Title:	**Zetes Estonia OÜ - Certification Practice Statement for the Root CA for ID-1 Documents of the Republic of Estonia**
Label:	**[ZE CPS-ID1-ROOT-CA]**
Document OID:	**[1.3.6.1.4.1.47718.3.11].01**
Category:	**Practice Statements and Policies**
Version:	**2.0**
Status:	**Approved**
Effective date:	**17/07/2026**
Organisation:	**Zetes Estonia OÜ**
Classification	**PUBLIC**

Table of Content

1 INTRODUCTION 7
1.1 Overview 7
1.2 Document name and identification 7
1.3 PKI Participants 7
1.3.1 Certification Authority (CA) 7
1.3.2 Registration Authorities (RA) 7
1.3.3 Subjects and Subscribers 7
1.3.4 Relying Parties 8
1.3.5 Other Participants 8
1.4 Certificate Usage 8
1.4.1 Appropriate Certificate uses 8
1.4.2 Prohibited Certificate uses 8
1.5 Policy administration 8
1.5.1 Organisation administering the document 8
1.5.2 Contact person 8
1.5.3 Person determining suitability for the policy 8
1.5.4 Approval procedures 8
1.6 Definitions and acronyms 8
1.6.1 Definitions 8
1.6.2 Acronyms 8
1.6.3 References 8

2 PUBLICATION AND REPOSITORY RESPONSIBILITIES 9
2.1 Repositories 9
2.2 Publication of certification information 9
2.3 Time or frequency of publication 9
2.4 Access controls on repositories 9

3 IDENTIFICATION AND AUTHENTICATION 10
3.1 Naming 10
3.1.1 Types of names 10
3.1.2 Need for names to be meaningful 10
3.1.3 Anonymity or pseudonymity of subscribers 10
3.1.4 Rules for interpreting various name forms 10
3.1.5 Uniqueness of names 10
3.1.6 Recognition, authentication, and role of trademarks 10
3.2 Initial identity validation 10
3.2.1 Method to prove possession of private key 10
3.2.2 Authentication of organization identity 10
3.2.3 Authentication of individual identity 10
3.2.4 Non-verified subscriber information 11
3.2.5 Validation of authority 11
3.2.6 Criteria for interoperation 11
3.3 Identification and authentication for re-key requests 11
3.3.1 Identification and authentication for routine re-key 11
3.3.2 Identification and authentication for re-key after revocation 11
3.4 Identification and authentication for revocation requests 11

4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS 12
4.1 Certificate application 12
4.1.1 Who can submit a Certificate application 12
4.1.2 Enrolment process and responsibilities 12
4.2 Certificate application processing 12
4.2.1 Performing identification and authentication functions 12
4.2.2 Approval or rejection of Certificate applications 12
4.2.3 Time to process Certificate applications 12
4.3 Certificate Issuance 13
4.3.1 CA actions during Certificate issuance 13
4.3.2 Notification to subscriber by the CA of issuance of Certificate 13
4.4 Certificate acceptance 13

4.4.1 Conduct constituting Certificate acceptance 13
4.4.2 Publication of the Certificate by the CA 13
4.4.3 Notification of Certificate issuance by the CA to other entities 13
4.5 Key pair and Certificate usage 13
4.5.1 Subscriber private key and Certificate usage 13
4.5.2 Relying party public key and Certificate usage 14
4.6 Certificate renewal 14
4.6.1 Circumstance for Certificate renewal 14
4.6.2 Who may request renewal 14
4.6.3 Processing Certificate renewal requests 14
4.6.4 Notification of new Certificate issuance to subscriber 15
4.6.5 Conduct constituting acceptance of a renewal Certificate 15
4.6.6 Publication of the renewal Certificate by the CA 15
4.6.7 Notification of Certificate issuance by the CA to other entities 15
4.7 Certificate re-key 15
4.7.1 Circumstance for Certificate re-key 15
4.7.2 Who may request certification of a new public key 15
4.7.3 Processing Certificate re-keying requests 15
4.7.4 Notification of new Certificate issuance to subscriber 15
4.7.5 Conduct constituting acceptance of a re-keyed Certificate 15
4.7.6 Publication of the re-keyed Certificate by the CA 15
4.7.7 Notification of Certificate issuance by the CA to other entities 15
4.8 Certificate modification 15
4.8.1 Circumstance for Certificate modification 15
4.8.2 Who may request Certificate modification 15
4.8.3 Processing Certificate modification requests 15
4.8.4 Notification of new Certificate issuance to subscriber 16
4.8.5 Conduct constituting acceptance of modified Certificate 16
4.8.6 Publication of the modified Certificate by the CA 16
4.8.7 Notification of Certificate issuance by the CA to other entities 16
4.9 Certificate revocation and suspension 16
4.9.1 Circumstances for revocation 16
4.9.2 Who can request revocation 16
4.9.3 Procedure for revocation request 16
4.9.4 Revocation request grace period 16
4.9.5 Time within which CA must process the revocation request 16
4.9.6 Revocation checking requirement for Relying Parties 16
4.9.7 CRL issuance frequency (if applicable) 17
4.9.8 Maximum latency for CRLs (if applicable) 17
4.9.9 On-line revocation/status checking availability 17
4.9.10 On-line revocation checking requirements 17
4.9.11 Other forms of revocation advertisements available 17
4.9.12 Special requirements re key compromise 17
4.9.13 Circumstances for suspension 17
4.9.14 Who can request suspension 17
4.9.15 Procedure for suspension request 17
4.9.16 Limits on suspension period 17
4.9.17 Circumstances for Termination of Suspension' 17
4.9.18 Who can Request Termination of Suspension 17
4.9.19 Procedure for Termination of Suspension 18
4.10 Certificate status services 18
4.10.1 Operational characteristics 18
4.10.2 Service availability 18
4.10.3 Optional features 18
4.11 End of subscription 18
4.12 Key escrow and key recovery 18
4.12.1 Key escrow and recovery policy and practices 18
4.12.2 Session key encapsulation and recovery policy and practices 18

