

# Certificate Policy for the root Certification Authority of the Republic of Estonia (Root CP)

Version 1.1

OID: 1.3.6.1.4.1.51361.3

Effective since: 15.10.2025

Version History		
Date	Version	Changes/Updates/Amendments
21.05.2025	1.1	Minor updates to 1.6 and 9.15 (capitalization of terminology and update to references). Removed reference to expired certificates from 9.1.3 as it pertains to revoked certificates. Added an effective date to the Root CP.
29.01.2025	1.0	

## Table of Contents

1. Introduction.....	8
1.1. Overview.....	8
1.2. Document Name and Identification .....	9
1.3. PKI Participants .....	9
1.3.1. Certification Authorities.....	9
1.3.2. Registration Authorities .....	9
1.3.3. Subscribers.....	10
1.3.4. Relying Parties .....	10
1.3.5. Other Participants.....	10
1.4. Certificate Usage.....	10
1.4.1. Appropriate Certificate Uses.....	10
1.4.2. Prohibited Certificate Uses .....	10
1.5. Policy Administration .....	10
1.5.1. Organization Administering the Document.....	10
1.5.2. Contact Person .....	10
1.5.3. Person Determining CPS Suitability for the Policy .....	10
1.5.4. CP Approval Procedures .....	11
1.6. Definitions and Acronyms .....	11
1.6.1. Terminology .....	11
1.6.2. Acronyms .....	12
2. Publication and Repository Responsibilities.....	13
2.1. Repositories.....	13
2.2. Publication of Certificate Information .....	13
2.2.1. Publication and Notification Policies.....	13
2.2.2. Items not Published in the Certification Practice Statement.....	14
2.3. Time or Frequency of Publication.....	14
2.4. Access Controls on Repositories.....	14
3. Identification and Authentication.....	14
3.1. Naming.....	14
3.1.1. Types of Names.....	14
3.1.2. Need for Names to be Meaningful .....	15
3.1.3. Anonymity or Pseudonymity of Subscribers .....	15
3.1.4. Rules for Interpreting Various Name Forms .....	15
3.1.5. Uniqueness of Names.....	15
3.1.6. Recognition, Authentication, and Role of Trademarks .....	15
3.2. Initial Identity Validation .....	15
3.2.1. Method to Prove Possession of Private Key .....	15
3.2.2. Authentication of Organisation Identity.....	15
3.2.3. Authentication of Individual Identity.....	15
3.2.4. Non-verified Subscriber Information.....	15
3.2.5. Validation of Authority.....	15
3.2.6. Criteria for Interoperability .....	15
3.3. Identification and Authentication for Re-Key Requests .....	16
3.3.1. Identification and Authentication for Routine Re-Key .....	16
3.3.2. Identification and Authentication for Re-Key After Revocation.....	16
3.4. Identification and Authentication for Revocation Requests.....	16
4. Certificate Life-Cycle Operational Requirements.....	16
4.1. Certificate Application .....	16
4.1.1. Who Can Submit a Certificate Application.....	16
4.1.2. Enrolment Process and Responsibilities .....	16

4.2. Certificate Application Processing .....	16
4.2.1. Performing Identification and Authentication Functions .....	16
4.2.2. Approval or Rejection of Certificate Applications .....	17
4.2.3. Time to Process Certificate Applications .....	17
4.3. Certificate Issuance .....	17
4.3.1. CA Actions During Certificate Issuance .....	17
4.3.2. Notification to Subscriber by the CA of Issuance of Certificate .....	17
4.4. Certificate Acceptance .....	17
4.4.1. Conduct Constituting Certificate Acceptance .....	17
4.4.2. Publication of the Certificate by the CA .....	17
4.4.3. Notification of Certificate Issuance by the CA to Other Entities .....	17
4.5. Key Pair and Certificate Usage .....	17
4.5.1. Subscriber Private Key and Certificate Usage .....	17
4.5.2. Relying Party Public Key and Certificate Usage .....	17
4.6. Certificate Renewal.....	17
4.6.1. Circumstance for Certificate Renewal .....	18
4.6.2. Who May Request Renewal.....	18
4.6.3. Processing Certificate Renewal Requests .....	18
4.6.4. Notification of New Certificate Issuance to Subscribers .....	18
4.6.5. Conduct Constituting Acceptance of a Renewal Certificate .....	18
4.6.6. Publication of the Renewal Certificate by the CA .....	18
4.6.7. Notification of Certificate Issuance by the CA to Other Entities .....	18
4.7. Certificate Re-Key .....	18
4.7.1. Circumstance for Certificate Re-Key.....	18
4.7.2. Who May Request Certification of a New Public Key .....	18
4.7.3. Processing Certificate Re-Key Requests.....	18
4.7.4. Notification of New Certificate Issuance to Subscriber.....	18
4.7.5. Conduct Constituting Acceptance of a Re-Keyed Certificate .....	18
4.7.6. Publication of the Re-Keyed Certificate by the CA .....	18
4.7.7. Notification of Certificate Issuance by the CA to Other Entities .....	18
4.8. Certificate Modification.....	19
4.8.1. Circumstance for Certificate Modification .....	19
4.8.2. Who May Request Certificate Modification .....	19
4.8.3. Processing Certificate Modification Requests .....	19
4.8.4. Notification of New Certificate Issuance to Subscriber.....	19
4.8.5. Conduct Constituting Acceptance of Modified Certificate .....	19
4.8.6. Publication of the Modified Certificate by the CA .....	19
4.8.7. Notification of Certificate Issuance by the CA to Other Entities .....	19
4.9. Certificate Revocation and Suspension.....	19
4.9.1. Circumstances for Revocation .....	19
4.9.2. Who Can Request Revocation .....	19
4.9.3. Procedure for Revocation Request.....	19
4.9.4. Revocation Request Grace Period.....	20
4.9.5. Time Within Which CA Must Process the Revocation Request .....	20
4.9.6. Revocation Checking Requirements for Relying Parties .....	20
4.9.7. CRL Issuance Frequency.....	20
4.9.8. Maximum Latency for CRLs .....	20
4.9.9. On-Line Revocation/Status Checking Availability .....	20
4.9.10. On-Line Revocation Checking Requirements.....	20
4.9.11. Other Forms of Revocation Advertisements Available .....	20
4.9.12. Special Requirements Re key Compromise .....	20
4.9.13. Circumstances for Suspension .....	20
4.9.14. Who Can Request Suspension .....	20

