Title:	**Zetes Estonia OÜ - Trust Services Practice Statement for the ID-1 Documents of the Republic of Estonia**
Label:	**[ZE TSPS ID1]**
Document OID:	**[1.3.6.1.4.1.47718.3.99].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

Document History

Version	Changes
2.0	Text was updated after the update of CP and CPS documents to version 2.0; Reference was made to the number of persons for a task in 5.2.2; the control on quality for public keys was added in 6.1.6; when private key backup is done was stipulated in 6.2.4; Communication of results to PBGB was added in 8.6; 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. Internal review version. Some minor adaptations. Also, all references to the HSM certification scheme concentrated into chapter 6.2.1. Chapter 6.2.11 now refers to 6.2.1. Updated chapter 6.6 and added Appendices 9 and 10 for references to the key generation standards for NIST and Brainpool curves. Corrected the e-mail address in 1.5.2.
1.1	For internal use only, no public effect, for pre-production context only. Internal review version. First adaptations after audit feedback. Chapter 5.6 and Appendix A.5
1.0	For internal use only, no public effect, for pre-production context only. Internal review version. Approved version for initial audit.

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 Trust Services Practice Statement (hereafter TSPS) covers the common practices applied by ZE as QTSP for delivering CA services that adhere to the Certificate Policies defined by the Police and Boarder Guard Board (hereafter PBGB).

This document is to be read in conjunction with the Certification Practice Statements [ZE CPS-ID1-EID-CA] and [ZE CPS-ID1-ROOT-CA]. All three document have the same chapter structure and refer to each other where appropriate.

Policies and Practice Statements

The following table lists all the related policy documents and practice statement documents, including this document:

Document OID	Document Reference and Document Title
[1.3.6.1.4.1.47718.3.99].01	**[ZE TSPS-ID1]** **Zetes Estonia OÜ - Trust Services Practice Statement for ID-1 Documents of the Republic of Estonia**
[1.3.6.1.4.1.47718.3.11].01	[ZE CPS-ID1-ROOT-CA] Zetes Estonia OÜ - Certification Practice Statement for the Root CA for ID-1 Documents of the Republic of Estonia
[1.3.6.1.4.1.47718.3.11].02	[ZE CPS-ID1-EID-CA] Zetes Estonia OÜ - Certification Practice Statement for the Intermediate CA for ID-1 documents of the Republic of Estonia
[1.3.6.1.4.1.47718.3.14].01	[ZE TC-ID1-SUB] Zetes Estonia OÜ – Subscriber Terms and Conditions for Subscriber Certificates issued by Zetes Estonia OÜ for ID-1 format identity documents of the Republic of Estonia
[1.3.6.1.4.1.47718.3.14].02	[ZE TC-ID1] Zetes Estonia OÜ - Relying Party Agreement and Terms and Conditions for CRL, OCSP, LDAP and other Services for Certificates issued by Zetes Estonia OÜ for ID1 Documents of the Republic of Estonia
[1.3.6.1.4.1.47718.3.13].01	[ZE PDS-ID1] Zetes Estonia OÜ –PKI Disclosure Statement for Subscriber Certificates issued by Zetes Estonia OÜ for ID-1 format identity documents of the Republic of Estonia
[1.3.6.1.4.1.51361].3	[PBGB CP-ID1-ROOT] Police and Border Guard Board – Certificate Policy for the root Certification Authority of the Republic of Estonia (Root CP)
[1.3.6.1.4.1.51361].2 for PBGB [1.3.6.1.4.1.51455].2 for MFA	[PBGB CP-ID1-EID] Police and Border Guard Board – Certificate Policy for ID-1 format identity documents of the Republic of Estonia (eID CP)

EU legislation and standards

Where applicable the QTSP follows the requirements laid down in the eIDAS Regulation [EU 910/2014 EIDAS] and the following normative standards set out by ETSI and CEN in the following European Norms (EN), Technical Reports (TR) and Technical Specifications (TS):

[ETSI EN 319 401]	Policy and security requirements for Trust Service Providers
[ETSI EN 319 411-1]	Policy and security requirements for Trust Service Providers issuing Certificates; Part 1: General requirements
[ETSI EN 319 411-2]	Policy and Security Requirements for Trust Service Providers issuing Certificates; Part 2: Requirements for trust service providers issuing EU Qualified Certificates

CEN and ETSI are officially recognized as European Standards Organizations by the European Union, see [EU 1025/2012].

