisions .....	37
9.14. Governing Law .....	37
9.15. Compliance with Applicable Law .....	37
9.16. Miscellaneous Provisions .....	38
9.16.1. Entire Agreement.....	38
9.16.2. Assignment .....	38
9.16.3. Severability.....	39
9.16.4. Enforcement (Attorney's Fees and Waiver of Rights) .....	39
9.16.5. Force Majeure.....	39
9.17. Other Provisions .....	39
References .....	39

# 1. Introduction

This document defines the Certificate Policy for ID-1 format identity documents of the Republic of Estonia (hereinafter *eID CP*). The *eID CP* stipulates the procedural and operational requirements that the Certification Authority (CA) adheres to, and requires other entities to adhere to, when issuing and servicing certificates that enable encryption as well as authentication and certificates that enable creation of qualified electronic signatures with ID-1 format identity documents (hereinafter *Documents*) pursuant to the Identity Documents Act (*IDA*) [1].

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, as amended by Regulation (EU) 2024/1183 (*eIDAS Regulation*) [2], establishes the legal framework for certification and qualified trust services for the Republic of Estonia.

The Police and Border Guard Board (*PBGB*) or the Ministry of Foreign Affairs (*MFA*) is the issuer of Documents in the Republic of Estonia.

The PBGB is the issuer of the following Documents:

- identity card;
- e-resident's digital identity card;
- residence permit card.

The MFA is the issuer of the following Documents:

- diplomatic identity cards.

Pursuant to the IETF RFC 3647 [3], the *eID CP* is divided into nine parts. To preserve the outline specified by IETF RFC 3647 [3], section headings that do not apply have the statement "Not applicable". The *eID CP* is based on QCP-n-qscd policy defined in ETSI EN 319 411-2 [4] and NCP+ policy defined in ETSI EN 319 411-1 [5]. The semantics of "no stipulation" in the *eID CP* refers that no additional restrictions are set out in the *eID CP*; restrictions may be set out in other contractual documentation and relevant provisions from applicable standards and regulations as outlined throughout the *eID CP* shall apply.

The implementation of the *eID CP* shall be described in the Certification Practice Statement (hereinafter *eID CPS*) by the CA.

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

- *eIDAS Regulation* [2];
- ETSI EN 319 411-2 [4] and/or ETSI EN 319 411-1 [5];
- *eID CP*;
- *eID CPS*.

## 1.1. Overview

The root CA is the national trust anchor for managing and servicing the lifecycle of intermediate CA's certificates in order to provide certification and qualified trust services for the Republic of Estonia. A self-signed root certificate identifies the root CA. The root CA issues the intermediate certificates. The Certificate Revocation List (*CRL*) signed by the root CA contains revoked intermediate certificates during their validity period.

The intermediate CA issues a certificate that enables digital authentication and a certificate that enables creation of qualified electronic signatures (hereinafter *Subscriber Certificates*). The intermediate CA also issues the Online Certificate Status Protocol (OCSP) responder certificates that are used to sign confirmations on the Subscriber Certificate validity at the moment of making an inquiry. A CRL signed by an intermediate CA contains suspended and revoked Subscriber Certificates during their validity period. Valid authentication certificates are also used for encryption purposes and are therefore published in a publicly available Lightweight Directory Access Protocol (*LDAP*) directory service. The overview of the CA hierarchy and related services are presented below. The eID CP covers the part highlighted in yellow.

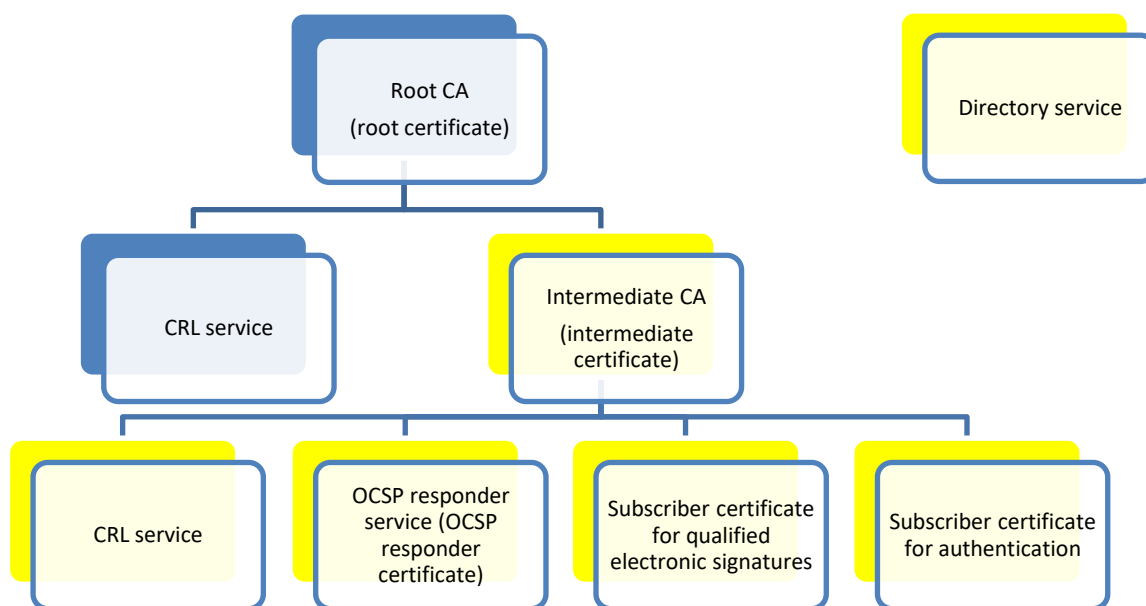


Figure 1. The CA hierarchy and related services for the Republic of Estonia.

The CA shall have a qualified status in accordance with the eIDAS Regulation [2] and shall be included in the Trusted List of the Republic of Estonia for issuing certificates enabling qualified electronic signatures (hereinafter *QES*). The CA shall also issue certificates enabling authentication on level of assurance high.

Issuing and managing certificates enabling QES shall be based on the requirements of the QCP-n-qscd policy defined in ETSI EN 319 411-2 [4]. Issuing and managing certificates enabling digital authentication shall be based on the requirements of the NCP+ policy defined in ETSI EN 319 411-1 [5].

## 1.2. Document Name and Identification

This document is titled “Certificate Policy of ID-1 format identity documents of the Republic of Estonia (eID CP)”. The eID CP is identified by 2 (two) Object Identifiers (OIDs):

- 1.3.6.1.4.1.51361.2 for Documents issued by the PBGB;
- 1.3.6.1.4.1.51455.2 for Documents issued by the MFA.

OIDs are 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
Service attribute	2

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

Document type	Base OID	Sub-OID for system	Sub-OID for Document type
Identity card of Estonian citizens	1.3.6.1.4.1.51361.2 (PBGB)	1	1
Identity card of European Union citizens	1.3.6.1.4.1.51361.2 (PBGB)	1	2
Residence permit card for long-term residents	1.3.6.1.4.1.51361.2 (PBGB)	1	3
Residence permit card for temporary residents and the right of stay in the Republic of Estonia.	1.3.6.1.4.1.51361.2 (PBGB)	1	4
Residence permit card for family members of EU and UK citizens and the right of residence of UK citizens	1.3.6.1.4.1.51361.2 (PBGB)	1	5
Digital identity card of e-residents	1.3.6.1.4.1.51361.2 (PBGB)	1	6
Diplomatic identity card	1.3.6.1.4.1.51455.2 (MFA)	1	1

Example of sub-OIDs according to the Document type issued under the eID CP:

- Identity card of Estonian citizens: 1.3.6.1.4.1.51361.2.1.1;
- Diplomatic identity card: 1.3.6.1.4.1.51455.2.1.1.

Subscriber Certificate for QES shall include the following OIDs:

- 0.4.0.194112.1.2 according to ETSI EN 319 411-2 [4] clause 5.3 c) for QCP-n-qscd;

- eID CP OID.

Subscriber Certificate for authentication shall include the following OID:

- 0.4.0.2042.1.2 according to ETSI EN 319 411-1 [5] clause 5.3 b) for NCP+;
- eID CP OID.