4.9.15. Procedure for Suspension Request.....	20
4.9.16. Limits on Suspension Period.....	20
4.9.17. Circumstances for Termination of Suspension.....	20
4.9.18. Who can Request Termination of Suspension.....	21
4.9.19. Procedure for Termination of Suspension.....	21
4.10. Certificate Status Services.....	21
4.10.1. Operational Characteristics.....	21
4.10.2. Service Availability.....	21
4.10.3. Operational Features.....	21
4.11. End of Subscription.....	21
4.12. Key Escrow and Recovery.....	21
4.12.1. Key Escrow and Recovery Policy and Practices.....	21
4.12.2. Session Key Encapsulation and Recovery Policy and Practices.....	21
5. Facility, Management, and Operational Controls.....	21
5.1. Physical Controls.....	21
5.1.1. Site Location and Construction.....	22
5.1.2. Physical Access.....	22
5.1.3. Power and Air Conditioning.....	22
5.1.4. Water Exposures.....	22
5.1.5. Fire Prevention and Protection.....	22
5.1.6. Media Storage.....	22
5.1.7. Waste Disposal.....	22
5.1.8. Off-Site Backup.....	23
5.2. Procedural Controls.....	23
5.2.1. Trusted Roles.....	23
5.2.2. Number of Persons Required per Task.....	23
5.2.3. Identification and Authentication for Each Role.....	23
5.2.4. Roles Requiring Separation of Duties.....	23
5.3. Personnel Controls.....	23
5.3.1. Qualifications, Experiences, and Clearance Requirements.....	23
5.3.2. Background Check Procedures.....	23
5.3.3. Training Requirements.....	24
5.3.4. Retraining Frequency and Requirements.....	24
5.3.5. Job Rotation Frequency and Sequence.....	24
5.3.6. Sanctions for Unauthorized Actions.....	24
5.3.7. Independent Contractor Requirements.....	24
5.3.8. Documentation Supplied to Personnel.....	24
5.4. Audit Logging Procedures.....	24
5.4.1. Types of Events Recorded.....	24
5.4.2. Frequency of Processing Log.....	24
5.4.3. Retention Period for Audit Log.....	24
5.4.4. Protection of Audit Log.....	25
5.4.5. Audit Log Backup Procedures.....	25
5.4.6. Audit Collection System (Internal vs. External).....	25
5.4.7. Notification to Event-Causing Subject.....	25
5.4.8. Vulnerability Assessments.....	25
5.5. Records Archival.....	25
5.5.1. Types of Records Archived.....	25
5.5.2. Retention Period for Archive.....	25
5.5.3. Protection of Archive.....	25
5.5.4. Archive Backup Procedures.....	26
5.5.5. Requirements for Time-Stamping of Records.....	26

5.5.6. Archive Collection System (Internal or External).....	26
5.5.7. Procedures to Obtain and Verify Archive Information.....	26
5.6. Key Changeover.....	26
5.7. Compromise and Disaster Recovery.....	26
5.7.1. Incident and Compromise Handling Procedures.....	26
5.7.2. Computing Resources, Software, and/or Data Are Corrupted .....	26
5.7.3. Entity Private Key Compromise Procedures.....	26
5.7.4. Business Continuity Capabilities After a Disaster .....	27
5.8. CA or RA Termination .....	27
6. Technical Security Controls .....	27
6.1. Key Pair Generation and Installation .....	27
6.1.1. Key Pair Generation.....	27
6.1.2. Private Key Delivery to Subscriber.....	28
6.1.3. Public Key Delivery to Certificate Issuer .....	28
6.1.4. CA Public Key Delivery to Relying Parties .....	28
6.1.5. Key Sizes.....	28
6.1.6. Public Key Parameters Generation and Quality Checking .....	28
6.1.7. Key Usage Purposes (as per X.509 v3 Key Usage Field).....	28
6.2. Private Key Protection and Cryptographic Module Engineering Controls.....	28
6.2.1. Cryptographic Module Standards and Controls .....	28
6.2.2. Private Key (n out of m) Multi-Person Control .....	28
6.2.3. Private Key Escrow.....	28
6.2.4. Private Key Backup .....	28
6.2.5. Private Key Archival.....	28
6.2.6. Private Key Transfer into or From a Cryptographic Module .....	29
6.2.7. Private Key Storage on Cryptographic Module .....	29
6.2.8. Method of Activating Private Key .....	29
6.2.9. Method of Deactivating Private Key.....	29
6.2.10. Method of Destroying Private Key .....	29
6.2.11. Cryptographic Module Rating.....	29
6.3. Other Aspects of Key Pair Management .....	29
6.3.1. Public Key Archival.....	29
6.3.2. Certificate Operational Periods and Key Pair Usage Periods .....	29
6.4. Activation Data .....	29
6.4.1. Activation Data Generation and Installation.....	29
6.4.2. Activation Data Protection .....	30
6.4.3. Other Aspects of Activation Data.....	30
6.5. Computer Security Controls.....	30
6.5.1. Specific Computer Security Technical Requirements.....	30
6.5.2. Computer Security Rating.....	30
6.6. Life Cycle Technical Controls .....	30
6.6.1. System Development Controls.....	30
6.6.2. Security Management Controls.....	30
6.6.3. Life Cycle Security Controls.....	30
6.7. Network Security Controls.....	30
6.8. Time-Stamping.....	31
7. Certificate, CRL, and OCSP Profiles .....	31
7.1. Certificate Profile.....	31
7.1.1. Version Number(s) .....	31
7.1.2. Certificate Extensions .....	31
7.1.3. Algorithm Object Identifiers .....	31
7.1.4. Name Forms .....	31
7.1.5. Name Constraints.....	31

7.1.6. Certificate Policy Object Identifier .....	31
7.1.7. Usage of Policy Constraints Extension .....	31
7.1.8. Policy Qualifiers Syntax and Semantics .....	31
7.1.9. Processing Semantics for the Critical Certificate Policies Extension .....	31
7.2. CRL Profile .....	31
7.2.1. Version Number(s) .....	31
7.2.2. CRL and CRL Entry Extensions .....	32
7.3. OCSP Profile .....	32
7.3.1. Version Number(s) .....	32
7.3.2. OCSP Extensions .....	32
8. Compliance Audit and Other Assessments .....	32
8.1. Frequency or Circumstances of Assessment .....	32
8.2. Identity/Qualifications of Assessor .....	32
8.3. Assessor's Relationship to Assessed Entity .....	32
8.4. Topics Covered by Assessment .....	32
8.5. Actions Taken as a Result of Deficiency .....	33
8.6. Communication of Results .....	33
9. Other Business and Legal Matters .....	33
9.1. Fees .....	33
9.1.1. Certificate Issuance or Renewal Fees .....	33
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 .....	34
9.2. Financial Responsibility .....	34
9.2.1. Insurance Coverage .....	34
9.2.2. Other Assets .....	34
9.2.3. Insurance or Warranty Coverage for End-Entities .....	34
9.3. Confidentiality of Business Information .....	34
9.3.1. Scope of Confidential Information .....	34
9.3.2. Information Not Within the Scope of Confidential Information .....	34
9.3.3. Responsibility to Protect Confidential Information .....	34
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 .....	35
9.4.5. Notice and Consent to Use Private Information .....	35
9.4.6. Disclosure Pursuant to Judicial or Administrative Process .....	35
9.4.7. Other Information Disclosure Circumstances .....	35
9.5. Intellectual Property Rights .....	35
9.6. Representations and Warranties .....	35
9.6.1. CA Representations and Warranties .....	35
9.6.2. RA Representations and Warranties .....	35
9.6.3. Subscriber Representations and Warranties .....	35
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 .....	36
9.10.1. Term .....	36