Internet Engineering Task Force X.509 Standards

Where applicable the QTSP follows the following RFC:

[IETF RFC 3647]	X.509 Public Key Infrastructure - Certificate Policy and Certification Practices Framework
[IETC RFC 5280]	X.509 Public Key Infrastructure - Certificate and Certificate Revocation List (CRL) Profile
[IETF RFC 6960]	X.509 Public Key Infrastructure - Online Certificate Status Protocol – OCSP

The CA hierarchy and related services

Below is the schematic of the CA hierarchy and related services. The Root CA scope is highlighted in yellow. The Intermediate CA scope is highlighted in blue.

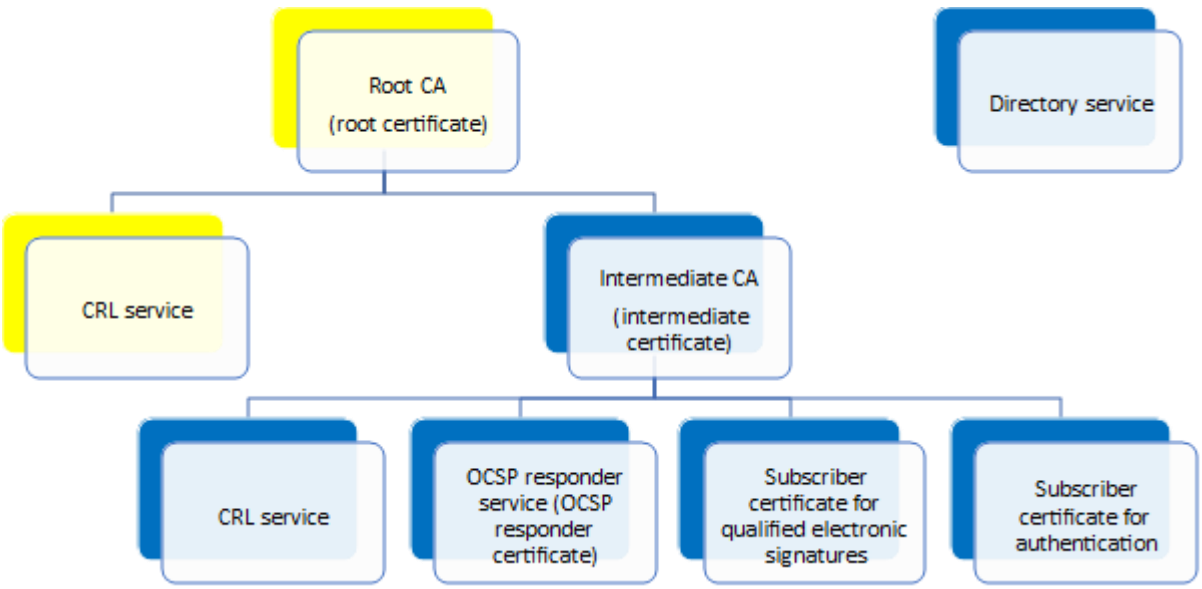

Figure 1. The CA hierarchy and related services for the Republic of Estonia.

The Root CA

The Root CA is the national trust anchor for managing and servicing the lifecycle of the 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 Certificates for Intermediate CAs and a CRL to validate the Intermediate CAs.