5 FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS 19
5.1 Physical controls 19
5.1.1 Site location and construction 19
5.1.2 Physical access 19

5.1.3 Power and air conditioning 19
5.1.4 Water exposures 19
5.1.5 Fire prevention and protection 19
5.1.6 Media storage 19
5.1.7 Waste disposal 19
5.1.8 Off-site backup 19
5.2 Procedural controls 19
5.2.1 Trusted roles 19
5.2.2 Number of persons required per task 19
5.2.3 Identification and authentication for each role 19
5.2.4 Roles requiring separation of duties 19
5.3 Personnel security controls 19
5.3.1 Qualifications, experience, and clearance requirements 19
5.3.2 Background check procedures 20
5.3.3 Training requirements 20
5.3.4 Retraining frequency and requirements 20
5.3.5 Job rotation frequency and sequence 20
5.3.6 Sanctions for unauthorized actions 20
5.3.7 Independent contractor requirements 20
5.3.8 Documentation supplied to personnel 20
5.4 Audit logging procedures 20
5.4.1 Types of events recorded 20
5.4.2 Frequency of processing log 20
5.4.3 Retention period for audit log 20
5.4.4 Protection of audit log 20
5.4.5 Audit log backup procedures 20
5.4.6 Audit collection system (internal vs. external) 20
5.4.7 Notification to event-causing Subject 20
5.4.8 Vulnerability assessments 20
5.5 Records archival 21
5.5.1 Types of records archived 21
5.5.2 Retention period for archive 21
5.5.3 Protection of archives 21
5.5.4 Archive backup procedures 21
5.5.5 Requirements for time-stamping of records 21
5.5.6 Archive collection system 21
5.5.7 Procedures to obtain and verify archive information 21
5.6 Key changeover 21
5.7 Compromise and disaster recovery 21
5.7.1 Incident and compromise handling procedures 21
5.7.2 Computing resources, software and/or data are corrupted 21
5.7.3 Entity private key compromise procedures 21
5.7.4 Business continuity capabilities after a disaster 21
5.8 CA or RA Termination 21

6 TECHNICAL SECURITY CONTROLS 22
6.1 Key pair generation and installation 22
6.1.1 Key pair generation 22
6.1.2 Private key delivery to Subscriber or Subject 22
6.1.3 Public key delivery to Certificate issuer 22
6.1.4 CA public key delivery to Relying Parties 22
6.1.5 Key sizes 22
6.1.6 Public key parameters generation and quality checking 22
6.1.7 Key usage purposes (as per X.509 v3 key usage field) 22
6.2 Private Key Protection and Cryptographic Module Engineering Controls 22
6.2.1 Cryptographic module standards and controls 22
6.2.2 Private key (n out of m) multi-person control 22
6.2.3 Private key escrow 22
6.2.4 Private key backup 22
6.2.5 Private key archival 22
6.2.6 Private key transfer into or from a cryptographic module 22
6.2.7 Private key storage on cryptographic module 22
6.2.8 Method of activating private keys 23

6.2.9 Method of deactivating private key ... 23
6.2.10 Method of destroying private key ... 23
6.2.11 Cryptographic Module Rating ... 23
6.3 Other aspects of key pair management ... 23
6.3.1 Public key archival ... 23
6.3.2 Certificate operational periods and key pair usage periods ... 23
6.4 Activation data ... 23
6.4.1 Activation data generation and installation ... 23
6.4.2 Activation data protection ... 23
6.4.3 Other aspects of activation data ... 23
6.5 Computer security controls ... 23
6.5.1 Specific computer security technical requirements ... 23
6.5.2 Computer security rating ... 23
6.6 Life cycle technical controls ... 23
6.6.1 System development controls ... 23
6.6.2 Security management controls ... 23
6.6.3 Life cycle security controls ... 24
6.7 Network security controls ... 24
6.8 Time-Stamping ... 24

7 CERTIFICATE, CRL AND OCSP PROFILES ... 25
7.1 Certificate profile ... 25
7.2 CRL profile ... 25
7.3 OCSP profile ... 25

8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS ... 26
8.1 Frequency or Circumstances of Assessment ... 26
8.2 Identity/qualifications of assessor ... 26
8.3 Assessor's relationship to assessed entity ... 26
8.4 Topics covered by assessment ... 26
8.5 Actions taken as a result of deficiency ... 26
8.6 Communication of results ... 26

9 OTHER BUSINESS AND LEGAL MATTERS ... 27
9.1 Fees ... 27
9.1.1 Certificate Issuance or Renewal Fees ... 27
9.1.2 Certificate Access Fees ... 27
9.1.3 Revocation or Status Information Access Fees ... 27
9.1.4 Fees for other services ... 27
9.1.5 Refund Policy ... 27
9.2 Financial responsibility ... 27
9.2.1 Insurance coverage ... 27
9.2.2 Other assets ... 27
9.2.3 Insurance or warranty coverage for end-entities ... 27
9.3 Confidentiality of business information ... 27
9.3.1 Scope of confidential information ... 27
9.3.2 Information not within the scope of confidential information ... 27
9.3.3 Responsibility to protect confidential information ... 27
9.4 Privacy of personal information ... 28
9.4.1 Privacy plan ... 28
9.4.2 Information treated as private ... 28
9.4.3 Information not deemed private ... 28
9.4.4 Responsibility to protect private information ... 28
9.4.5 Notice and consent to use private information ... 28
9.4.6 Disclosure pursuant to judicial or administrative process ... 28
9.4.7 Other information disclosure circumstances ... 28
9.5 Intellectual property rights ... 28
9.6 Representations and warranties ... 28
9.6.1 CA representations and warranties ... 28
9.6.2 RA representations and warranties ... 28
9.6.3 Subscriber representations and warranties ... 28
9.6.4 Relying party representations and warranties ... 28
9.6.5 Representations and warranties of other participants ... 28