9.10.2. Termination .....	36
9.10.3. Effect of Termination and Survival .....	36
9.11. Individual Notices and Communications with Participants .....	36
9.12. Amendments.....	36
9.12.1. Procedure for Amendment .....	36
9.12.2. Notification Mechanism and Period.....	37
9.12.3. Circumstances Under Which OID Must be Changed .....	37
9.13. Dispute Resolution Procedures .....	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 .....	38
9.16.4. Enforcement (Attorney’s Fees and Waiver of Rights) .....	38
9.16.5. Force Majeure .....	38
9.17. Other Provisions.....	38
References.....	38

# 1. Introduction

This document defines the Certificate Policy for the root Certification Authority of the Republic of Estonia (hereinafter *Root CP*). The Root CP stipulates the procedural and operational requirements that the Certification Authority (hereinafter *CA*) adheres to when servicing the root certificate and issuing intermediate certificate.

Pursuant to the IETF RFC 3647 [1], the Root CP is divided into nine parts. To preserve the outline specified by IETF RFC 3647 [1], section headings that do not apply have the statement "Not applicable".

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

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

- Root CP;
- Root 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 Root CP covers the part highlighted in yellow.

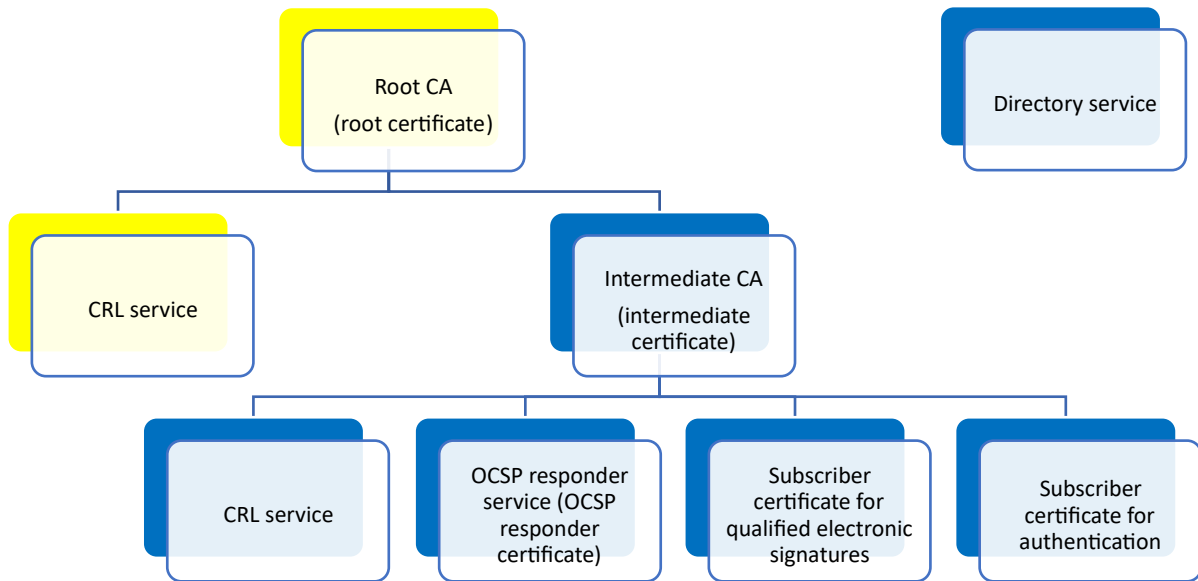


Figure 1. The CA hierarchy and related services for the Republic of Estonia.

## 1.2. Document Name and Identification

This document is titled “Certificate Policy of the root Certification Authority of the Republic of Estonia (Root CP)”. The Root CP is identified by the following Object Identifier (OID):

- 1.3.6.1.4.1.51361.3.

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
Service attribute	3

## 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 Root CP exclusively for the Republic of Estonia.

### 1.3.2. Registration Authorities

The contract partner of the PBGB shall fulfil the role of the Registration Authority (hereinafter *RA*).

### **1.3.3. Subscribers**

The contract partner of the PBGB shall fulfil the role of the Subscriber.

### **1.3.4. Relying Parties**

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

### **1.3.5. Other Participants**

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

The PBGB shall delegate one or more representatives of the PBGB to the key ceremony as a participant.

## **1.4. Certificate Usage**

### **1.4.1. Appropriate Certificate Uses**

The private keys of the root certificate shall only be used for signing the following objects:

- self-signed root certificate;
- intermediate certificate;
- CRL.

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

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

## **1.5. Policy Administration**

### **1.5.1. Organization Administering the Document**

The Root 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)

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

### **1.5.2. Contact Person**

Any questions and change proposals regarding the Root 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 QTSP PMA validates and determines the Root CPS conformity to the Root 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 Root CP annually, or if significant changes occur, to ensure the continuing suitability, adequacy and effectiveness of applicable standard to the current Root CP. Change proposals to the Root CP may be sent at any time to the CP contact person. The government Policy Administrator shall coordinate the changes to the Root CP with the CA and the RIA.

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

The amended Root CP, along with the enforcement date, shall be published electronically on the [www.id.ee](http://www.id.ee) website. The enforcement date shall be at least 30 (thirty) days after publication, unless there are special circumstances, which require a faster publication and enforcement date.

All amendments shall be approved by the Identity and Status Bureau of the PBGB and the eID department of RIA. The amended Root CP shall be enforced by the Deputy Director of the PBGB.

The government Policy Administrator shall notify the RIA and the CA when a new version of the Root CP is published 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.
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 Root CP.
Certification Authority's systems	A technical certificate generation service that is used by the Certification Authority to provide certification and qualified trust services.
Certification Practice Statement	One of the several documents that all together form the governance framework in which certificates are created, issued, managed, and used.