## 1.3. PKI Participants

### 1.3.1. Certification Authorities

The contract partner of the PBGB shall fulfil the role of the CA. The CA shall provide certification and qualified trust services including all the procedures related to the lifecycle of the keys, certificates and related services described in the eID CP exclusively for the Republic of Estonia.

### 1.3.2. Registration Authorities

The PBGB shall fulfil the role of RA when identifying the Subscribers or their representatives, processing the Subscriber applications, issuing Documents and revoking Subscriber Certificates (except for diplomatic identity card). In case of re-key on the existing Document, the Subscriber is authenticated by the authentication certificate or in person by the PBGB.

In case of diplomatic identity card, the MFA shall fulfil the role of RA when identifying the Subscribers or their representatives, processing the Subscriber applications, issuing diplomatic identity cards and revoking Subscriber Certificates. In case of re-key on an existing diplomatic identity card, the Subscriber is authenticated by the authentication certificate. The MFA shall also identify the Subscribers and issue the Documents (except for diplomatic identity cards) on behalf of the PBGB.

External service providers who are contract partners of the PBGB shall fulfil the role of RA when identifying the Subscribers or their representatives and issuing Documents (except diplomatic identity cards) with the Subscriber Certificates.

The responsibilities of the RAs are laid down in IDA [1] and Electronic Identification and Trust Services for Electronic Transactions Act (EUTS Act) [6]. Transfer of functions listed under IDA section 3<sup>1</sup> may be applied.

Hereinafter the RA will refer to the roles of the PBGB and the MFA only. In case the RA is the contract partner of the PBGB, the requirement will be pointed out separately.

The following table summarizes the responsibilities of the RAs:

	Documents (except diplomatic identity cards)	Diplomatic identity cards
Identification of the Subscriber or their representative	PBGB, MFA, external service providers in RA role	MFA
Processing Subscriber applications (Document and Subscriber Certificates)	PBGB	MFA
Packing and logistics of the Documents	PBGB, MFA, external service providers, Card manufacturer	MFA, external service providers, Card manufacturer
Document, including the security code envelope, handover to the Subscriber or their representative	PBGB, MFA, external service providers in RA role	MFA
Subscriber Certificates activation (once Subscriber Certificates are active, then the private key can also be used)	Initiated by PBGB Activated by CA	Initiated by MFA Activated by CA

Subscriber Certificate revocation request application	PBGB, Subscriber via Revocation portal	MFA, Subscriber via Revocation portal
Subscriber Certificate revocation request approval	PBGB, CA	MFA, CA
Subscriber Certificate revocation	CA	CA
Subscriber Certificates re-key application	PBGB, Subscriber via Card Manufacturer's portal	MFA, Subscriber via Card Manufacturer's portal
Subscriber Certificate re-key	CA	CA
Replacement PUK envelope application, processing and approval	PBGB	Not applicable
Replacement PUK envelope generation and logistics	Card manufacturer	Not applicable
Replacement PUK envelope handover	Sent by postal mail	Not applicable
PUK transfer online	Subscriber via Card Manufacturer's portal	Subscriber via Card Manufacturer's portal

### 1.3.3. Subscribers

The Subscriber is the subject of the Subscriber Certificates issued under the eID CP. The Subscriber can only be a natural person entitled by IDA [1]. IDA [1] refers to the Subscriber as “the document holder”. The Subscriber can have only one Document of the same Document type valid at any point of time.

### 1.3.4. Relying Parties

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

### 1.3.5. Other Participants

The Card Manufacturer is a contract partner of the PBGB. The Card Manufacturer is responsible for:

- production of blank Documents;
- security certification, QSCD status and QSCD compliance of the chip in the Documents;
- graphic and electronic personalisation of Documents including
  - generation of key pairs for the Subscriber Certificates;
  - generation of the Subscriber Certificates' request;
  - loading the Subscriber Certificates on the Document.
- physical and logical security in the personalisation site;
- packing and logistics of the Documents;
- Card Manufacturer's portal, re-key system and operations.

The IT and Development Centre of the Ministry of the Interior (hereinafter *SMIT*) is responsible for allocating a correct and unique e-mail address in the [eesti.ee](http://eesti.ee) domain for the Subscriber (except for the holder of diplomatic identity card).

The MFA is responsible for allocating a correct and unique e-mail address in the [eesti.ee](http://eesti.ee) domain for the Subscriber holding a diplomatic identity card.

The PBGB shall fulfil the role of the government Policy Administrator as described in clause 1.5. of the eID CP.

## 1.4. Certificate Usage

### 1.4.1. Appropriate Certificate Uses

The private keys of the intermediate CA certificate shall only be used for signing the following:

- the Subscriber Certificates compliant with QCP-n-qscd or NCP+;
- the certificates for the OCSP responder for the Subscriber Certificate status validation;
- the CRL for certificate status validation.

The Subscriber Certificate for QES is intended for the creation of QES.

The Subscriber Certificate for authentication is intended for

- authentication;
- encryption;
- secure e-mail.

### **1.4.2. Prohibited Certificate Uses**

It is prohibited to use the intermediate certificate for purposes that are not covered in clause 1.4.1. of the eID CP.

The Subscriber Certificates issued under the eID CP shall not be used for any of the following purposes:

- unlawful activity (including cyber-attacks and attempt to infringe the Subscriber Certificate(s) or the Document);
- issuance of new certificates;
- enabling other parties to use the Subscriber's private key;
- enabling the Subscriber Certificate for QES to be used in an automated way;
- using the Subscriber Certificate for QES for any other purpose than creating a QES, including for signing documents which can bring about unwanted consequences or signing such documents for testing purposes;
- using the Subscriber Certificate for authentication to create QES.

## **1.5. Policy Administration**

### **1.5.1. Organisation Administering the Document**

The eID CP is administered by the PBGB.

Police and Border Guard Board

Registry code: 70008747

Address: Pärnu mnt 139, 15060 Tallinn, Estonia

E-mail: [ppa@politsei.ee](mailto:ppa@politsei.ee)

Webpage: [www.politsei.ee/en](http://www.politsei.ee/en)

### **1.5.2. Contact Person**

Any questions and change proposals regarding the eID CP shall be sent to the government Policy Administrator's e-mail: [eid.list@politsei.ee](mailto:eid.list@politsei.ee).

### **1.5.3. Person Determining CPS Suitability for the Policy**

The government Policy Administrator and the Qualified Trust Service Provider's (hereinafter *QTSP*) Policy Management Authority (hereinafter *PMA*) validates and determines the eID CPS conformity to the eID CP. The government Policy Administrator may involve the Information System Authority (hereinafter *RIA*) for an additional opinion.

### **1.5.4. CP Approval Procedures**

The government Policy Administrator shall review the eID CP annually, or if significant changes occur, to ensure the continuing suitability, adequacy and effectiveness of applicable standard to the

current eID CP. Change proposals to the eID CP may be sent at any time to the CP contact person. The government Policy Administrator shall coordinate changes to the eID CP with the CA and the RIA, and may coordinate changes to the eID CP with the MFA and the Card Manufacturer if applicable.

Amendments which do not change the meaning of the eID CP, such as annual reviews with no amendments, spelling corrections and/or contact detail updates, shall be documented in the version history section of the eID CP. In this case, the fractional part of the version number shall be incremented. In the case of substantial changes, the new eID CP version shall be clearly distinguishable from the previous ones, and the serial number shall be incremented by one.

The amended eID CP, along with the enforcement date, which cannot be earlier than 30 (thirty) days after publication, shall be published electronically on the [www.id.ee](http://www.id.ee) website.

All amendments shall be approved by the Identity and Status Bureau of the PBGB and the eID Department of RIA. The amended eID CP shall be enforced by the Deputy Director of the PBGB. The government Policy Administrator shall notify the RIA, the CA, the MFA and the Card Manufacturer when a new version of the eID CP is uploaded on the [www.id.ee](http://www.id.ee) website.