9.7 Disclaimers of warranties 28
9.8 Limitations of liability 29
9.9 Indemnities 29
9.10 Term and termination of the present TSPS 29
9.10.1 Term 29
9.10.2 Termination 29
9.10.3 Effect of termination and survival 29
9.11 Individual notices and communications with participants 29
9.12 Amendments to the present TSPS 29
9.12.1 Procedure for amendment 29
9.12.2 Notification mechanism and period 29
9.12.3 Circumstances under which OID must be changed 29
9.13 Dispute resolution provisions 29
9.14 Governing law 29
9.15 Compliance with applicable law 29
9.16 Miscellaneous provisions 29
9.16.1 Entire agreement 29
9.16.2 Assignment 30
9.16.3 Severability 30
9.16.4 Enforcement (attorneys' fees and waiver of rights) 30
9.16.5 Force Majeure 30
9.17 Other provisions 30

APPENDIX A - REFERENCES 31

Document History

Version	Changes
2.0	The update brings the CPS in line with the updated Root CP v2.0 document. Reference to timing for revocation was added in 4.9.5; Stipulation was added in 9.1.3; Linguistic corrections were done.
1.3	No content change compared to 1.2. This version is the first version for production purposes and with an effective date for the public issuance of Certificates. Approved by the PMA and labelled “PUBLIC” for publication.
1.2	For internal use only, no public effect, for pre-production context only. Version after initial audit. No content change compared to 1.1.
1.1	For internal use only, no public effect, for pre-production context only. Minor corrections after review (capitalisation, typos).
1.0	For internal use only, no public effect, for pre-production context only. First approved version

1 INTRODUCTION

1.1 Overview

Zetes Estonia OÜ

Zetes Estonia OÜ (hereafter ZE) is a private limited company established in Tallinn, Estonia under registry code 17066049 and listed as a Qualified Trust Service Provider (hereafter QTSP) on the Trusted List of Estonia. The principal activities of ZE are offering eIDAS trust services for the public and private sector.

Scope

This document is the Certification Practice Statement (CPS) for a Root CA (RCA) that is exclusively reserved as the trust anchor for a CA hierarchy for the ID-1 format identity documents for the Republic of Estonia (hereafter Documents). For an overview of the CA hierarchy and related services see chapter 1 in [ZE TSPS-ID1].

This document is a public document that describes the practices applied by ZE for the RCA which issues top-level Certificates to Intermediate CA that in turn issue Subscriber Certificates for holders of Document.

This Root CPS outlines the issuance of Certificates for the Intermediate CAs within the ZE CA-hierarchy. For the issuance of Certificates for holders of Documents by an Intermediate CA, see [ZE CPS-ID1-EID-CA] for the relevant Intermediate CA.

This Root CPS adheres to a Certificate Policy defined by the Police and Border Guard Board (hereafter PBGB) and which is referenced as [PBGB CP-ID1-ROOT-CA]. Where relevant the Root CPS also refers to other public documents, the most important of which are Trust Services Practice Statement [ZE TSPS-ID1] and the Certificate Profile documentation [ZE PROFILES].

This document follows the structure and content as defined in [IETF RFC 3647]. Pursuant to [IETF RFC 3647] this CPS is divided into nine chapters. To preserve the outline specified by [IETF RFC 3647], section headings that do not apply have the statement "Not applicable".

1.2 Document name and identification

See the table on the cover page of this document.

1.3 PKI Participants

The PKI participants are all the legal persons or natural persons who are involved in any of the processes and activities and/or who are impacted by the use of Certificates issued under the RCA. All participants adhere to or are bound by [PBGB CP-ID1-ROOT-CA] and [ZE CPS-ID1-ROOT-CA].

For the issuance of the RCA Certificate and for CA Certificates in the RCA-hierarchy for electronic Document schemes of the Republic of Estonia, ZE is the CA, the RA and the Subscriber. The RCA adheres to the procedures and practices for managing the lifecycle of the keys and Certificates as well as other related services described in the Root CP, exclusively for the Republic of Estonia. For the execution of its duties as CA and RA, ZE uses authorized staff employed by Zetes Estonia OÜ (Estonia) and Zetes NV (Belgium).

1.3.1 Certification Authority (CA)

ZE is the Certification Authority.

1.3.2 Registration Authorities (RA)

ZE is the Registration and Revocation Authority (RA).

1.3.3 Subjects and Subscribers

ZE is the Subscriber. The Subject is the PKI entity (a CA or an OCSP responder) that is operated by ZE.

1.3.4 Relying Parties

Relying Parties are all natural persons and legal persons who need to validate a Certificate issued by an Intermediate CA in the RCA hierarchy.

1.3.5 Other Participants

See the corresponding clause in [PBGB CP-ID1-ROOT-CA].

1.4 Certificate Usage

1.4.1 Appropriate Certificate uses

See the corresponding clause in [PBGB CP-ID1-ROOT-CA].

1.4.2 Prohibited Certificate uses

See the corresponding clause in [PBGB CP-ID1-ROOT-CA].

1.5 Policy administration

1.5.1 Organisation administering the document

See the corresponding clause in [ZE TSPS-ID1].

1.5.2 Contact person

See the corresponding clause in [ZE TSPS-ID1].

1.5.3 Person determining suitability for the policy

See the corresponding clause in [ZE TSPS-ID1].

1.5.4 Approval procedures

See the corresponding clause in [ZE TSPS-ID1].

1.6 Definitions and acronyms

1.6.1 Definitions

Subject	ZE is the QTSP and is therefore the owner and operator of the QTSP's PKI infrastructure. ZE is the legal person to whom CA Certificates and OCSP Certificates are issued and who has the usage rights for the Certificate. The Certificate name fields identify ZE as the Subject, as defined in [ZE PROFILES].
Subscriber	ZE is the QTSP and is therefore the owner and operator of the QTSP's PKI infrastructure. ZE is the legal person that subscribes to the Trust Service. For CA Certificates and OCSP Certificates, Subscriber and a Subject are the same legal person.

For the definition of Subject, Subscriber and Subscriber Certificates in the context of Document Certificates, see the corresponding clause in [ZE CPS-ID1-EID-CA]. For all other definitions, see the corresponding clause in [ZE TSPS-ID1].