Conformity Assessment Body	A body defined in Regulation (EC) No 765/2008 [2], 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.
intermediate CA/certificate	Certification Authority whose certificate is issued by the root CA. Intermediate CA issues the Subscriber Certificates.
key ceremony	A procedure whereby a key pair is generated using a HSM and where the public key is certified.
OCSP responder service	A certificate status service on the basis of OCSP.
Policy Management Authority (PMA)	The PMA is the internal management and governance body of the QTSP.
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.
qualified trust service	An electronic service as defined in the eIDAS Regulation [4]. In the context of Root CP, qualified trust service consists of services provided by a qualified trust service provider according to the eIDAS Regulation [4] which consists of the creation, verification, and validation of qualified electronic certificates.
Relying Party	Legal or natural person who is making decisions based on the certificates.
root CA/certificate	Highest level Certification Authority, which is identified by the root certificate. The root CA issues certificate for the intermediate CA.
Subscriber Certificates	A uniform term for a certificate that enables digital authentication and a certificate that enables creation of qualified electronic signatures.
Supervisory Body	An entity who is carrying out the supervision over the compliance with the requirements established for trust service providers pursuant to the EUTS Act [3]. In the Republic of Estonia, a Cyber Security Branch of RIA is holding the role of the Supervisory Body.
trust service provider	An organisation that provides trust service(s).

### 1.6.2. Acronyms

Acronym	Definition
CA	Certification Authority
CA systems	Certification Authority's systems
CN	Common Name

CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List, a list of invalid (revoked) certificates
DN	Distinguished Name
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 [4]
EU	European Union
HSM	Hardware Security Module
OCSP	Online Certificate Status Protocol
OID	Object Identifier, a unique object identification code
PBGB	Police and Border Guard Board
PMA	Policy Management Authority
RIA	Information System Authority
Root CP	Certificate Policy of the root Certification Authority of the Republic of Estonia, this document
Root CPS	Certification Practice Statement of the root Certification Authority of the Republic of Estonia

## 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 Certificate 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:

- Root CPS;
- Certificate Profiles;
- the terms and conditions for the use of CRL service.

The CA shall publish the following CA certificates on the CA's repository:

- root certificate;
- intermediate certificates.

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

- Root CP.

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 Root CP in the CA's repository.

Any changes to the Root CPS, the Certificate Profiles and the terms and conditions for the use of CRL service shall be approved by the 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 and the PBGB may be left out of the Root CPS. Information about confidential internal procedures of the CA or PBGB shall be left out of the Root CPS.

## **2.3. Time or Frequency of Publication**

Documentation referred to in clause 2.2.1. of the Root CP shall be published at least 30 days prior to coming into force, unless there are special circumstances, which require a faster publication and enforcement date.

## **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**

Issuer distinguished name (hereinafter *DN*) shall be identified as follows:

- Common Name (CN)
  - CN of the root CA shall be EEGovCAYYYY, unless there is a need to issue more than one root CA in the same year. If more than one root CA is issued in a given year, then the subsequent root CA(s) will include a serial number (i.e. EEGovCAYYYY, EEGovCAYYYY01, EEGovCAYYYY02 etc.);
  - CN of the intermediate CA shall be ESTEIDYYYY, unless there is a need to issue more than one intermediate CA in the same year. If more than one intermediate CA is issued in a given year, then the subsequent intermediate CA(s) will include a serial number (i.e. ESTEIDYYYY, ESTEIDYYYY01, ESTEIDYYYY02 etc.);
  - YYYY refers to the year of the issuance.
- Organisation Identifier shall be according to clause 5.1.4 of ETSI EN 319 412-1 [5];
- Organisation shall include the name of the CA;
- Country shall be the alpha-2 country code for the Republic of Estonia as defined in ISO 3166 [6].

Types of names are set in the Certificate Profiles.

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

All the names in the certificates shall be meaningful.

### **3.1.3. Anonymity or Pseudonymity of Subscribers**

Anonymity and pseudonymity of the Subscribers shall not be allowed.

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

Rules for interpreting various name forms are set in the Certificate Profiles.

### **3.1.5. Uniqueness of Names**

Multiple certificates with identical DNs shall not be valid at the same time.

### **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**

Possession of the private key shall be guaranteed by the key ceremony procedures of the CA. The private key shall be generated under the supervision of the representative of the PBGB and shall be witnessed by an independent auditor.

### **3.2.2. Authentication of Organisation Identity**

Organisation identity shall be identified by the Organisation Identifier in the certificate. Refer to clause 3.1.1. of the Root CP.

### **3.2.3. Authentication of Individual Identity**

An independent auditor shall identify and verify the authorisation of the CA personnel and the representative of the PBGB in the beginning of the key ceremony.

### **3.2.4. Non-verified Subscriber Information**

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

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

At a minimum, 4 (four) personnel of the CA shall be assigned for different roles in the key ceremony. The head of the CA shall authorise the personnel of the CA for specific roles for every key ceremony. The Director General of the PBGB shall authorise the representative of the PBGB to participate in and to supervise the key ceremony.

### **3.2.6. Criteria for Interoperability**

Not applicable.

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

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

Not applicable.

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

Not applicable.

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

Refer to clause 3.2.3. of the Root CP. Revocation requests shall be authenticated to verify that the revocation has been requested by an authorised entity according to the EUTS Act [3]. Acceptable procedures for authenticating the revocation shall be implemented.

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

### **4.1. Certificate Application**

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

The authorised personnel of the CA can submit the certificate application.

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

The CA shall describe and define all procedures and required roles in the internal documentation. The certificate key generation shall adhere to the principle of shared responsibility, i.e. it shall be made sure that no individual PKI participant alone, has the access to all assets necessary to generate CA keys and CA certificates. The CA keys may only be generated under supervision of the representative of the PBGB. CA certificates may only be generated under supervision of the representative of the PBGB. CA certificates may only be listed on the Trusted List of the Republic of Estonia under the approval of the PBGB.

Prior to the key ceremony, the independent auditor shall identify the participants of the key ceremony and their authorisation. Every key ceremony shall be recorded in the protocol and signed by all participants.

### **4.2. Certificate Application Processing**

The CA shall describe the certificate application processing in the Root CPS.

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

Refer to clause 3.2.3. of the Root CP.

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

Only the certificate applications that are submitted during the key ceremony by the authorised personnel of the CA shall be approved. The certificate applications that are not submitted during the key ceremony or by authorised personnel for the role shall be rejected.

#### **4.2.3. Time to Process Certificate Applications**

The time to process the certificate applications shall be determined by the CA in the Root CPS.

### **4.3. Certificate Issuance**

#### **4.3.1. CA Actions During Certificate Issuance**

The certificate shall be issued manually from the CA system according to the CA's internal documentation. The certificates shall be valid from the moment of issuance unless otherwise agreed upon with the PBGB. The end of validity of the intermediate certificate shall not exceed the validity of the root certificate. After issuance of the intermediate certificate, the root CA shall sign a new CRL and a backup of the database shall be made.