## 1.6. Definitions and Acronyms

### 1.6.1. Terminology

Term	Definition
Authentication	A unique identification of a person by checking his/her alleged identity.
authentication certificate	A digital certificate that enables authentication and enables encryption.
Card Manufacturer	The contract partner of the PBGB who is responsible for <ul style="list-style-type: none"> <li>• production of blank Documents;</li> <li>• graphic and electronic personalisation of Documents including <ul style="list-style-type: none"> <li>○ generation of key pair for the Subscriber Certificates;</li> <li>○ generation of the Subscriber Certificates requests;</li> <li>○ loading the Subscriber Certificates on the Document;</li> </ul> </li> <li>• physical and logical security in the personalisation site;</li> <li>• packing and logistics of the Documents.</li> </ul>
Certificate	Public key, together with additional information, laid down in the Certificate Profiles, rendered unforgeable via encipherment using the private key of the CA which issued the certificate.
Certificate Policy	A set of rules that indicates applicability of a specific certificate to a particular community and/or implementation of public key infrastructure with common security requirements.
Certificate Profiles	A document or documents that determine the information contained within a certificate, CRL and OCSP response as well as the minimal requirements for them.
Certification Authority	A trust service provider who provides certification and qualified trust services including all the procedures related to the lifecycle of the keys, certificates and related services described in the eID CP.
Certification Practice Statement	Statement of the practices which a Certification Authority employs in issuing, managing, revoking, and renewing or re-keying certificates.

Conformity Assessment Body	A body defined in Regulation (EC) No 765/2008 [7], which is accredited in accordance with that Regulation as competent to carry out conformity assessment of a qualified trust service provider and the qualified trust services it provides.
CRL service	A service for publishing Certificate Revocation Lists.
Documents	A uniform term for ID-1 format identity documents (identity card, residence permit card, e-resident's digital identity card and diplomatic identity card) that the CA issues the Subscriber Certificates for.
intermediate CA/certificate	Certification Authority whose certificate is signed by the root CA. Intermediate CA issues the Subscriber Certificates.
LDAP directory service	A certificate directory service for the Subscriber Certificates on the basis of LDAP.
Ministry of Foreign Affairs (MFA)	In this CP, when referring to locations of the MFA, the MFA includes either both or one: the MFA headquarters and/or foreign representations abroad (i.e. embassies, consulates, honorary consuls, consular missions).
OCSP responder service	A certificate status service on the basis of OCSP.
PIN code	Activation code for the Subscriber Certificate enabling digital authentication and the Subscriber Certificate enabling qualified electronic signatures.
Policy Management Authority (PMA)	The PMA is the internal management and governance body of the QTSP.
Revocation portal	Self-service portal operated by CA to revoke Documents together with the Subscriber Certificates.
Card Manufacturer's portal	Self-service portal managed by the Card Manufacturer that enables: <ul style="list-style-type: none"> <li>• PUK transfer/display online;</li> <li>• re-key for an existing Document during mass re-key operations in exceptional circumstances;</li> <li>• operating system patching;</li> <li>• eID activation.</li> </ul>
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 messages, records or files that were encrypted with the corresponding public key.
public key	The key of a key pair that may be publicly disclosed by the 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, records and files so that they can be decrypted only with the holder's corresponding private key.
PUK code	The code enabling to reset blocked PIN1 and PIN2.
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 trust service	An electronic service as defined in the eIDAS Regulation [2]. In the context of eID CP, qualified trust service consists of services provided by a QTSP according to the eIDAS Regulation [2] which consists of the creation, verification, and validation of qualified electronic certificates.
Registration Authority	Entity that is responsible for the identification and authentication of the Subscribers. The Registration Authority may process the Subscribers applications, issue Documents and revoke the Subscriber Certificates.

Relying Party	Legal or natural person who is making decisions based on the certificates.
Subject	A natural person identified in the Certificate name fields for whom a Certificate is issued.
Subscriber	A natural person that subscribes to the trust service. In this document, the Subscriber is to be interpreted as either the Subject or the Subscriber based on instances of legal guardianship or legal representation, in accordance with Estonian legislation (i.e. the Subscriber and Subject may or may not be the same natural person).
Subscriber Certificate(s)	A Certificate issued upon the request of the Subscriber in relation to a Document. Each Document contains two Subscriber Certificates: one for authentication and one for electronic signature.
trust service provider	An organisation that provides trust service(s).

### 1.6.2. Acronyms

Acronym	Definition
CA	Certification Authority
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List, a list of invalid (revoked, suspended) certificates
eIDAS Regulation	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, as amended by Regulation (EU) 2024/1183 [2]
eID CP	Certificate Policy of ID-1 format identity documents of the Republic of Estonia, this document
eID CPS	Certification Practice Statement of ID-1 format identity documents of the Republic of Estonia
EU	European Union
EUTS	Electronic Identification and Trust Services for Electronic Transactions Act [6].
Root CP	Certificate Policy of the root Certification Authority of the Republic of Estonia [10]
IDA	Identity Documents Act [1]
LDAP	Lightweight Directory Access Protocol
MFA	Ministry of Foreign Affairs
OCSP	Online Certificate Status Protocol
OID	Object Identifier, a unique object identification code
PBGB	Police and Border Guard Board
PMA	Policy Management Authority
QSCD	Qualified Electronic Signature Creation Device
QTSP	Qualified Trust Service Provider
RA	Registration Authority
RIA	Information System Authority
SMIT	IT and development centre of the Ministry of the Interior

## 2. Publication and Repository Responsibilities

## 2.1. Repositories

The CA shall host a repository that shall be available 24 (twenty-four) hours a day, 7 (seven) 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

At a minimum, the CA shall publish the following documentation with the enforcement dates on the CA's repository:

- eID CPS;
- Certificate Profiles;
- the terms and conditions for the use of Subscriber Certificates;
- the terms and conditions for the use of OCSP responder service;
- the terms and conditions for the use of CRL service;
- the terms and conditions for the use of the LDAP directory service.

At a minimum, the following documentation with the enforcement dates shall be published in the repository appointed by the PBGB and shall be available on the [www.id.ee](http://www.id.ee) website.

- eID CP;
- terms and conditions for the use of Subscriber Certificates.

RIA may add references to documentation published by the CA on the [www.id.ee](http://www.id.ee) website. The CA may add a reference to the eID CP in the CA's repository.

Any changes to the eID CPS, the Certificate Profiles and the terms and conditions for the use of Subscriber Certificates, OCSP responder service, CRL service and LDAP directory service shall be approved by the government Policy Administrator prior to publishing.

### 2.2.2. Items not Published in the Certification Practice Statement

Information about service levels, fees and technical details laid down in mutual agreements between the CA, the RA and the Card Manufacturer may be left out of the eID CPS. Information about confidential internal procedures of the PBGB, the MFA, the CA, the RA's (including PBGB's contract partners in a RA role), or the Card Manufacturer shall be left out of the eID CPS.

## 2.3. Time or Frequency of Publication

Documentation referred to in clause 2.2.1. of the eID CP shall be published at least 30 days prior to coming into force.

## 2.4. Access Controls on Repositories

Information published in the repositories is public and not considered as confidential information. The owner of the repository shall implement security measures and enforce access control in order to prevent misuse and unauthorised harvesting of information.

## 3. Identification and Authentication

### 3.1. Naming

#### 3.1.1. Types of Names

The Subject distinguished name shall be identified by

- subjectSerialNumber = PNOEE-[personal identification code];
- G = [given name(s)];
- SN = [surname(s)];
- CN = [surname(s)],[given name(s)],[personal identification code];
- C = EE.

Types of names are set in the Certificate Profiles.

#### 3.1.2. Need for Names to be Meaningful

All the values in the Subject information section of the Subscriber Certificate shall be meaningful.

#### 3.1.3. Anonymity or Pseudonymity of Subscribers

Anonymity and pseudonymity of the Subjects shall not be allowed.

#### 3.1.4. Rules for Interpreting Various Name Forms

Pursuant to IDA [1], foreign letters in the Subject's name shall be encoded according to the International Civil Aviation Organization (ICAO) doc 9303 transcription rules if necessary.