1.6.2 Acronyms

See the corresponding clause in [ZE TSPS-ID1].

1.6.3 References

References to other documents or other sources are labelled between square brackets, e.g. **[EST ID ACT].**

For a list of references see Appendix A in [ZE TSPS-ID1].

2 PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 Repositories

See the corresponding clause in [ZE TSPS-ID1].

2.2 Publication of certification information

See the corresponding clause in [ZE TSPS-ID1].

2.3 Time or frequency of publication

See the corresponding clause in [ZE TSPS-ID1].

2.4 Access controls on repositories

See the corresponding clause in [ZE TSPS-ID1].

3 IDENTIFICATION AND AUTHENTICATION

3.1 Naming

3.1.1 Types of names

Types of names assigned to the Subscriber are described in [ZE PROFILES] and in [PBGB CP-ID1-ROOT-CA].

3.1.2 Need for names to be meaningful

The Certificate Distinguished Name (DN) field will clearly and unambiguously identify the purpose and ownership of the CA. The DN in a RCA Certificate and in an Intermediate CA make clear the type of CA the Certificate is for.

3.1.3 Anonymity or pseudonymity of subscribers

Not applicable.

3.1.4 Rules for interpreting various name forms

Rules for interpreting various name forms are described in [ZE PROFILES].

3.1.5 Uniqueness of names

The Certificate Subject field is unique for each RCA Certificate and each Intermediate CA Certificate.

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

In accordance with internal procedures, possession of private keys of the RCA and Intermediate CAs is guaranteed by virtue of the key generation procedure and the equipment used. Keys are generated on a certified HSM and are recorded in the Key Ceremony report. Designated authorized ZE operators generate the key pair, export and include the public key into a Certificate request format, transfer the Certificate request to the RCA and ensure that the correct Certificate request is used to generate the Certificate. The Certificate request is signed with the private key for which the Certificate is requested. The RCA software will verify that the public key in the Certificate request matches with the private key with which the Certificate was signed. The procedure of the Key Ceremony is attended by one or more representatives of PBGB and by an independent external auditor.

3.2.2 Authentication of organization identity

Only authorised representatives of PBGB can order the creation of an Intermediate CA Certificate. The list of representatives is previously validated and approved by PBGB and the PMA of ZE. The organization identity represented in a RCA Certificate and in an Intermediate CA Certificates is that of ZE itself. The representation of the ZE organization identity in the Certificates is prescribed in the Certificate Profile [ZE PROFILES].

3.2.3 Authentication of individual identity

The PMA appoints a Key Ceremony commission of at least 4 authorized people to carry out the key generation and Certificate issuance. The PMA appoints the head of the Key Ceremony commission. The PMA appoints an independent external auditor who together with the head of the commission verifies the identity and the authorization of each person participating in the Key Ceremony. The PMA may also appoint internal and external witnesses. Witnesses can be but are not limited to trainees, internal or external subject matter experts, internal auditors, security officers, etc.

3.2.4 Non-verified subscriber information

Not applicable.

3.2.5 Validation of authority

The PMA nominates the personnel carrying out the procedures of key generation, Certificate issuance and CRL issuance. The Director General of PBGB nominates the representative of PBGB participating in the key generation procedure and Certificate issuance.

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

Not applicable.

3.3.2 Identification and authentication for re-key after revocation

Not applicable.

3.4 Identification and authentication for revocation requests

The PMA is the only entity that can initiate and authorize a revocation request, either in response to a request from PBGB, in response to a request from the Supervisory Body of the Republic of Estonia or on its own initiative. The PMA appoints a revocation ceremony commission of at least 4 authorized people to carry out the revocation procedure. The PMA appoints the head of the commission. The head of the commission verifies the identity and the authorization of each person participating in the revocation ceremony. The PMA may also appoint internal and external witnesses. Witnesses can be but are not limited to trainees, internal or external subject matter experts, internal auditors, security officers, etc.

4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 Certificate application

4.1.1 Who can submit a Certificate application

PBGB has the exclusive authority to instruct ZE to create a new RCA or a new Intermediate CA.

ZE is the CA, the RA and the Subscriber (the Certificate applicant and the Certificate holder). Although the Certificate application process and Certificate issuance processes are entirely internal to ZE, ZE is only allowed to issue these CA Certificates to itself on explicit instruction of PBGB.

A Certificate application in this context is always the result of an approved, internal, scheduled Key Ceremony.

Prior to the Key Ceremony, ZE will present to PBGB and the external auditor:

- Internal documentation and evidences
- The formal approval from PBGB to perform the Key Ceremony
- A list with the name, function and organization of the authorized participants
- The statement from each participant's organization that the participant is authorized to participate and represent the organization and will be available at the foreseen date(s) for the Key Ceremony

At the predefined date, all participants will gather and participate in the Key Ceremony that will be led by the head assigned by the PMA.

4.1.2 Enrolment process and responsibilities

The PMA of ZE approves the procedures for key generation and Certificate issuance and nominates a list of at least 4 persons to carry out the procedure, contents, time and place of the Key Ceremony.

An independent external auditor is nominated by the PMA of ZE.

The Director General of the PBGB shall authorise the representative of the PBGB to participate in and to supervise the Key Ceremony. The PMA of ZE will confirm the appointed representative of PBGB.

The enrolment process is implicit and is an internal process of ZE. The authorized staff of ZE generates the key, selects the pre-approved Certificate profile and provides the pre-approved Subject field DN.

These steps are an integral part of the CA Key Ceremony process.

4.2 Certificate application processing

4.2.1 Performing identification and authentication functions

Certificate application is an integral and implicit part of the Key Ceremony process.

See clause 3.2.3.

4.2.2 Approval or rejection of Certificate applications

Certificate applications that are not part of an approved Key Ceremony will not be processed. Certificate applications that do not adhere to the approved Key Ceremony instructions will be rejected.

Before a Certificate is imported into the RCA, the data in the request is checked for completeness, integrity and correctness. The content of all the Certificate fields and the public key are checked by multiple participants in the Key Ceremony for compliance with the authorized Certificate profile and Certificate content.