#### **4.3.2. Notification to Subscriber by the CA of Issuance of Certificate**

Every key ceremony shall be recorded in the protocol and signed by all participants.

### **4.4. Certificate Acceptance**

#### **4.4.1. Conduct Constituting Certificate Acceptance**

The CA and the representative of the PBGB shall verify that the issued certificate is correct during the key ceremony.

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

The certificates shall be published in the CA's repository.

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

Refer to clause 4.4.2. of the Root CP.

### **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 certificate in accordance with the Root CP and Root CPS.

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

The Relying Party shall use the public key and the certificate in accordance with the Root CP and Root CPS.

### **4.6. Certificate Renewal**

Certificate renewal is not allowed.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Certificate re-key is not allowed.

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

Not applicable. Refer to clause 4.7. of the Root CP.

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

Not applicable. Refer to clause 4.7. of the Root CP.

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

Not applicable. Refer to clause 4.7. of the Root CP.

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

Not applicable. Refer to clause 4.7. of the Root CP.

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

Not applicable. Refer to clause 4.7. of the Root CP.

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

Not applicable. Refer to clause 4.7. of the Root CP.

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

Not applicable. Refer to clause 4.7. of the Root CP.

## **4.8. Certificate Modification**

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

Certificate modification is not allowed.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Circumstances for certificate revocation are the following:

- The private key corresponding to a public key contained in the certificate has been or may possibly be used without the consent of the certificate owner;
- The activities of the qualified trust service provider are terminated;
- Appearance of an error in the data entered in the certificate or in the certificate itself;
- Other cases provided by the applicable law.

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

An authorised entity according to the EUTS Act [3] can request certificate revocation.

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

A revocation request shall be submitted to the head of the CA. The CA shall verify the correctness and applicability of the presented evidences and other available information in accordance with the internal revocation process document agreed upon between the CA and the PBGB. If it is determined that the revocation request is legitimate and justified, the root CA shall revoke the relevant certificate and sign a CRL that contains information about the revoked intermediate certificate in accordance with the aforementioned document. The CA shall immediately notify the PBGB, the Estonian Supervisory Body and where applicable, other relevant authorised entities.

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

Not applicable.

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

The revocation requests initiated by the authorised entity shall be processed immediately after the correctness and applicability of the revocation has been verified and/or upon agreement with the PBGB.

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

Relying Parties can verify the revocation of the intermediate certificate against the CRL service.

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

At a minimum, the root CA shall sign a new CRL once a year. In case of intermediate certificate revocation, the root CA shall immediately sign a new CRL that contains information about the revoked intermediate certificate.

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

The CRL shall be published immediately, but no later than 1 (one) business day after the issuance.

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

Not applicable.

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

Not applicable.

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

Not applicable.

#### **4.9.12. Special Requirements Re key Compromise**

Not applicable.

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

Not applicable.

#### **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**

Not applicable.

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

Not applicable.

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

Not applicable.

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

Not applicable.

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

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

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 a 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.

#### **4.10.3. Operational Features**

Not applicable.

### **4.11. End of Subscription**

The subscription ends when the certificate is revoked, expired or the CA terminates its operation.

### **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 and the CA systems shall be compliant with ISO/IEC 27001 [7], ETSI EN 319 411-2 [8], ETSI EN 319 411-1 [9] and ETSI EN 319 401 [10].

### **5.1. Physical Controls**

The CA shall control physical access to any part of their system that is critical to providing certification and qualified trust services. The CA shall minimize risks that are related to physical security and shall implement controls to avoid loss, damage, theft, compromise of assets and information.

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

Any critical components for the secure operation of the certification and qualified trust services shall be located in a protected security perimeter. The security perimeter shall have physical protections in place to prevent intrusions, shall have alarms to detect intrusions, and shall have access control in place. All key ceremonies and related activities shall be held at the secure area, which is located on the territory of the Republic of Estonia unless otherwise agreed upon with the PBGB.

### **5.1.2. Physical Access**

All entries to any physically secure areas shall be subject to the CA independent oversight and procedures shall be implemented to ensure that any non-authorized person shall be accompanied by an authorized person at all times. All entries and exits shall be logged.

Access to any part of the CA's system that is critical to providing certification and qualified trust services shall be limited to authorized individuals only. The location, in which certificate management services are provided, shall have a clearly defined security perimeter around it.

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

The CA shall ensure that the CA systems shall have a power supply that ensures both temporary and continuous supply of electricity, and that the CA systems shall have heating, ventilation, and air conditioning systems that control temperature and relative moisture. The CA shall have an environmental and physical security policy for any systems concerned with the certificate management services.

### **5.1.4. Water Exposures**

The CA shall have an environmental and physical security policy for any systems concerned with the certificate management services, which shall address measures to prevent water exposure.

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

The CA shall comply with the local fire safety regulations and have an environmental and physical security policy for any systems concerned with the certificate management services, which shall address fire prevention and protection.

### **5.1.6. Media Storage**

The CA shall implement controls that prevent any equipment, information, media, or software relating to the CA's services from being taken off-site without authorisation. Data storage media shall be protected against unauthorised or unintended use, access, disclosure, or damage by people or other threats (e.g. fire, water). Media containing sensitive data shall be stored only in a special fireproof safe designed for storing data media.

### **5.1.7. Waste Disposal**

Media containing sensitive data shall be securely disposed when no longer required in order to avoid unauthorised use, access or disclosure.

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

The CA shall perform regular backups of all critical system data, sensitive information, and audit log data in their systems. The CA shall have processes in place where the most critical information is kept off site in secure storage.

## **5.2. Procedural Controls**

### **5.2.1. Trusted Roles**

At a minimum, trusted roles shall include: security officers, system administrators, system operators, system auditors, registration officers, and revocation officers. Trusted roles involved in certificate management services shall be free from any commercial, financial, or other pressures which may influence trust in the services that the CA provides.

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

The following activities shall be under the control of at least two authorised, trusted personnel:

- Certificate issuance by the root CA;
- Generation of Root CA certification keys;
- Backup of certification keys;
- Restoration of certification keys;
- Management of HSMs and the CA core systems;
- Physical visits to data centres;
- Destruction of data.

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

Personnel of the CA shall be identified and authenticated before using any critical applications related to the certification and qualified trust services. Personnel shall be accountable for their actions and all actions relating to critical applications for certification and qualified trust services shall be logged.

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

Separation of trusted roles identified in clause 5.2.1. of the Root CP shall be required. Separation of duties includes, but is not limited to, the separation of security administration and operation functions. Separation of roles for actions described in clause 5.2.2. of the Root CP shall be enforced.