#### 3.1.5. Uniqueness of Names

The RA shall ensure that Subscriber Certificates with a matching distinguished name and e-mail address in the Subject Alternative Name (SAN) field are not issued to different Subjects.

#### 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

The Card Manufacturer creates private and public keys within an unpersonalised QSCD. The method to prove the possession of the private key shall be described in the eID CPS.

#### 3.2.2. Authentication of Organisation Identity

Not applicable.

#### 3.2.3. Authentication of Individual Identity

Identity proofing and verification of a natural person shall be done in accordance with IDA [1] and is based on the Commission Implementing Regulation (EU) 2015/1502 [8], that sets out minimum technical specifications and procedures for assurance levels for electronic identification means. Identity proofing and verification of natural persons is done according to Level of Assurance *high*. The CA and the Card Manufacturer shall rely on the identification data provided by the RA.

#### 3.2.4. Non-Verified Subscriber Information

Non-verified Subject information shall not be allowed in the Subscriber Certificate.

### **3.2.5. Validation of Authority**

The right of representation of the Subscriber's representative shall be carried out by the RA in accordance with IDA [1].

### **3.2.6. Criteria for Interoperation**

Not applicable.

## **3.3. Identification and Authentication for Re-Key Requests**

### **3.3.1. Identification and Authentication for Routine Re-Key**

Refer to clause 3.2.3. of the eID CP and ETSI EN 319 411-1 [5].

### **3.3.2. Identification and Authentication for Re-Key After Revocation**

Refer to clause 3.2.3. of the eID CP.

## **3.4. Identification and Authentication for Revocation Request**

Refer to clause 3.2.3. of the eID CP.

# **4. Certificate Life-Cycle Operational Requirements**

## **4.1. Certificate Application**

### **4.1.1. Who Can Submit a Certificate Application**

The Subscriber can submit a certificate application by applying for a Document. The eligibility for persons to apply for a Document is defined in IDA [1].

### **4.1.2. Enrolment Process and Responsibilities**

The Subscriber shall confirm the correctness of the information presented to the RA, be familiar with the terms and conditions for the use of Subscriber Certificates and accept them upon applying for the Document. The responsibilities and process for making decisions about the eligibility to apply for a Document are laid down in IDA [1].

The RA shall ensure the submitting of correct identification data for the name fields in the Subscriber Certificate (e.g. given name, surname, personal identification code) to the Card Manufacturer. The Card Manufacturer sets the Subscriber Certificate expiration date according to the Document expiry submitted by the RA. The Card Manufacturer and the CA shall rely upon the values provided by the RA, no alteration of the data provided by the RA shall be allowed.

SMIT shall be responsible for assigning and keeping track of e-mail addresses in the eesti.ee domain for the Subscriber Certificate for authentication (except for diplomatic identity cards) by

- re-using the previous one if the Subject already has an address assigned;
- generating a previously unused address according to data provided by the RA.

The MFA shall be responsible for assigning and keeping track of e-mail addresses in the eesti.ee domain for the Subscriber Certificate for authentication for diplomatic identity cards only.

## **4.2. Certificate Application Processing**

### **4.2.1. Performing Identification and Authentication Functions**

The Subscriber's identity shall be verified by the RA as described in IDA [1]. The RA shall send an application to the Card Manufacturer. The Card Manufacturer shall generate private keys and associated certificate application for authentication and QES certificates. The Card Manufacturer shall submit certificate applications to the CA via the PBGB. The CA shall accept certificate applications only from the Card Manufacturer via the PBGB.

### **4.2.2. Approval or Rejection of Certificate Applications**

The acceptance or rejection to issue a Document shall be decided by the RA. The CA shall refuse to issue the Subscriber Certificate if the certificate request does not comply with the technical requirements set out in the Certificate Profiles and applicable agreements. In such case, the CA shall notify the Card Manufacturer via the PBGB.

### **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**

The CA shall ensure that Subscriber Certificates are issued securely to maintain their authenticity. The Subscriber Certificates shall be issued in accordance with the Certificate Profiles. The CA shall verify the technical compliance of certificate requests, and if the verification is successful, the CA shall automatically issue the Subscriber Certificates to the Card Manufacturer via the PBGB.

### **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**

During the issuance of a Document, the Subscriber or the representative of the Subscriber confirms that the Document, together with the security code envelope, has been received from the RA or a contract partner of the PBGB. Confirmation of receiving the Document, together with the security code envelope, is deemed as acceptance of Subscriber Certificates.

### **4.4.2. Publication of the Certificate by the CA**

After terminating the suspension of the Subscriber Certificates, the CA shall immediately publish the authentication certificate in the LDAP directory service. Suspended and revoked authentication certificates shall not be available in the LDAP directory service. Expired authentication certificates shall be deleted from the LDAP directory service on the next day following the expiration.

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

The CA shall notify the Card Manufacturer by delivering issued Subscriber Certificates immediately via the PBGB in order to load the Subscriber Certificates on the QSCD.

## **4.5. Key Pair and Certificate Usage**

### **4.5.1. Subscriber Private Key and Certificate Usage**

The Subscriber shall use the private key and the Subscriber Certificates lawfully and in accordance with the terms and conditions for the use of Subscriber Certificates.

When using the signature key to sign documents or transactions, the Subscribers are recommended to use a signature solution that embeds the status of the Subscriber Certificate in the signature data structure and are recommended to apply a qualified time stamp. The Subscribers are recommended to use signature functionality of the ID software (i.e. DigiDoc).

### **4.5.2. Relying Party Public Key and Certificate Usage**

When asking a Subject to use the signature key to sign documents or transactions, Relying Parties must use a signature solution that embeds or includes the status of the Subscriber Certificate with the signature data structure and are highly recommended to apply a qualified time stamp.

When verifying documents or transactions that were signed with a certificate that has already expired at the time of verification, Relying Parties may not rely on the CRL to determine the certificate's status at the (supposed) date of signature because the CRL does not contain status information for expired certificates. If the Relying Party has no other means of verifying the certificate's status, e.g. because the OCSP service is temporarily unavailable or has been decommissioned, then the Relying Party may not make assumptions about the validity of the signature or the date of signature and must decide for themselves whether to accept or reject the signature based on its own criteria and risk acceptance.

## **4.6. Certificate Renewal**

Certificate renewal is not applicable and not allowed. Refer to ETSI EN 319 411-1 [5] clause 6.3.6 for the definition of certificate renewal.

### **4.6.1. Circumstance for Certificate Renewal**

Not applicable. Refer to clause 4.6. of the eID CP.

### **4.6.2. Who May Request Renewal**

Not applicable. Refer to clause 4.6. of the eID CP.

### **4.6.3. Processing Certificate Renewal Requests**

Not applicable. Refer to clause 4.6. of the eID CP.

### **4.6.4. Notification of New Certificate Issuance to Subscriber**

Not applicable. Refer to clause 4.6. of the eID CP.

### **4.6.5. Conduct Constituting Acceptance of a Renewal Certificate**

Not applicable. Refer to clause 4.6. of the eID CP.

### **4.6.6. Publication of the Renewal Certificate by the CA**

Not applicable. Refer to clause 4.6. of the eID CP.

### **4.6.7. Notification of Certificate Issuance by the CA to Other Entities**

Not applicable. Refer to clause 4.6. of the eID CP.

## **4.7. Certificate Re-Key**

Refer to ETSI EN 319 411-1 [5] clause 6.3.7 for the definition of certificate re-key.

### **4.7.1. Circumstance for Certificate Re-Key**

The re-key for the Subscriber Certificates is allowed on a valid Document to address actual or potential security issues and/or vulnerabilities.

### **4.7.2. Who May Request Certification of a New Public Key**

If the PBGB has enabled the re-key process for the Subscriber Certificates, it may be requested via the Card Manufacturer's portal by the Subscriber or by the PBGB service point officer, if the Subscriber appears in person at the PBGB service point. In case of diplomatic identity card, re-key may only be requested by the Subscriber via the Card Manufacturer's portal.

### **4.7.3. Processing Certificate Re-Keying Requests**

The Subscriber or the PBGB service point officer shall submit a re-key request on a valid Document via the Card Manufacturer's portal over the public data communication network.