4.2.3 Time to process Certificate applications

The Certificate application process starts with the formal demand from PBGB to ZE to create a new CA and issue the CA Certificate and ends with the actual creation and acceptance of the new CA Certificate, regardless whether it is for a

RCA or an Intermediate CA. The entire process may span a period of several weeks and includes one or more formal meetings of the PMA, preparations and testing and one or more scheduled sessions that together constitute the Key Ceremony. The Key Ceremony may be spread over multiple non-consecutive days.

4.3 Certificate Issuance

4.3.1 CA actions during Certificate issuance

Certificate issuance is an integral and implicit part of the Key Ceremony process.

Certificate issuance is a manual process that involves activating the RCA, importing the Certificate request into the CA and generating the Certificate. The Certificate is exported from the CA and checked for compliance with the authorized Certificate profile and Certificate content.

A backup of the RCA Certificate database and audit logs is made. This data is transferred and synchronized to the backup CA infrastructure at a later date.

4.3.2 Notification to subscriber by the CA of issuance of Certificate

ZE is the RA, the CA and the Subscriber. Notification of the creation of the issued CA Certificate is therefore implicit to the Key Ceremony process.

4.4 Certificate acceptance

4.4.1 Conduct constituting Certificate acceptance

The Key Ceremony report shows the activities performed and the Certificate issued. The report is signed by the participants and witnesses of the Key Ceremony.

During the Key Ceremony, the authorized participants from ZE and PBGB will validate and jointly confirm that the generated Certificate is compliant to the authorized CA Certificate profile and that the procedures described in the Key Ceremony have been followed.

Finally, the CA Certificate and Key Ceremony report will be presented to the PMA for formal approval and acceptance of the Certificate. Only after acceptance by the PMA will the CA Certificate be considered as accepted and can it be used in production and published in the public repository.

4.4.2 Publication of the Certificate by the CA

Accepted RCA Certificates and Intermediate CA Certificate are made available in the CA's Repository.

The CA Certificates are also stored on the QSCD chip in the Documents and can be extracted from the QSCD chip for installation in a computing device's local certificate store.

4.4.3 Notification of Certificate issuance by the CA to other entities

See clause 4.4.2.

4.5 Key pair and Certificate usage

4.5.1 Subscriber private key and Certificate usage

As the Subscriber of the CA Certificates, ZE is bound by the usage conditions and obligations mentioned in the Root CPS, including the referenced Root CP from PBGB but also by the contract with PBGB for the provision of CA services for Documents as well as by the applicable laws of the Republic of Estonia.

ZE may only use the RCA key and Certificate for the purpose authorized by PBGB:

- for the issuance of Intermediate CA Certificates related to the Documents
- for the issuance of CRLs

ZE may only use the Intermediate CA key and Certificate for the purpose authorized by PBGB:

- for the issuance of Subscriber Certificates for the Documents
- for the issuance of associated OCSP Certificates
- for the issuance of CRLs

ZE ensure that the necessary security measures and procedures are applied to prevent the compromise, loss, disclosure, modification, or otherwise unauthorized use of the CA private keys.

4.5.2 Relying party public key and Certificate usage

Relying Parties are entirely responsible to decide whether a Certificate and its status information are fit for purpose.

Relying Parties may not rely on a CA Certificate unless they have performed the following actions:

- Evaluate whether the Certificate is appropriate for the intended usage and the Relying Party's use case.
- Restrictively accept the Certificate only for the intended usage and for the appropriate applications, in compliance with the key usage information encoded in the Certificate and in compliance with the limitation of use stated in the Certificate directly or through the referred CPS and CP.
- Successfully perform public key operations as a condition of relying on a Certificate.
- Validate the status of the CA Certificate chain using the European Union List of Trusted Lists (LOTL), a public online service provided by the European Commission.
- Validate the Certificate status and that of each Certificate in the Certificate's trust hierarchy by using at least one of the mechanisms for Certificate status information indicated in the Certificate or in the CPS for that Certificate.
- If the Certificate status has changed or the Certificate has expired, the Relying Party must immediately stop trusting the Certificate, and must undertake the necessary checks and corrections with respect to prior use of the Certificate in relation to the date and time and the nature of the Certificate's change of status.
- Take all precautions with regards to the use of the Certificate as set out in this CPS and in [PBGB CP-ID1-ROOT-CA].
- Only rely on a Certificate as may be reasonable under the circumstances.

Relying Parties must always validate the CA Certificates using a valid and non-expired CRL. Relying Parties are required to take into account the refresh date indicated in each CRL and retrieve an up to date CRL before the indicated refresh date. Relying Parties are allowed and encouraged to keep a local copy (cache) of the CRL. Relying Parties must update a cached CRL in accordance with the CRL refresh date and when ZE or PBGB have publicly announced that a non-periodic CRL was issued due to the revocation of one or more CA Certificates.

A Relying Party must follow the limitations stated within the Intermediate CA Certificate and make sure that the purpose for which it relies on the CA Certificates complies with intended use as stated in this CPS and in [PBGB CP-ID1-ROOT-CA].

4.6 Certificate renewal

4.6.1 Circumstance for Certificate renewal

Not applicable.

4.6.2 Who may request renewal

Not applicable.

4.6.3 Processing Certificate renewal requests

Not applicable.

4.6.4 Notification of new Certificate issuance to subscriber

Not applicable.

4.6.5 Conduct constituting acceptance of a renewal Certificate

Not applicable.

4.6.6 Publication of the renewal Certificate by the CA

Not applicable.

4.6.7 Notification of Certificate issuance by the CA to other entities

Not applicable.

4.7 Certificate re-key

4.7.1 Circumstance for Certificate re-key

Not applicable.

4.7.2 Who may request certification of a new public key

Not applicable.

4.7.3 Processing Certificate re-keying requests

Not applicable.

4.7.4 Notification of new Certificate issuance to subscriber

Not applicable.

4.7.5 Conduct constituting acceptance of a re-keyed Certificate

Not applicable.