Intermediate CAs

Intermediate CA issues:

- Subscriber Certificates for ID-1 format identity documents of the Republic of Estonia (hereafter Documents)
- CRLs for validating the Subscriber Certificates

- Certificates for the OCSP service for validating the Subscriber Certificates

Public Certificate repositories

CA Certificates are published for http/https download on the ZE public repository web site. Valid Subscriber Certificates for authentication are published in the Lightweight Directory Access Protocol (LDAP) directory.

1.2 Document name and identification

See the table on the cover page of this document.

1.3 PKI Participants

1.3.1 Certification Authority (CA)

See the ZE Certification Practice Statements [ZE CPS-ID1-ROOT-CA] and [ZE CPS-ID1-EID-CA].

See the PBGB Certificate Policies [PBGB CP-ID1-ROOT] and [PBGB CP-ID1-EID].

1.3.2 Registration Authorities (RA)

See the ZE Certification Practice Statements [ZE CPS-ID1-ROOT-CA] and [ZE CPS-ID1-EID-CA].

See the PBGB Certificate Policies [PBGB CP-ID1-ROOT] and [PBGB CP-ID1-EID].

1.3.3 Subjects and Subscribers

See the ZE Certification Practice Statements [ZE CPS-ID1-ROOT-CA] and [ZE CPS-ID1-EID-CA].

See the PBGB Certificate Policies [PBGB CP-ID1-ROOT] and [PBGB CP-ID1-EID].

1.3.4 Relying Parties

See the ZE Certification Practice Statements [ZE CPS-ID1-ROOT-CA] and [ZE CPS-ID1-EID-CA].

See the PBGB Certificate Policies [PBGB CP-ID1-ROOT] and [PBGB CP-ID1-EID].

1.3.5 Other Participants

See the ZE Certification Practice Statements [ZE CPS-ID1-ROOT-CA] and [ZE CPS-ID1-EID-CA].

See the PBGB Certificate Policies [PBGB CP-ID1-ROOT] and [PBGB CP-ID1-EID].

1.4 Certificate Usage

1.4.1 Appropriate Certificate uses

See the ZE Certification Practice Statements [ZE CPS-ID1-ROOT-CA] and [ZE CPS-ID1-EID-CA].

See the PBGB Certificate Policies [PBGB CP-ID1-ROOT] and [PBGB CP-ID1-EID].

1.4.2 Prohibited Certificate uses

See the ZE Certification Practice Statements [ZE CPS-ID1-ROOT-CA] and [ZE CPS-ID1-EID-CA].

See the PBGB Certificate Policies [PBGB CP-ID1-ROOT] and [PBGB CP-ID1-EID].

1.5 Policy administration

1.5.1 Organisation administering the document

This document is administered by Zetes Estonia OÜ. The Policy Management Authority (PMA) is the internal management body that has overall authority and responsibility for the Trust Services for Documents.

The ZE PMA members are representatives from:

- Zetes Estonia OÜ, incorporated in Estonia, registry code 17066049
- Zetes SA, incorporated in Belgium, registry code 0408 425 626

Both are fully owned subsidiaries of Zetes Industries SA incorporated in Belgium, registry code 0425.609.373.

The ZE PMA responsibilities are:

- Selecting internal and external policies that will be used for the Trust Services operations.
- Approving the Practice Statements and defining their review process.
- Publication to the Subscribers and Relying Parties of the relevant declaration of practices and of policies.
- Continually and effectively managing PKI related risks.
- Specifying cross-certification or mutual recognition procedures and handling related requests.
- Defining internal and external auditing processes with the aim to ensure the proper implementation of the applicable practices, policies and procedures.
- Initiating and supervising internal and external audits and reviewing the audit recommendations.
- Initiating when appropriate highly sensitive PKI operations such as CA root key revocation and renewal or termination of the PKI services.

The ZE PMA internal rules are detailed in classified internal documents.