During certificate re-key, the erroneous or unusable Subscriber Certificates shall be revoked immediately. The end of validity period of the newly issued Subscriber Certificates shall not exceed the end of validity period of the underlying Document.

### **4.7.4. Notification of New Certificate Issuance to Subscriber**

The CA shall notify the Subject about the change of Subscriber certificate statuses.

### **4.7.5. Conduct Constituting Acceptance of a Re-Keyed Certificate**

Refer to clause 4.4.1. of the eID CP. In case of certificate re-key on the valid Document, the Subscriber shall confirm the acceptance of the Subscriber Certificates either via an application at the PBGB service point or via the Card Manufacturer's portal over the public data communication network.

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

Refer to clause 4.4.2. of the eID CP.

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

Refer to clause 4.4.3. of the eID CP.

## **4.8. Certificate Modification**

Certificate modification is not applicable and not allowed. Refer to ETSI EN 319 411-1 [5] clause 6.3.8 for the definition of certificate modification.

### **4.8.1. Circumstance for Certificate Modification**

Not applicable. Refer to clause 4.8. of the eID CP.

### **4.8.2. Who May Request Certificate Modification**

Not applicable. Refer to clause 4.8. of the eID CP.

### **4.8.3. Processing Certificate Modification Requests**

Not applicable. Refer to clause 4.8. of the eID CP.

#### **4.8.4. Notification of New Certificate Issuance to Subscriber**

Not applicable. Refer to clause 4.8. of the eID CP.

#### **4.8.5. Conduct Constituting Acceptance of Modified Certificate**

Not applicable. Refer to clause 4.8. of the eID CP.

#### **4.8.6. Publication of the Modified Certificate by the CA**

Not applicable. Refer to clause 4.8. of the eID CP.

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

Not applicable. Refer to clause 4.8. of the eID CP.

### **4.9. Certificate Revocation and Suspension**

#### **4.9.1. Circumstances for Revocation**

Circumstances for the Subscriber Certificates' revocation are laid down in IDA [1], in the eIDAS Regulation [2], and in corresponding ETSI standards.

In addition, the issuer of the Document may revoke the certificates if

- the issuer of the Document obtains evidence that the Subscriber has lost control over the private keys or PIN codes;
- the initial application was not authorized by the Subscriber or the Subscriber Certificates were not issued in accordance with the eID CP, eID CPS, Certificate Profiles or other applicable agreements.

The CA has the right to revoke a Subscriber Certificates in the following circumstances:

- The CA obtains evidence that the Subject's PIN have been compromised;
- The CA obtains evidence that the key algorithms or key lengths have been compromised;
- The CA obtains evidence that the Subscriber's initial application was not authorised and the Subscriber does not retroactively grant authorisation;
- The CA obtains evidence that the Subject's private key corresponding to the public key in the Subscriber Certificate suffered a key compromise or no longer complies with the requirements;
- The CA obtains evidence that the Subscriber Certificate was misused;
- The CA is made aware that the Subscriber has violated one or more of their obligations under the terms and conditions for the use of Subscriber Certificates;
- The CA is made aware of a material change in the information contained in the Subscriber Certificate(s);
- The CA is made aware that the Subscriber Certificates were not issued in accordance with the eID CP and/or eID CPS;
- The CA determines that any of the information appearing in the Subscriber Certificates is inaccurate or misleading;
- The CA has the right to revoke a previous certificate, in case of a repeat certificate application from the Card Manufacturer;
- The CA terminates provisioning of the certification and qualified trust services or the CA is dissolved;
- The CA is made aware of a possible compromise of the private key of the CA used for issuing the Subscriber Certificates;

- When revocation is required by the eID CP;
- When the technical content or format of the Subscriber Certificates presents an unacceptable risk to Relying Parties;
- The CA obtains evidence that the QSCD has been compromised or its QSCD status has expired;
- If such an obligation is foreseen by the law or any legislation established on the basis thereof.

The Subscriber may request the revocation of their Subscriber Certificates.

#### **4.9.2. Who Can Request Revocation**

Entities eligible to request the Subscriber Certificate revocation are laid down in IDA [1], in the eIDAS Regulation [2], and in corresponding ETSI standards:

- The issuer of the Document;
- The Competent Authority within the meaning of the aforementioned legislation;
- The CA;
- The Subscriber.

#### **4.9.3. Procedure for Revocation Request**

The provisions and procedures for revocation of Subscriber Certificates are laid down in IDA [1]. The revocation of the Subscriber Certificates shall be recorded in the certificate database provided by the CA. After the revocation of the Subscriber Certificate, the CA shall immediately remove the revoked authentication certificate from the LDAP directory service. The CA shall notify the Subject about the revocation of the Subscriber Certificates.

#### **4.9.4. Revocation Request Grace Period**

No stipulation.

#### **4.9.5. Time Within Which CA Must Process the Revocation Request**

Revocation requests shall be processed immediately after verifying the existence of the legal basis for applying for revocation of a certificate.

#### **4.9.6. Revocation Checking Requirement for Relying Parties**

Relying Parties can verify the revocation of the Subscriber Certificates against the OCSP responder service and CRL service. The CA shall provide information on the certificate status information of the revoked Subscriber Certificates until the termination of CA's operation.

#### **4.9.7. CRL Issuance Frequency**

The CA shall issue the CRL for the Subscriber Certificates at least every 10 (ten) hours.

#### **4.9.8. Maximum Latency for CRLs**

The CA shall monitor the CRL expiry so that new CRL is issued on time and prior the expiry of the previous one. The maximum validity of the CRL is 12 (twelve) hours.

#### **4.9.9. On-Line Revocation/Status Checking Availability**

The CA shall provide certificate status service via OCSP responder for the Subscriber Certificate status information. The Subscriber Certificate status information shall be available until the termination of CA's operation. The CA shall not issue a last CRL until all the Subscriber Certificates in the scope of the CRL are either expired or revoked as stated in clause 6.3.10 of ETSI EN 319 411-2 [4].

#### **4.9.10. On-Line Revocation Checking Requirements**

A Relying Party shall follow the limitations stated within the Subscriber Certificates and make sure that the transaction to be accepted corresponds to the eID CP and eID CPS.

#### **4.9.11. Other Forms of Revocation Advertisements Available**

The CA shall provide information on the revocation status of the Subscriber Certificates.

#### **4.9.12. Special Requirements re Key Compromise**

No stipulation.

#### **4.9.13. Circumstances for Suspension**

During the personalisation process of the Document, the certificates are issued in a suspended state.

#### **4.9.14. Who Can Request Suspension**

Not applicable.

#### **4.9.15. Procedure for Suspension Request**

Not applicable.

#### **4.9.16. Limits on Suspension Period**

Document together with the suspended Subscriber Certificates may be revoked according to the IDA [1].

#### **4.9.17. Circumstances for Termination of Suspension**

Termination of suspension is allowed in the process of activating the eID functionality of the Document.

#### **4.9.18. Who can Request Termination of Suspension**

Termination of suspension is allowed during the issuance of the Document by RAs, including contract partners of the PBGB.

#### **4.9.19. Procedure for Termination of Suspension**

The RAs, including contract partners of the PBGB, shall be able to terminate the suspension of the Subscriber Certificates after the issuance of Document. The termination of suspension of the Subscriber Certificates shall be recorded in the certificate database provided by the CA. The termination of suspension shall be processed immediately.

### **4.10. Certificate Status Services**

#### **4.10.1. Operational Characteristics**

The OCSP responder service shall be accessible over HTTP and HTTPS protocol. The CRL service shall be accessible over HTTP and HTTPS protocol. Operational characteristics are set in the Certificate Profiles.

#### **4.10.2. Service Availability**

The CA shall provide the OCSP responder service and CRL service 24 (twenty four) hours a day, 7 (seven) days a week with a minimum of 99% availability overall per year with a scheduled downtime that does not exceed 0,5% annually. The CA shall update CRL on the revocation status of the expired or revoked Subscriber Certificates at least every 10 (ten) hours.

### **4.10.3. Optional Features**

Not applicable.