4.7.6 Publication of the re-keyed Certificate by the CA

Not applicable.

4.7.7 Notification of Certificate issuance by the CA to other entities

Not applicable.

4.8 Certificate modification

4.8.1 Circumstance for Certificate modification

Not applicable.

4.8.2 Who may request Certificate modification

Not applicable.

4.8.3 Processing Certificate modification requests

Not applicable.

4.8.4 Notification of new Certificate issuance to subscriber

Not applicable.

4.8.5 Conduct constituting acceptance of modified Certificate

Not applicable.

4.8.6 Publication of the modified Certificate by the CA

Not applicable.

4.8.7 Notification of Certificate issuance by the CA to other entities

Not applicable.

4.9 Certificate revocation and suspension

4.9.1 Circumstances for revocation

See the corresponding clause in [PBGB CP-ID1-ROOT-CA].

4.9.2 Who can request revocation

ZE is the Revocation Authority and is the Subscriber. The PMA is the only entity that can initiate and authorize a revocation request, either in response to a request from PBGB, in response to a request from the Supervisory Body of the Republic of Estonia or on its own initiative.

4.9.3 Procedure for revocation request

See the corresponding clause in [PBGB CP-ID1-ROOT-CA].

ZE is the CA, the RA and the Subscriber. The Certificate revocation process is entirely internal to ZE. ZE involves PBGB in the decision to revoke a CA Certificate and aligns with PBGB for the scheduled date and for the notification towards Relying Parties.

A Certificate revocation in this context is always the result of an approved, internal, scheduled Key Ceremony.

Prior to the revocation ceremony, ZE will present to PBGB and the external auditor:

- Internal documentation and evidences
- The formal approval from PBGB to perform the revocation ceremony
- A list with the name, function and organization of the authorized participants
- The statement from each participant's organization that the participant is authorized to participate and represent the organization and will be available at the foreseen date(s) for the revocation ceremony

At the predefined date, all participants will gather and participate in the Key Ceremony that will be led by the head assigned by the PMA.

4.9.4 Revocation request grace period

No stipulations.

4.9.5 Time within which CA must process the revocation request

See the corresponding clause in [PBGB CP-ID1-ROOT-CA].

4.9.6 Revocation checking requirement for Relying Parties

See clause 4.5.2.

4.9.7 CRL issuance frequency (if applicable)

For periodic CRL issuance, the RCA creates a fresh CRL at least once per year and will be published before the expiration date of the preceding CRL. It is possible that a fresh CRL is created and published ad hoc, unrelated to the preceding CRL's expiration date. Such ad-hoc CRL shall have the same or a later expiration date as the preceding CRL.

When a published CA Certificate is revoked, a fresh CRL is created immediately. The appropriate date and time of publication of the new CRL will be coordinated with PBGB.

4.9.8 Maximum latency for CRLs (if applicable)

A CRL is published at latest the next business day before 24:00. If the CRL was created due to the revocation of a CA Certificate, then the appropriate date and time of publication of the new CRL will be coordinated with PBGB.

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

In exceptional circumstances ZE or PBGB may opt to communicate about the revocation of a CA Certificate via their respective web site, via e-mails or other appropriate channels. This does not replace, reduce or negate in any way the use of the CRL.

4.9.12 Special requirements re key compromise

In case of a key compromise ZE has the obligation to inform PBGB and the Estonian Supervisory Body. A key compromise is covered by the business continuity plan. ZE will work closely with both agencies to organize the revocation of the impacted CA Certificate and to communicate to all stakeholders.

All actions in response to a key compromise will take into account the best interests of the Subscribers and will comply with the requirements laid out in [EU 910/2014 EIDAS] and in [PBGB CP-ID1-ROOT-CA].

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

For maximum interoperability with 3rd party software

- the CRL format adheres to the RFC 5280 standard.
- the Certificate to be checked contains the URI for the CRL
- the CRL is signed by the RCA itself
- the TSP does not use another trusted authority to sign the CRL
- the CRL files can be downloaded using HTTP(S)

The TSP will generate a last and final CRL when all the Certificates within the scope of the CRL have either expired or have been revoked.

A Relying Party is sole responsible for taking into account the periodicity of the CRL and for deciding whether this is fit for purpose.

Relying Parties may consider caching CRLs in their own environment for faster processing and for reducing their network traffic.

4.10.2 Service availability

See the corresponding clause in [PBGB CP-ID1-ROOT-CA].

4.10.3 Optional features

Not applicable.

4.11 End of subscription

Subscriber subscription ends when a Certificate is revoked, expired or the service is terminated.

4.12 Key escrow and key 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

5.1 Physical controls

5.1.1 Site location and construction

See the corresponding clause in [ZE TSPS-ID1].

5.1.2 Physical access

See the corresponding clause in [ZE TSPS-ID1].

5.1.3 Power and air conditioning

See the corresponding clause in [ZE TSPS-ID1].

5.1.4 Water exposures

See the corresponding clause in [ZE TSPS-ID1].

5.1.5 Fire prevention and protection

See the corresponding clause in [ZE TSPS-ID1].

5.1.6 Media storage

See the corresponding clause in [ZE TSPS-ID1].

5.1.7 Waste disposal

See the corresponding clause in [ZE TSPS-ID1].

5.1.8 Off-site backup

See the corresponding clause in [ZE TSPS-ID1].

5.2 Procedural controls

5.2.1 Trusted roles

See the corresponding clause in [ZE TSPS-ID1].

5.2.2 Number of persons required per task

See the corresponding clause in [ZE TSPS-ID1].

5.2.3 Identification and authentication for each role

See the corresponding clause in [ZE TSPS-ID1].

5.2.4 Roles requiring separation of duties

See the corresponding clause in [ZE TSPS-ID1].

5.3 Personnel security controls

5.3.1 Qualifications, experience, and clearance requirements

See the corresponding clause in [ZE TSPS-ID1].

5.3.2 Background check procedures

See the corresponding clause in [ZE TSPS-ID1].