## **5.3. Personnel Controls**

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

The CA systems shall be operated and governed by personnel who are competent, experienced and authorized, in order to ensure the trustworthiness of the trust service provided. Personnel shall have the necessary expertise, reliability, experience, and qualifications as required by the eIDAS Regulation [4].

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

An employee of the CA shall not have been punished for an intentional crime. During initial hiring or appointing of roles, personnel shall not have access to certification and trusted

functions until background checks are completed. Reoccurring background checks shall be done on a periodic basis on existing employees.

### **5.3.3. Training Requirements**

The CA's personnel shall have expert knowledge, experience, and qualifications, which may be obtained through formal training and credentials or through experience.

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

The CA's personnel shall receive regular, reoccurring training at least once every 12 (twelve) months. Training shall consist of updates on best current security practices as well as on threat updates.

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

No job rotation shall be established.

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

The CA shall inform the PBGB and the Supervisory Body of any unauthorised actions upon discovery of such actions. Appropriate disciplinary sanctions shall be applied to personnel who violate the CA's policies or procedures.

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

The CA may employ subcontractors if applicable. Subcontractors shall adhere to the same background check, training, qualifications, and expertise requirements as the CA's personnel.

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

The CA shall provide their personnel the necessary training and other related documentation to perform their duties. Job responsibilities and security related roles shall be documented in documents that are available to all concerned personnel (may be in the form of job descriptions).

## **5.4. Audit Logging Procedures**

The CA shall perform audit logging procedures in compliance with the eIDAS Regulation article 24 [4] and applicable ETSI and ISO standards.

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

In their systems, the CA shall implement logging solutions to analyse and detect any proper and improper use of the system and provide evidence for legal proceedings. All relevant information concerning the operation and security of the system shall be recorded.

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

The CA shall ensure that audit logs are regularly reviewed and analysed.

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

All logs shall be retained for time periods required by applicable standards, regulatory, CA's risk assessment and as necessary for any legal proceedings. The CA shall state the period of retention for each type of record in the Root CPS.

The CA shall maintain information beyond the termination of the CA to meet legal requirements as required by the eIDAS Regulation [4].

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

Audit logs shall be protected against deletion, modification, unauthorized view, and other damage. Should the audit logs concerning the operation or security of the system be required for the purposes of providing evidence of the correct operation of the certification and qualified trust services and for the purpose of legal proceedings, they shall be made available to legal authorities and/or persons whose right of access to them arises from the law.

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

The CA shall perform regular backups of audit log data and critical system data within their systems.

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

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

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

The event causing subjects shall be notified about all security relevant events caused by his or her actions.

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

The CA shall perform regular vulnerability assessments of their systems, based on data logs. The results of the vulnerability assessment shall be documented.

### **5.5. Records Archival**

The CA shall ensure that records related to the operation of certification and qualified trust services are completely and confidentially archived in accordance with disclosed business practices. Records shall be archived in a manner that they can be made available for legal proceedings to provide evidence of the correct operation of the CA's services.

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

The CA shall retain all events relating to the life cycle of keys managed by the CA, including the subject key pairs that are generated by the CA. The CA shall state the types of records archived in the Root CPS.

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

The CA shall retain the records for at least 10 (ten) years from the date any certificate based on these records ceases to be valid.

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

The archive shall be protected from deletion or modification of records, against unauthorised view or access, and against other damage. The media holding the archive data and the applications required to process the archive data are maintained properly to ensure that the archive data can be accessed for the time period required.

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

The CA shall implement appropriate records archival procedures. Procedures shall ensure the integrity, authenticity and confidentiality of the data.

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

Records shall contain the precise date and time of event.

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

The CA shall describe the type of archival collection system used in the Root CPS.

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

Only authorised personnel in trusted roles shall access the archive. Information shall be made available to legal authorities for the purpose of legal proceedings, as long as their right to access information is in accordance with Estonian and EU legislation. The CA shall ensure the integrity of information is maintained and verified.

### **5.6. Key Changeover**

The public key of the root and intermediate certificate shall not change. CN shall always contain the number of the year it was issued.

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

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

The CA shall have a business continuity plan for incident and compromise handling procedures in line with the eIDAS Regulation [4], GDPR [11], applicable international standards, the EUTS Act [3], and the Emergency Act [12].

In line with the above-mentioned legislation, the CA shall develop notification procedures to notify the appropriate parties in case of breach of security, in case of loss of integrity, and in cases where personal data has been compromised.

The CA's business continuity plan shall ensure that damage from any security incidents and compromises are minimized and interrupted certification and qualified trust services are restored without delay.

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

The CA shall have a documented plan in place for when computing resources, software, and/or data are corrupted to ensure the potential impact from the corruption is minimized.

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

The CA shall include the process for an entity private key compromise (or suspected or potential compromise) procedures in their business continuity plan or in their disaster recovery plan. The incident report and the solution of the security problem having caused the incident shall be documented.

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

The CA shall have at least one back-up facility to ensure all essential information and software can be recovered following a disaster. The CA shall be able to resume CA operations in a timely manner. The CA shall include the process and plans for business continuity after a disaster in their business continuity plan.

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

As required by the eIDAS Regulation [4] and the EUTS Act [3], the CA shall have a termination plan to ensure continuity of service with the least impact on Relying Parties. The termination plan shall be reviewed and updated on a regular basis.

At a minimum, the CA termination plan shall include the following:

- Before termination, the CA shall inform all Subscribers, Relying Parties, Supervisory Bodies, and other entities who have agreements or relations with the CA of the plans to terminate;
- Before termination, the CA shall also make the information related to termination available to other Relying Parties who are not already notified (example: posting on website, media notification, etc.);
- Before termination, the CA shall revoke authorization of all subcontractors who act on behalf of the CA in functions related to issuing certificates;
- Before termination, the CA shall transfer obligations to the PBGB or entity determined by the PBGB for maintaining all information necessary for a reasonable period for the purpose of providing proof of the CA's operations;
- Before termination, the CA's private keys and back-up copies shall be destroyed or withdrawn from use in a manner where the keys cannot be retrieved, or the PBGB shall instruct the keys to be transferred over to an entity appointed by the PBGB;
- Before termination, where possible, the CA shall make arrangements to transfer provisions of certification and qualified trust services of existing customers to another QTSP that the Republic of Estonia chooses to ensure the continuity of service.

To the extent possible within the constraints of applicable legislation, the CA shall ensure they have the necessary arrangements to ensure financing is available to fulfil the above minimum requirements in case of bankruptcy or other financial strain.

## **6. Technical Security Controls**

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

The CA shall follow the industry best practices for key lifecycle management, key length and algorithms.