## **4.11. End of Subscription**

The subscription ends when the Subscriber Certificates expire or the Subscriber requests the revocation of the Subscriber Certificates.

## **4.12. Key Escrow and Recovery**

### **4.12.1. Key Escrow and Recovery Policy and Practices**

Not applicable.

### **4.12.2. Session Key Encapsulation and Recovery Policy and Practices**

Not applicable.

# **5. Facility, Management, and Operational Controls**

The CA shall be compliant with ISO/IEC 27001 [9], ETSI EN 319 411-2 [4], ETSI EN 319 411-1 [5] and ETSI EN 319 401 [17].

## **5.1. Physical Controls**

Refer to clause 5.1. of the Root CP [10].

### **5.1.1. Site Location and Construction**

Refer to clause 5.1.1. of the Root CP [10].

### **5.1.2. Physical Access**

Refer to clause 5.1.2. of the Root CP [10].

### **5.1.3. Power and Air Conditioning**

Refer to clause 5.1.3. of the Root CP [10].

### **5.1.4. Water Exposures**

Refer to clause 5.1.4. of the Root CP [10].

### **5.1.5. Fire Prevention and Protection**

Refer to clause 5.1.5. of the Root CP [10].

### **5.1.6. Media Storage**

Refer to clause 5.1.6. of the Root CP [10].

### **5.1.7. Waste Disposal**

Refer to clause 5.1.7. of the Root CP [10].

### **5.1.8. Off-Site Backup**

Refer to clause 5.1.8. of the Root CP [10].

## **5.2. Procedural Controls**

### **5.2.1. Trusted Roles**

Refer to clause 5.2.1. of the Root CP [10].

### **5.2.2. Number of Persons Required per Task**

Refer to clause 5.2.2. of the Root CP [10].

### **5.2.3. Identification and Authentication for Each Role**

Refer to clause 5.2.3. of the Root CP [10].

### **5.2.4. Roles Requiring Separation of Duties**

Refer to clause 5.2.4. of the Root CP [10].

## **5.3. Personnel Controls**

### **5.3.1. Qualifications, Experience, and Clearance Requirements**

Refer to clause 5.3.1. of the Root CP [10].

### **5.3.2. Background Check Procedures**

Refer to clause 5.3.2. of the Root CP [10].

### **5.3.3. Training Requirements**

Refer to clause 5.3.3. of the Root CP [10].

### **5.3.4. Retraining Frequency and Requirements**

Refer to clause 5.3.4. of the Root CP [10].

### **5.3.5. Job Rotation Frequency and Sequence**

Refer to clause 5.3.5. of the Root CP [10].

### **5.3.6. Sanctions for Unauthorized Actions**

Refer to clause 5.3.6. of the Root CP [10].

### **5.3.7. Independent Contractor Requirements**

Refer to clause 5.3.7. of the Root CP [10].

### **5.3.8. Documentation Supplied to Personnel**

Refer to clause 5.3.8. of the Root CP [10].

## **5.4. Audit Logging Procedures**

The CA shall perform audit logging procedures in compliance with the eIDAS Regulation article 24 [2] and applicable ETSI and ISO standards.

#### **5.4.1. Types of Events Recorded**

Refer to clause 5.4.1. of the Root CP [10].

#### **5.4.2. Frequency of Processing Log**

Refer to clause 5.4.2. of the Root CP [10].

#### **5.4.3. Retention Period for Audit Log**

Refer to clause 5.4.3. of the Root CP [10]. The CA shall state the period of retention for each type of record in the eID CPS.

#### **5.4.4. Protection of Audit Log**

Refer to clause 5.4.4. of the Root CP [10].

#### **5.4.5. Audit Log Backup Procedures**

Refer to clause 5.4.5. of the Root CP [10].

#### **5.4.6. Audit Collection System (Internal vs. External)**

The CA shall describe their audit collection system in the eID CPS.

#### **5.4.7. Notification to Event-Causing Subject**

Refer to clause 5.4.7. of the Root CP [10].

#### **5.4.8. Vulnerability Assessments**

Refer to clause 5.4.8. of the Root CP [10].

### **5.5. Records Archival**

Refer to clause 5.5. of the Root CP [10].

#### **5.5.1. Types of Records Archived**

Refer to clause 5.5.1. of the Root CP [10]. The CA shall state the types of records archived in the eID CPS.

#### **5.5.2. Retention Period for Archive**

Refer to clause 5.5.2. of the Root CP [10].

#### **5.5.3. Protection of Archive**

Refer to clause 5.5.3. of the Root CP [10].

#### **5.5.4. Archive Backup Procedures**

Refer to clause 5.5.4. of the Root CP [10].

#### **5.5.5. Requirements for Time-Stamping of Records**

Refer to clause 5.5.5. of the Root CP [10].

#### **5.5.6. Archive Collection System (Internal or External)**

The CA shall describe the type of archival collection system used in the eID CPS. The RA may use external archive collection systems for physical archive records.

### **5.5.7. Procedures to Obtain and Verify Archive Information**

Refer to clause 5.5.7. of the Root CP [10].

## **5.6. Key Changeover**

Refer to clause 5.6. of the Root CP [10].

## **5.7. Compromise and Disaster Recovery**

### **5.7.1. Incident and Compromise Handling Procedures**

Refer to clause 5.7.1. of the Root CP [10].

### **5.7.2. Computing Resources, Software, and/or Data Are Corrupted**

Refer to clause 5.7.2. of the Root CP [10].

### **5.7.3. Entity Private Key Compromise Procedures**

Refer to clause 5.7.3. of the Root CP [10].

### **5.7.4. Business Continuity Capabilities After a Disaster**

Refer to clause 5.7.4. of the Root CP [10].

## **5.8. CA or RA Termination**

Refer to clause 5.8. of the Root CP [10]. The RA termination plan shall be determined by the PBGB.

# **6. Technical Security Controls**

## **6.1. Key Pair Generation and Installation**

### **6.1.1. Key Pair Generation**

The private key for the Subscriber Certificates shall be generated on the QSCD during the Document personalisation or re-key on a valid Document. The generated keys shall not be extracted or restored from the Document. The private keys shall be protected by the activation codes.

### **6.1.2. Private Key Delivery to Subscriber**

The private keys shall be delivered to the Subscriber on a QSCD, i.e. on the chip of the Document during the issuance of Document. The Card Manufacturer and the RA are responsible for the secure storage and logistics of the Document prior issuance.

In case of re-key process on a valid Document, the private keys shall be generated on the Subject's QSCD.

### **6.1.3. Public Key Delivery to Certificate Issuer**

The Card Manufacturer shall deliver the Subject's public keys to the CA via the PBGB.

### **6.1.4. CA Public Key Delivery to Relying Parties**

The CA public key shall be available at the CA's repository.

### **6.1.5. Key Sizes**

The CA shall use cryptographic keys for providing certification and qualified trust services and follow the latest version of ETSI TS 119 312 [18] and industry best practices for key lifecycle management, key length and algorithms. Allowed key sizes are set in the Certificate Profiles.

### **6.1.6. Public Key Parameters Generation and Quality Checking**

The CA shall check the public key against duplicates prior to issuing the Subscriber Certificates and/or regularly in the certificate database.

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

Allowed key usages are set in the Certificate Profiles.

## **6.2. Private Key Protection and Cryptographic Module Engineering Controls**

### **6.2.1. Cryptographic Module Standards and Controls**

The chip of the Document shall be certified as a QSCD according to the eIDAS Regulation [2].

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

The Subject's private keys are not under n out of m multi-person control.

### **6.2.3. Private Key Escrow**

Private key escrow is not allowed.

### **6.2.4. Private Key Backup**

The Subject's private keys shall not be extracted or restored from the QSCD and shall not be backed up.

### **6.2.5. Private Key Archival**

The Subject's private keys shall not be extracted or restored from the QSCD and shall not be archived.

### **6.2.6. Private Key Transfer Into or From a Cryptographic Module**

The Subject's private keys are generated on the QSCD.

### **6.2.7. Private Key Storage on Cryptographic Module**

The Subject's private keys shall be stored on a QSCD only.