5.3.3 Training requirements

See the corresponding clause in [ZE TSPS-ID1].

5.3.4 Retraining frequency and requirements

See the corresponding clause in [ZE TSPS-ID1].

5.3.5 Job rotation frequency and sequence

See the corresponding clause in [ZE TSPS-ID1].

5.3.6 Sanctions for unauthorized actions

See the corresponding clause in [ZE TSPS-ID1].

5.3.7 Independent contractor requirements

See the corresponding clause in [ZE TSPS-ID1].

5.3.8 Documentation supplied to personnel

See the corresponding clause in [ZE TSPS-ID1].

5.4 Audit logging procedures

5.4.1 Types of events recorded

See the corresponding clause in [ZE TSPS-ID1].

5.4.2 Frequency of processing log

See the corresponding clause in [ZE TSPS-ID1].

5.4.3 Retention period for audit log

See the corresponding clause in [ZE TSPS-ID1].

5.4.4 Protection of audit log

See the corresponding clause in [ZE TSPS-ID1].

5.4.5 Audit log backup procedures

See the corresponding clause in [ZE TSPS-ID1].

5.4.6 Audit collection system (internal vs. external)

See the corresponding clause in [ZE TSPS-ID1].

5.4.7 Notification to event-causing Subject

See the corresponding clause in [ZE TSPS-ID1].

5.4.8 Vulnerability assessments

See the corresponding clause in [ZE TSPS-ID1].

5.5 Records archival

5.5.1 Types of records archived

See the corresponding clause in [ZE TSPS-ID1].

5.5.2 Retention period for archive

See the corresponding clause in [ZE TSPS-ID1].

5.5.3 Protection of archives

See the corresponding clause in [ZE TSPS-ID1].

5.5.4 Archive backup procedures

See the corresponding clause in [ZE TSPS-ID1].

5.5.5 Requirements for time-stamping of records

See the corresponding clause in [ZE TSPS-ID1].

5.5.6 Archive collection system

See the corresponding clause in [ZE TSPS-ID1].

5.5.7 Procedures to obtain and verify archive information

See the corresponding clause in [ZE TSPS-ID1].

5.6 Key changeover

See the corresponding clause in [ZE TSPS-ID1].

5.7 Compromise and disaster recovery

5.7.1 Incident and compromise handling procedures

See the corresponding clause in [ZE TSPS-ID1].

5.7.2 Computing resources, software and/or data are corrupted

See the corresponding clause in [ZE TSPS-ID1].

5.7.3 Entity private key compromise procedures

See the corresponding clause in [ZE TSPS-ID1].

5.7.4 Business continuity capabilities after a disaster

See the corresponding clause in [ZE TSPS-ID1].

5.8 CA or RA Termination

See the corresponding clause in [ZE TSPS-ID1].

6 TECHNICAL SECURITY CONTROLS

6.1 Key pair generation and installation

6.1.1 Key pair generation

See the corresponding clause in [ZE TSPS-ID1].

6.1.2 Private key delivery to Subscriber or Subject

See the corresponding clause in [ZE TSPS-ID1].

6.1.3 Public key delivery to Certificate issuer

See the corresponding clause in [ZE TSPS-ID1].

6.1.4 CA public key delivery to Relying Parties

See the corresponding clause in [ZE TSPS-ID1].

6.1.5 Key sizes

See the corresponding clause in [ZE TSPS-ID1].

6.1.6 Public key parameters generation and quality checking

See the corresponding clause in [ZE TSPS-ID1].

6.1.7 Key usage purposes (as per X.509 v3 key usage field)

See the corresponding clause in [ZE TSPS-ID1].

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic module standards and controls

See the corresponding clause in [ZE TSPS-ID1].

6.2.2 Private key (n out of m) multi-person control

See the corresponding clause in [ZE TSPS-ID1].

6.2.3 Private key escrow

See the corresponding clause in [ZE TSPS-ID1].

6.2.4 Private key backup

See the corresponding clause in [ZE TSPS-ID1].

6.2.5 Private key archival

See the corresponding clause in [ZE TSPS-ID1].

6.2.6 Private key transfer into or from a cryptographic module

See the corresponding clause in [ZE TSPS-ID1].

6.2.7 Private key storage on cryptographic module

See the corresponding clause in [ZE TSPS-ID1].

6.2.8 Method of activating private keys

See the corresponding clause in [ZE TSPS-ID1].

6.2.9 Method of deactivating private key

See the corresponding clause in [ZE TSPS-ID1].

6.2.10 Method of destroying private key

See the corresponding clause in [ZE TSPS-ID1].

6.2.11 Cryptographic Module Rating

See the corresponding clause in [ZE TSPS-ID1].

6.3 Other aspects of key pair management

6.3.1 Public key archival

See the corresponding clause in [ZE TSPS-ID1].

6.3.2 Certificate operational periods and key pair usage periods

See the corresponding clause in [ZE TSPS-ID1].

6.4 Activation data

6.4.1 Activation data generation and installation

See the corresponding clause in [ZE TSPS-ID1].

6.4.2 Activation data protection

See the corresponding clause in [ZE TSPS-ID1].

6.4.3 Other aspects of activation data

See the corresponding clause in [ZE TSPS-ID1].

6.5 Computer security controls

6.5.1 Specific computer security technical requirements

See the corresponding clause in [ZE TSPS-ID1].

6.5.2 Computer security rating

See the corresponding clause in [ZE TSPS-ID1].

6.6 Life cycle technical controls

See the corresponding clause in [ZE TSPS-ID1].

6.6.1 System development controls

See the corresponding clause in [ZE TSPS-ID1].

6.6.2 Security management controls

See the corresponding clause in [ZE TSPS-ID1].

6.6.3 Life cycle security controls

See the corresponding clause in [ZE TSPS-ID1].

6.7 Network security controls

See the corresponding clause in [ZE TSPS-ID1].

6.8 Time-Stamping

See the corresponding clause in [ZE TSPS-ID1].

7 CERTIFICATE, CRL AND OCSP PROFILES

7.1 Certificate profile

See the corresponding section in the profiles specifications [ZE PROFILES].