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

Key pair generation shall be performed using trustworthy systems and processes that provide the required cryptographic strength of the generated keys, and prevent the loss, disclosure, modification, or unauthorised use of such keys. The CA shall use an off-line HSM that meets at least the requirements established in the security standard FIPS PUB 140-2 Level 3 or another agreed upon security standard for key pair generation and storage. The HSM protects the keys

from external compromise and shall be operated in a physically secure environment. All key pair generation procedures shall be documented.

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

The private key is delivered during the key ceremony.

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

The public key is delivered during the key ceremony.

#### **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**

Allowed key sizes are set in the Certificate Profiles.

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

Refer to clause 6.1.1. of the Root CP. The quality of the generated keys shall be checked by the CA personnel during the key ceremony.

#### **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**

Refer to clause 6.1.1. of the Root CP. The CA shall ensure the security of HSMs throughout its lifecycle.

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

Dual control for private key activation shall be applied to procedures where the private key is used for signing.

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

Private key escrow is not allowed.

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

CA private keys shall be backed up to guarantee continuity of service. Backup shall be performed during the key ceremony.

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

The CA systems shall not archive its private keys after expiration.

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

All key pairs shall be generated in the HSM. Key pairs may be transferred between the HSMs for backup purposes, HSM resynchronization and for resolving an incident only. The requirements in section 6.2.4 of the Root CP shall apply.

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

Private keys shall be stored in the HSM in encrypted form.

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

Private keys shall be activated according to the specifications of the HSM manufacturer. The requirements in section 6.2.2. of the Root CP shall apply.

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

Private keys shall be deactivated according to the specifications of the HSM manufacturer.

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

Private keys shall be destroyed by using the methods of the HSM manufacturer.

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

Refer to clause 6.2.1. of the Root CP. The cryptographic modules used by the CA shall be evaluated and certified in accordance FIPS PUB 140-2 Level 3 or another agreed upon security standard.

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

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

All issued (including expired and revoked) certificates shall be retained and archived during routine backup procedures. The retention period shall be in accordance with the eIDAS Regulation [4], EUTS [3] and applicable standards.

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

The operational period of a certificate ends upon revocation or expiry.

The key pair of the intermediate certificates shall not be used beyond the end of the root certificate lifecycle. The CA is not allowed to issue intermediate certificates which exceed the lifetime of the root certificate that issued the intermediate certificate. The issuance of the new intermediate certificates shall stop at an appropriate date prior to the expiration of the root certificate so that no intermediate certificate expires after the expiration of the root certificate.

## **6.4. Activation Data**

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

HSM data generation and installation shall be performed according to the user manual of HSM.

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

Only authorised personnel shall have access to the HSM and HSM activation data. HSM activation data shall be kept secret and in a safe at all times unless there is a HSM to be activated or deactivated.

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

Not applicable.

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

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

The CA systems, including software components, shall be secure and correctly operated, with an acceptable risk of failure. Change procedures shall include system testing in test environment and all changes shall be approved by an authorised personnel of the CA. Approval shall be documented for further reference. All software components shall be installed and updated from trusted sources only. Procedures to protect the integrity of software components against viruses, malicious and unauthorised software shall be implemented. All media containing production environment software and data, audit, archive, or backup information shall be stored with appropriate physical and logical access controls. Sufficient computer security controls for the separation of roles identified in the Root CP shall be provided. Access shall be restricted only allowing access to personnel as necessary for carrying out the specific role.

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

Standard computer systems shall be used.

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

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

The configuration of the CA systems as well as any modifications and upgrades shall be documented and controlled. A mechanism for detecting unauthorised modification to software or configuration shall be implemented. New version of software shall be tested in test environment of the appropriate service and deployment shall be conducted according to documented change management procedures.

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

The CA shall implement security management controls to verify the integrity of software components.

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

New available security patches shall be applied to software components each time when the root CA is activated. The reasons for not applying any security patch shall be documented.

### **6.7. Network Security Controls**

The requirements on network security in ETSI EN 319 401 [10] and ETSI EN 319 411-1 [9] shall apply.

## **6.8. Time-Stamping**

No stipulation.

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

## **7.1. Certificate Profile**

The certificates shall be issued in accordance with X.509 version 3, IETF RFC 5280 [13], IETF RFC 5480 [14], IETF RFC 5639 [15] and ETSI EN 319 411-1 [9] and ETSI EN 319 411-2 [8]. The root certificate and intermediate certificate profiles are set in the Certificate Profiles.

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

Refer to clause 7.1. of the Root CP.

### **7.1.2. Certificate Extensions**

Refer to clause 7.1. of the Root CP.

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

Refer to clause 7.1. of the Root CP.

### **7.1.4. Name Forms**

Refer to clause 7.1. of the Root CP.

### **7.1.5. Name Constraints**

Refer to clause 7.1. of the Root CP.

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

Refer to clause 7.1. of the Root CP.

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

Refer to clause 7.1. of the Root CP.

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

Refer to clause 7.1. of the Root CP.

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

Refer to clause 7.1. of the Root CP.

## **7.2. CRL Profile**

The CRL shall be issued in accordance IETF RFC 5280 [13], IETF RFC 5480 [14], IETF RFC 5639 [15], ETSI EN 319 411-1 [9], and ETSI EN 319 411-2 [8]. The CRL profile is set in the Certificate Profiles.

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

Refer to clause 7.2. of the Root CP.

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

Refer to clause 7.2. of the Root CP.

## **7.3. OCSP Profile**

Not applicable.

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

Not applicable.

### **7.3.2. OCSP Extensions**

Not applicable.

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

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

The conformity of information system, policies and practices, facilities, personnel, and assets of the CA are assessed by a Conformity Assessment Body pursuant to the eIDAS Regulation [4]. Assessments are done at least once every 24 (twenty four) months in accordance with the applicable legislation and standards. Assessments shall also be done whenever a major change is made to the operation of certification and qualified trust services covered in the applicable CP and/or CPS, or when requested by the Supervisory Body.

The CA shall also have an internal audit plan and shall carry out regular internal audits. Internal audits shall be performed at least once every 12 (twelve) months, or shall be performed within a 12-month period for a rolling or segmented internal audit.

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

Assessments are done by a Conformity Assessment Body. A Conformity Assessment Body shall be accredited in accordance with Regulation EC no 765/2008 [2], as competent to carry out conformity assessments of a qualified trust service provider and the certification and qualified trust services it provides.

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

The lead auditor of the Conformity Assessment Body shall be independent from the participants to the certification services and assessed systems. For internal audits, the auditor(s) of the CA shall not audit their own areas of responsibility.

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

Conformity assessments shall be done in compliance with the eIDAS Regulation [4], respective legislation, and applicable standards.

The first stage of the conformity assessment shall cover the conformity of documentation. Documentation assessed may include, but is not limited to:

- Root CP;
- Root CPS;
- business continuity, disaster recovery and termination plan;
- applicable technical documentation;
- documentation related to the qualified trust service provider (facilities, services, etc.);
- evidence of secure and compliant operations (i.e. logs and protocols).