### **6.2.8. Method of Activating Private Key**

The private key shall be protected by the activation codes (PIN1 and PIN2) and each Document shall have a single unlock key (PUK). PIN1, PIN2 and PUK are security codes that enable electronic usage of the Document. Private keys are activated after the issuance of the Document by the issuer of the Document.

Once the Subscriber initiates authentication with the corresponding private key, they shall be prompted to enter PIN1 at least once. The Subject shall be prompted to enter PIN2 before every single operation done with the corresponding private key.

### **6.2.9. Method of Deactivating Private Key**

In case the Subscriber has initiated authentication, they shall be able to deactivate the private key by

logging out of the e-service. In case the Subject has entered PIN2, the corresponding private key is deactivated after each operation.

#### **6.2.10. Method of Destroying Private Key**

The private keys can be destroyed by physically destroying or damaging the chip of the Document.

#### **6.2.11. Cryptographic Module Rating**

The chip of the Document shall be certified as a QSCD according to eIDAS Regulation [2].

### **6.3. Other Aspects of Key Pair Management**

#### **6.3.1. Public Key Archival**

All Subjects' public keys shall be stored in the certificate database provided by the CA and may be archived. Retention period shall be in accordance with the eIDAS Regulation [2], EUTS [6] and applicable standards.

#### **6.3.2. Certificate Operational Periods and Key Pair Usage Periods**

The operational period of a Subscriber Certificate ends upon revocation or expiry of the Subscriber Certificate.

The Subscriber shall not use the key pair of the Subscriber Certificates beyond the end of the Subscriber Certificate lifecycle. The CA shall not issue Subscriber Certificates which exceed the lifetime of the intermediate certificate that issued the Subscriber Certificate. The issuance of the new Subscriber Certificates shall stop at an appropriate date prior to the expiration of the intermediate certificate so that no Subscriber Certificate expires after the expiration of the intermediate certificate. End of validity period of the Subscriber Certificate shall be the same as the end of validity period of the corresponding Document for which it was issued. The validity period of Subscriber Certificate shall be up to 5 (five) years.

### **6.4. Activation Data**

#### **6.4.1. Activation Data Generation and Installation**

Activation data shall be generated and installed during the personalisation of Documents. The process shall be described in the eID CPS. In case of re-key on a valid Document, activation data shall remain unchanged.

#### **6.4.2. Activation Data Protection**

The Subscriber is responsible for protecting the private key, private key activation codes and PUK. It shall be prohibited to transfer the Document and/or activation codes to a third party. It is the responsibility of the Subscriber to immediately revoke the Subscriber Certificates or the Document (when the Document is revoked, the certificates are also always revoked), in case the Document is lost or there is a reasonable suspicion that the Subscriber Certificates may be used without the Subscriber's knowledge and consent.

#### **6.4.3. Other Aspects of Activation Data**

Not applicable.

### **6.5. Computer Security Controls**

### **6.5.1. Specific Computer Security Technical Requirements**

The Subscriber shall be responsible for applying reasonable protection on the device where the private keys are used.

### **6.5.2. Computer Security Rating**

The Subscriber shall be responsible for applying reasonable protection on the device where the private keys are used.

## **6.6. Life Cycle Technical Controls**

### **6.6.1. System Development Controls**

The Subscriber shall be responsible for applying reasonable protection on the device where the private keys are used.

### **6.6.2. Security Management Controls**

The Subscriber shall be responsible for applying reasonable protection on the device where the private keys are used.

### **6.6.3. Life Cycle Security Controls**

The Subscriber shall be responsible for applying reasonable protection on the device where the private keys are used.

## **6.7. Network Security Controls**

The Subscriber shall be responsible for applying reasonable protection on the device where the private keys are used.

## **6.8. Time-Stamping**

Not applicable.

# **7. Certificate, CRL, and OCSP Profiles**

## **7.1. Certificate Profile**

The Subscriber Certificates shall be issued in accordance with X.509 version 3, IETF RFC 5280 [11], IETF RFC 5480 [12], IETF RFC 5639 [13], ETSI EN 319 412-2 [14] and ETSI EN 319 411-2 (chapter 6.6) [4]. The Subscriber Certificate profiles are set in the Certificate Profiles.

### **7.1.1. Version Number(s)**

Refer to the clause 7.1. of the eID CP.

### **7.1.2. Certificate Extensions**

Refer to the clause 7.1. of the eID CP.

### **7.1.3. Algorithm Object Identifiers**

Refer to the clause 7.1. of the eID CP.

#### **7.1.4. Name Forms**

Refer to the clause 7.1. of the eID CP.

#### **7.1.5. Name Constraints**

Refer to the clause 7.1. of the eID CP.

#### **7.1.6. Certificate Policy Object Identifier**

Refer to the clause 7.1. of the eID CP.

#### **7.1.7. Usage of Policy Constraints Extension**

Refer to the clause 7.1. of the eID CP.

#### **7.1.8. Policy Qualifiers Syntax and Semantics**

Refer to the clause 7.1. of the eID CP.

#### **7.1.9. Processing Semantics for the Critical Certificate Policies Extension**

Refer to the clause 7.1. of the eID CP.

### **7.2. CRL Profile**

The CRL shall be issued in accordance with IETF RFC 5280 [11], IETF RFC 5480 [12] and IETF RFC 5639 [13]. The CRL profile is set in the Certificate Profiles.

#### **7.2.1. Version Number(s)**

Refer to the clause 7.2. of the eID CP.

#### **7.2.2. CRL and CRL Entry Extensions**

Refer to the clause 7.2. of the eID CP.

### **7.3. OCSP Profile**

The OCSP response shall be issued in accordance with IETF RFC 6960 [15]. The OCSP response and OCSP responder certificate profile are set in the Certificate Profiles.

#### **7.3.1. Version Number(s)**

Refer to the clause 7.3. of the eID CP.

#### **7.3.2. OCSP Extensions**

Refer to the clause 7.3. of the eID CP.

## **8. Compliance Audit and Other Assessments**

### **8.1. Frequency or Circumstances of Assessment**

Refer to clause 8.1. of the Root CP [10].

### **8.2. Identity/Qualifications of Assessor**

Refer to clause 8.2. of the Root CP [10].

### **8.3. Assessor's Relationship to Assessed Entity**

Refer to clause 8.3. of the Root CP [10].

### **8.4. Topics Covered by Assessment**

In addition to the conformity of documentation at the first stage of the conformity assessment referred to in clause 8.4. of the Root CP [10], the documentation assessed may include, but is not limited to:

- eID CP;
- eID CPS;
- terms and conditions for the use of Subscriber Certificates.

Furthermore, the following topics shall be covered by internal audits:

- data protection of the Subscribers, security policies, performance of work procedures and contractual obligations, and the compliance with the eID CP and eID CPS.

The Conformity Assessment Body and/or the auditor of the CA shall also perform audits of the Card manufacturer and RAs (including the external service providers who are contract partners of the PBGB) and subcontractors to the extent that they are related to providing certification and qualified trust services.

### **8.5. Actions Taken as a Result of Deficiency**

Refer to clause 8.5. of the Root CP [10].

### **8.6. Communication of Results**

Refer to clause 8.6. of the Root CP [10].

## **9. Other Business and Legal Matters**

### **9.1. Fees**

#### **9.1.1. Certificate Issuance or Renewal Fees**

The fee for the Subscriber certificate issuance is included in the fee for the review of a Document application, in accordance with the State Fees Act [16]. The fee for the issuance of the Subscriber Certificate for the diplomatic identity card is covered by the MFA as agreed in the mutual agreement between the MFA and the PBGB.

#### **9.1.2. Certificate Access Fees**

Access to the Subscriber Certificates shall be free of charge.

#### **9.1.3. Revocation or Status Information Access Fees**

Revocation of the Subscriber Certificate shall be free of charge. The Subscriber Certificate validity checking service via OCSP responder and information about the revoked Subscriber Certificates in the CRL shall be available free of charge.

#### **9.1.4. Fees for Other Services**

Fees for other services shall be laid down in mutual agreements between the CA, the PBGB, the MFA, the Card Manufacturer, or their contract partners and/or subcontractors.