1.5.2 Contact person

The contact point for the TSPS and related CPS is

E-mail: < tc_cps_tsps AT ee.zetes.com >

1.5.3 Person determining suitability for the policy

The PBGB is the organization administering the Certificate Policies [PBGB CP-ID1-ROOT-CA] and [PBGB CP-ID1-EID-CA] that govern this TSPS and the CPS [ZE CPS-ID1-ROOT-CA] and [ZE CPS-ID1-EID-CA] that refer to it.

The PBGB and the PMA jointly validate the suitability of the TSPS and related CPS to the respective CP. The PBGB may involve the Information System Authority (hereinafter RIA) for an additional opinion.

The ZE PMA has the final authority to approve Practice Statement documents.

1.5.4 Approval procedures

The PBGB and the PMA jointly validate the suitability of the TSPS and CPS. The PBGB may involve the RIA for an additional opinion. The PMA confirms the final acceptance and publication of Practice Statement documents.

A Change Control mechanism is used to trace all identified changes to the content of the documents.

Practice Statement documents shall be reviewed at least once per year and whenever a major version change of the applicable Certificate Policies is published by the PBGB.

Changes are classified as either minor or major depending on their nature and their impact.

Assessment of the changes is conducted by the PMA.

For minor changes such as clarifications, simple error correction, typo corrections, reference updates, etc. only the minor part of the document version number will be incremented (i.e. from v1.0 to v1.1). For major changes the major document version number will be incremented (i.e. from v1.4 to v2.0).

Minor changes can be approved by the PMA members either during ordinary PMA meetings or by means of a written approval statement e.g. via e-mail poll. Major Changes must always be approved by the PMA members in a formal PMA meeting.

1.6 Definitions and acronyms

1.6.1 Definitions

Activation Data	Data values other than whole private keys that are required to operate private keys or cryptographic modules containing private keys, such as a PIN, passphrase, or portions of a private key used in a key-splitting scheme. Protection of activation data prevents unauthorised use of the private key.
Certificate	A unit of information contained in a file that is digitally signed by the Certification Authority. It contains, at a minimum, the issuer, a public key, and a set of information that identifies the entity that holds the private key corresponding to the public key.
Certificate Policy	A named set of rules that indicates the applicability of a Certificate to a particular community and/or class of application with common security requirements
Certificate Revocation List	A list of revoked and suspended Certificates. Abbreviated as CRL. It is (periodically) made available by the CA to Subscribers and Relying Parties.
Certification Authority	Depending on the context this term can refer to 1) the software and hardware system that constitute the infrastructure for issuing a Certificate or 2) the organisation that manages the CA keys, issues Certificates and updates a Certificate's status throughout a Certificate's lifecycle.
Certification Practice Statement	A statement of the practices which a Certification Authority employs in issuing managing, revoking, and renewing or re-keying Certificates.
Hardware Security Module (HSM)	Hardware Security Module. An electronic device offering secure key pair generation and storage, and implementing cryptographic operations using the stored key pairs.
Key Ceremony	A formal procedure to generate new keys for a CA.
Qualified Certificate	A Certificate which meets the requirements laid down in the eIDAS Regulation [EU 910/2014 EIDAS] and is provided by a Qualified Trust Service Provider who fulfils the requirements laid down in the Regulation.
Qualified Signature Creation Device	This is the PKI-enabled chip in the Document. For the purpose of a Qualified Electronic Signature (QES) with a Certificate that adheres to the policy [QCP-n-qscd], the chip complies with the requirements for a Qualified Signature Creation Device (QSCD) as specified in the eIDAS Regulation [EU 910/2014 EIDAS].
Registration Authority	Depending on the context this term can refer to 1) the software and hardware system that constitute the infrastructure for onboarding, registration, identity proofing of Subjects and/or Subscribers 2) the organisation that performs onboarding, registration and identity proofing.
Relying Party	Any person or entity other than the Subscriber or Subject itself that needs to use, and rely upon the accuracy of, the binding between the Subscriber/Subject public key distributed via that Certificate and the identity and/or other attributes of the Subscriber/Subject contained in that Certificate.
Revocation Ceremony	A formal procedure to revoke Certificates for CA.
Subject	Legal or natural person to whom a Certificate is issued and who has the usage rights for the Certificate. The Certificate name fields identify the Subject. This is defined in more detail in each specific CPS to align with the context of the CPS.
Subscriber	Legal or natural person that subscribes to the Trust Service. A Subscriber and a Subject can be the same or different entities. This is defined in more detail in each specific CPS to align with the context of the CPS.
Subscriber Certificates	A Certificate issued to a Subscriber. This is defined in more detail in each specific CPS to align with the context of the CPS.