The second stage of the conformity assessment shall be an on-site audit. The on-site audit shall demonstrate compliance with the documents assessed in the first stage, compliance with applicable legislation, and compliance with applicable standards. This may include, but is not limited to: assessment of facilities, personnel, processes, procedures, products related to qualified trust services, information systems used to provide certification and qualified trust services, etc.

The following topics shall be covered by internal audits:

- quality of service;
- security of service;
- security of operations and procedures;
- security policies, performance of work procedures and contractual obligations, and the compliance with the Root CP and the Root CPS.

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

In the event of a result showing deficiency in the assessment, the Supervisory Body shall require the CA to remedy any failure to fulfil compliance requirements within a set time limit. The CA shall do what is necessary to stay compliant and shall fulfil all requirements of the deficiency by the set date(s). The CA shall be responsible for the implementation of a corrective action plan. The CA shall evaluate the significance of each deficiency, taking into account the Supervisory Body's requirements and the Conformity Assessment Body's recommendations, and shall prioritize the order of actions to be taken. Where personal data protection rules appear to have been breached, the Supervisory Body shall inform the data protection authority of the results of the compliance audit.

## **8.6. Communication of Results**

The CA shall submit the resulting conformity assessment report to the Supervisory Body and to the PBGB within 3 (three) business days of receiving it. Conformity assessment attestation letter(s) and certificate(s) for qualified trust services shall also be published on the CA's repository.

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

## **9.1. Fees**

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

The fee for the certificate issuance shall be laid down in mutual agreements between the CA and the PBGB.

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

Valid intermediate certificates shall be available via the CA's repository free of charge.

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

Revocation of the certificate shall be free of charge.

The certificate validity and information about the revoked intermediate 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 and the PBGB.

### **9.1.5. Refund Policy**

Refund shall be treated on a case-by-case basis, while taking into account the provisions of the contract between the CA and the PBGB.

## **9.2. Financial Responsibility**

### **9.2.1. Insurance Coverage**

To cover compensation for damages, the CA shall obtain liability insurance as required by Article 13 and Article 24 of the eIDAS Regulation [4] and the EUTS Act [3]. In accordance with the EUTS Act [3], the CA shall publish information on the existence of liability insurance and insurance coverage.

### **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**

Any information that the CA is made aware of in the course of offering certification and qualified trust services that is not provided for publication and provided only for internal use of the CA, in accordance with applicable laws and regulations, shall be confidential.

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

Any information that is not confidential by nature or listed as confidential or that is not intended for internal use only, shall be public information. The CA shall include a list of information considered public in the Root CPS.

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

Security controls and internal training shall be implemented to secure confidential information and information intended for internal use from compromise and unintentional disclosure to third

parties. Disclosure or forwarding of confidential information to a third party is permitted only with the written consent of the legal possessor of the information, on the basis of a court order or in other cases provided by law.

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

The participants to the certification services and the CA systems shall comply with GDPR [11], the Personal Data Protection Act [16], the eIDAS Regulation [4], and related standards.

### **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**

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

## **9.6. Representations and Warranties**

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

Employees and contractors shall not have been convicted for an intentional crime and the CA shall ensure that their employees and subcontractors support the trustworthiness of the certification and qualified trust services provided. The CA shall ensure their administrative and management procedures correspond to industry recognized EU and international standards.

### **9.6.2. RA Representations and Warranties**

Not applicable.

### **9.6.3. Subscriber Representations and Warranties**

Refer to clause 9.6.1. of the Root CP.

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

A Relying Party shall verify the validity of the intermediate certificate using the validation service offered by the CA, prior to relying on the intermediate certificate.

A Relying Party shall consider the limitations stated in the intermediate certificate and shall ensure that the transaction to be accepted corresponds to the Root CP.

A Relying Party shall comply with the eIDAS Regulation [4] and the GDPR [11] when relying on the certificate chain.

#### **9.6.5. Representations and Warranties of Other Participants**

Not applicable.

### **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 Root CP.

#### **9.10.2. Termination**

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

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

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

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

Refer to clause 1.5.2. of the Root CP.

## **9.12. Amendments**

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

Refer to clause 1.5.4. of the Root CP.

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

Refer to clause 1.5.4. of the Root 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 the issuance of certificates).

## **9.13. Dispute Resolution Procedures**

No stipulation.

## **9.14. Governing Law**

The Root 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 [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, 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 [17].
- 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 [2].
- GDPR [11] – 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,
- EUTS [3] – Electronic Identification and Trust Services for Electronic Transactions Act,
- IDA [18] – Identity Documents Act,
- State Fees Act [19],
- Personal Data Protection Act [16],
- Emergency Act [12],
- Consular Act [20],
- Cybersecurity Act [21],
- 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 [10] – Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers,

- ETSI EN 319 411-1 [9] – Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements,
- ETSI EN 319 411-2 [8] – 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 319 412-2 [22] – Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons.
- 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] 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>

[2] 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>

[3] Electronic Identification and Trust Services for Electronic Transactions Act, 26.10.2016. Published: <https://www.riigiteataja.ee/en/eli/527102016001/consolide/current>

[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, 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>.

[5] ETSI EN 319 412-1 Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures. Published: <https://www.etsi.org/>

[6] ISO 3166 Codes for the representation of names of countries and their subdivisions

[7] ISO/IEC 27001 Information technology - Security techniques - Information security management systems – Requirements

[8] 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/>

[9] 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/>

[10] ETSI EN 319 401 Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers. Published: <https://www.etsi.org/>

[11] 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>

[12] Emergency Act, RT I, 03.03.2017, 1. Published:

<https://www.riigiteataja.ee/en/eli/ee/505012018004/consolide/current>

[13] 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>

[14] IETF RFC 5480 – Request for Comments: 5480, Elliptic Curve Cryptography Subject Public Key Information. Published: <https://www.ietf.org/rfc/rfc5480.txt>

[15] 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>

[16] Personal Data Protection Act, 15.01.2019. Published:

<https://www.riigiteataja.ee/en/eli/ee/523012019001/consolide/current>

[17] 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)

[18] Identity Documents Act, RT I – 1999, 25, 365. Published:

<https://www.riigiteataja.ee/en/eli/ee/521062017003/consolide/current>

[19] State Fees Act. Published:

<https://www.riigiteataja.ee/en/eli/ee/519022016005/consolide/current>

[20] Consular Act, RT I 2009, 29, 175. Published:

<https://www.riigiteataja.ee/en/eli/ee/527012016004/consolide/current>

[21] Cybersecurity Act. Published: <https://www.riigiteataja.ee/en/eli/523052018003/consolide>

[22] 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/>