### **9.1.5. Refund Policy**

The Subscriber is entitled to apply for a refund of the state fee or the review of the Document application in accordance with State Fees Act [16].

## **9.2. Financial Responsibility**

### **9.2.1. Insurance Coverage**

Refer to clause 9.2.1. of the Root CP [10].

### **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**

### **9.3.1. Scope of Confidential Information**

Refer to clause 9.3.1. of the Root CP [10]. The Subscribers are entitled to receive information in relation to themselves in the amount and in accordance with applicable laws and regulations.

### **9.3.2. Information Not Within the Scope of Confidential Information**

Refer to clause 9.3.2. of the Root CP [10]. The CA shall include a list of information considered public in the eID CPS (i.e. terms and conditions, personal data processing principles, etc.). Non-personalised statistical information may be considered as public, and if necessary may be published.

### **9.3.3. Responsibility to Protect Confidential Information**

Refer to clause 9.3.3. of the Root CP [10].

## **9.4. Privacy of Personal Information**

Refer to clause 9.4. of the Root CP [10]. The CA shall maintain privacy of the Subscriber information. The CA shall take appropriate technical and organisational measures to prevent and protect against unauthorised or unlawful processing of personal data and against accidental loss, intentional destruction, or damage to personal data. The CA shall implement security controls outlined in clause 5. of the eID CP to ensure data protection by design and by default. Data exchange terms and details shall be outlined in data exchange contracts between the CA and other parties.

### **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**

Not applicable.

### **9.5. Intellectual Property rights**

The government Policy Administrator owns the intellectual property rights of the eID CP.

### **9.6. Representations and Warranties**

#### **9.6.1. CA Representations and Warranties**

Refer to clause 9.6.1. of the Root CP [10].

#### **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 for the use of Subscriber Certificates agreed upon when submitting an application for a Document.

#### **9.6.4. Relying Party Representations and Warranties**

Relying Party shall verify the validity of the Subscriber Certificate using validation services offered by the CA, prior to relying on the Subscriber Certificate. Relying Party shall consider the limitations stated in the Subscriber Certificate and shall ensure that the transaction to be accepted corresponds to the eID 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 1.5.4. of the eID CP.

### **9.10.2. Termination**

The eID CP shall remain in force until it is replaced by a new version or when the CA's service is terminated and all the Subscriber Certificates therefore become invalid.

### **9.10.3. Effect of Termination and Survival**

The PBGB shall communicate the conditions and effect of termination of the eID CP.

## **9.11. Individual Notices and Communications with Participants**

Refer to clause 1.5.2. of the eID CP.

## **9.12. Amendments**

### **9.12.1. Procedure for Amendment**

Refer to clause 1.5.4. of the eID CP.

### **9.12.2. Notification Mechanism and Period**

Refer to clause 1.5.4. of the eID CP.

### **9.12.3. Circumstances Under Which OID Must be Changed**

The government Policy Administrator shall determine the new OID when necessary (e.g. when a new contract partner begins issuance of Subscriber Certificates and/or in case new Document types are introduced).

## **9.13. Dispute Resolution Provisions**

No stipulation.

## **9.14. Governing Law**

The eID CP is governed by the jurisdictions of the EU and the Republic of Estonia.

## **9.15. Compliance with Applicable Law**

The participants to the certification services shall ensure compliance with the following legislation to the extent of their area of responsibility:

- eIDAS Regulation [2] – 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, as amended by Regulation (EU) 2024/1183;
- Commission Implementing Regulation (EU) 2015/1502 of 8 September 2015 on setting out minimum technical specifications and procedures for assurance levels for electronic identification means pursuant to Article 8(3) of 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];
- Regulation (EC) No 765/2008 of the European Parliament and of the Council of 9 July 2008 setting out the requirements for accreditation and repealing Regulation (EEC) No 339/93 [7];
  - 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 (General Data Protection Regulation). Published: ELI: <http://data.europa.eu/eli/reg/2016/679/oj>;
  - EUTS [6] – Electronic Identification and Trust Services for Electronic Transactions Act,
  - IDA [1] – Identity Documents Act;
  - State Fees Act [16];
  - Personal Data Protection Act, 15.01.2019. Published: <https://www.riigiteataja.ee/en/eli/ee/523012019001/consolide/current>;
  - Emergency Act, RT I, 03.03.2017, 1. Published: <https://www.riigiteataja.ee/en/eli/ee/505012018004/consolide/current>;
  - Consular Act, RT I 2009, 29, 175. Published: <https://www.riigiteataja.ee/en/eli/ee/527012016004/consolide/current>;
  - Cybersecurity Act. Published: <https://www.riigiteataja.ee/en/eli/523052018003/consolide/current>;
  - Other applicable laws of the Republic of Estonia and the EU.

The participants to the certification services shall ensure compliance with the following related EU standards to the extent of their area of responsibility:

- ETSI EN 319 401 [17] Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers;
- ETSI EN 319 411-1 [5] – Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements;
- ETSI EN 319 411-2 [4] – 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;
- ETSI EN 319 412-1 – Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures. Published: <https://www.etsi.org>;
- ETSI EN 319 412-2 [14] – Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons;
- CEN EN 419 211 Protection profiles for secure signature creation device. Published: <https://www.cencenelec.eu/>;
- Other referenced and relevant standards to comply with applicable laws.

## 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**

No stipulation.

## **References**

- [1] Identity Documents Act, RT I 1999, 25, 365. Published: <https://www.riigiteataja.ee/en/eli/ee/521062017003/consolide/current>
- [2] 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, as amended by Regulation (EU) 2024/1183 as regards establishing the European Digital Identity Framework. Published: ELI: <http://data.europa.eu/eli/reg/2014/910/2024-10-18> and <http://data.europa.eu/eli/reg/2024/1183/oj>
- [3] IETF 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>
- [4] 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. Published: <https://www.etsi.org/>
- [5] ETSI EN 319 411-1 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements. Published: <https://www.etsi.org/>
- [6] Electronic Identification and Trust Services for Electronic Transactions Act, 26.10.2016. Published: <https://www.riigiteataja.ee/en/eli/527102016001/consolide/current>
- [7] Regulation (EC) No 765/2008 of the European Parliament and of the Council of 9 July 2008 setting out the requirements for accreditation and repealing Regulation (EEC) No 339/93. Published: ELI: <http://data.europa.eu/eli/reg/2008/765/2021-07-16>
- [8] Commission Implementing Regulation (EU) 2015/1502 of 8 September 2015 on setting out minimum technical specifications and procedures for assurance levels for electronic identification means pursuant to Article 8(3) of 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. Published: ELI: [http://data.europa.eu/eli/reg\\_impl/2015/1502/oj](http://data.europa.eu/eli/reg_impl/2015/1502/oj)
- [9] ISO/IEC 27001 Information technology - Security techniques - Information security management systems – Requirements
- [10] Certificate Policy of the root Certification Authority of the Republic of Estonia
- [11] IETF RFC 5280 – Request for Comments 5280, Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile. Published: <https://www.ietf.org/rfc/rfc5280.txt>
- [12] IETF RFC 5480 – Request for Comments: 5480, Elliptic Curve Cryptography Subject Public

- Key Information. Published: <https://www.ietf.org/rfc/rfc5480.txt>
- [13] IETF RFC 5639 – Request for Comments: 5639, Elliptic Curve Cryptography (ECC) Brainpool Standard Curves and Curve Generation. Published: <https://www.ietf.org/rfc/rfc5639.txt>
- [14] ETSI EN 319 412-2 – Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons. Published: <https://www.etsi.org/>
- [15] IETF RFC 6960 – Request for Comments 6960, X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP. Published: <https://www.ietf.org/rfc/rfc6960.txt>
- [16] State Fees Act. Published:  
<https://www.riigiteataja.ee/en/eli/ee/519022016005/consolide/current>
- [17] ETSI EN 319 401 – Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers. Published: <https://www.etsi.org/>;
- [18] ETSI TS 119 312 – Electronic Signatures and Infrastructures (ESI); Cryptographic Suites. Published: <https://www.etsi.org>.