7.2 CRL profile

See the corresponding section in the profiles specifications [ZE PROFILES].

7.3 OCSP profile

Not applicable.

8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS

8.1 Frequency or Circumstances of Assessment

See the corresponding clause in [ZE TSPS-ID1].

8.2 Identity/qualifications of assessor

See the corresponding clause in [ZE TSPS-ID1].

8.3 Assessor's relationship to assessed entity

See the corresponding clause in [ZE TSPS-ID1].

8.4 Topics covered by assessment

See the corresponding clause in [ZE TSPS-ID1].

8.5 Actions taken as a result of deficiency

See the corresponding clause in [ZE TSPS-ID1].

8.6 Communication of results

See the corresponding clause in [ZE TSPS-ID1].

9 OTHER BUSINESS AND LEGAL MATTERS

9.1 Fees

9.1.1 Certificate Issuance or Renewal Fees

See the corresponding clause in [ZE CPS-ID1-EID-CA].

9.1.2 Certificate Access Fees

See the corresponding clause in [ZE CPS-ID1-EID-CA].

9.1.3 Revocation or Status Information Access Fees

See also the corresponding clause in [ZE CPS-ID1-EID-CA].

Revocation of the root CA certificate and intermediate CA certificates is free of charge.

Access to the certificate status information is free of charge.

9.1.4 Fees for other services

See the corresponding clause in [ZE CPS-ID1-EID-CA].

9.1.5 Refund Policy

See the corresponding clause in [ZE CPS-ID1-EID-CA].

9.2 Financial responsibility

9.2.1 Insurance coverage

See the corresponding clause in [ZE CPS-ID1-EID-CA].

9.2.2 Other assets

See the corresponding clause in [ZE CPS-ID1-EID-CA].

9.2.3 Insurance or warranty coverage for end-entities

See the corresponding clause in [ZE CPS-ID1-EID-CA].

9.3 Confidentiality of business information

9.3.1 Scope of confidential information

See the corresponding clause in [ZE CPS-ID1-EID-CA].

9.3.2 Information not within the scope of confidential information

See the corresponding clause in [ZE CPS-ID1-EID-CA].

9.3.3 Responsibility to protect confidential information

See the corresponding clause in [ZE CPS-ID1-EID-CA].

9.4 Privacy of personal information

9.4.1 Privacy plan

See the corresponding clause in [ZE CPS-ID1-EID-CA].

9.4.2 Information treated as private

See the corresponding clause in [ZE CPS-ID1-EID-CA].

9.4.3 Information not deemed private

See the corresponding clause in [ZE CPS-ID1-EID-CA].

9.4.4 Responsibility to protect private information

See the corresponding clause in [ZE CPS-ID1-EID-CA].

9.4.5 Notice and consent to use private information

See the corresponding clause in [ZE CPS-ID1-EID-CA].

9.4.6 Disclosure pursuant to judicial or administrative process

See the corresponding clause in [ZE CPS-ID1-EID-CA].

9.4.7 Other information disclosure circumstances

See the corresponding clause in [ZE CPS-ID1-EID-CA].

9.5 Intellectual property rights

See the corresponding clause in [ZE CPS-ID1-EID-CA].

9.6 Representations and warranties

9.6.1 CA representations and warranties

See the corresponding clause in [ZE CPS-ID1-EID-CA].

9.6.2 RA representations and warranties

See the corresponding clause in [ZE CPS-ID1-EID-CA].

9.6.3 Subscriber representations and warranties

See the corresponding clause in [ZE CPS-ID1-EID-CA].

9.6.4 Relying party representations and warranties

See the corresponding clause in [ZE CPS-ID1-EID-CA].

9.6.5 Representations and warranties of other participants

See the corresponding clause in [ZE CPS-ID1-EID-CA].

9.7 Disclaimers of warranties

See the corresponding clause in [ZE CPS-ID1-EID-CA].

9.8 Limitations of liability

See the corresponding clause in [ZE CPS-ID1-EID-CA].

9.9 Indemnities

See the corresponding clause in [ZE CPS-ID1-EID-CA].

9.10 Term and termination of the present TSPS

9.10.1 Term

See the corresponding clause in [ZE CPS-ID1-EID-CA].

9.10.2 Termination

See the corresponding clause in [ZE CPS-ID1-EID-CA].

9.10.3 Effect of termination and survival

See the corresponding clause in [ZE CPS-ID1-EID-CA].

9.11 Individual notices and communications with participants

See the corresponding clause in [ZE CPS-ID1-EID-CA].

9.12 Amendments to the present TSPS

9.12.1 Procedure for amendment

See the corresponding clause in [ZE CPS-ID1-EID-CA].

9.12.2 Notification mechanism and period

See the corresponding clause in [ZE CPS-ID1-EID-CA].

9.12.3 Circumstances under which OID must be changed

See the corresponding clause in [ZE CPS-ID1-EID-CA].

9.13 Dispute resolution provisions

See the corresponding clause in [ZE CPS-ID1-EID-CA].

9.14 Governing law

See the corresponding clause in [ZE CPS-ID1-EID-CA].

9.15 Compliance with applicable law

See the corresponding clause in [ZE CPS-ID1-EID-CA].

9.16 Miscellaneous provisions

9.16.1 Entire agreement

See the corresponding clause in [ZE CPS-ID1-EID-CA].

9.16.2 Assignment

See the corresponding clause in [ZE CPS-ID1-EID-CA].

9.16.3 Severability

See the corresponding clause in [ZE CPS-ID1-EID-CA].

9.16.4 Enforcement (attorneys' fees and waiver of rights)

See the corresponding clause in [ZE CPS-ID1-EID-CA].

9.16.5 Force Majeure

See the corresponding clause in [ZE CPS-ID1-EID-CA].

9.17 Other provisions

See the corresponding clause in [ZE CPS-ID1-EID-CA].

APPENDIX A - REFERENCES

See the corresponding Appendix in [ZE TSPS-ID1].

---------- Last page of this document ----------