1.6.2 Acronyms

Acronym	Full text
CA	Certification Authority
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
DN	Distinguished Name
HSA	High Security Area
HSM	Hardware Security Module
ICT	Information & Communication Technology
MFA	Ministry of Foreign Affairs of the Republic of Estonia
NTP	Network Time Protocol
OCSP	Online Certificate Status Protocol
OID	Object Identifier
PBGB	Police and Border Guard Board of the Republic of Estonia (Politsei- ja Piirivalveamet)
PDS	PKI Disclosure Statement
PIN	Personal Identification Number (private PIN-code for using the Document)
PKI	Public Key Infrastructure
PMA	Policy Management Authority
PUK	Personal Unblocking Key to reset the PIN-code
QSCD	Qualified Signature Creation Device

QTSP	Qualified Trust Service Provider
RA	Registration Authority
RIA	Information System Authority of the Republic of Estonia (Riigi Infosüsteemi Amet)
TSP	Trust Service Provider
TSPS	Trust Services Practice Statement
UTC	Coordinated Universal Time
ZE	Zetes Estonia OÜ

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 at the end of this document.

2 PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 Repositories

2.1.1 Overview

The QTSP maintains an online document repository for public information such as Terms and Conditions, Certificate Policies, Practice Statements, general information, CRLs and CA Certificates.

The repository is available 24/7 with a minimum of 99% availability overall per year with a scheduled down-time that does not exceed 0,5% annually.

CA Certificates and Certificate status information services such as CRL and OCSP are made available in standard-compliant formats and through protocols that support automated Certificate validation by standard-compliant software applications. The CA Certificates archive and the latest CRLs are also available for manual download from the public repository.

The QTSP does not publish information pertaining to certain security controls, procedures related to the functioning of inter alia registration authorities, internal security polices etc. Such documents and documented practices are, however, conditionally available to audit to designated parties that the QTSP owes duty to.

The landing page for the repository is: https://repository.eidpki.ee

The table below lists the available services and repositories:

repository.eidpki.ee	Landing page with links to: • general information about the trust services and the eID • announcements and notifications • links to the various sections of the public repository • a contact page
repository.eidpki.ee	Landing page with links to: • TSPS – Trust Service Practice Statements • CPS - Certification Practice Statements • PDS - PKI Disclosure Statements • Terms & Conditions • Certificate Profiles • links to Certificate Policies provided by PBGB
crt.eidpki.ee	Web page for manually downloading CA Certificates in addition to the direct links for automatic downloads using the URI encoded in the Certificates.
crl.eidpki.ee	Web page for manually downloading the latest CRL in addition to the direct links for automatic download using the URI encoded in the Certificates.
ocsp.eidpki.ee	Base URI for the OCSP service for immediate online Certificate status checks using URIs as encoded in the Certificates.
ldap.eidpki.ee	LDAP directory service
www.id.ee	Repository of the Information System Authority (*Riigi Infosüsteemi Amet - https://www.ria.ee*) of the Republic of Estonia containing the Certificate Policy documents.

2.1.2 LDAP directory service

Only valid Subscriber Certificates for authentication are published in the LDAP directory service. Subscriber Certificates for Qualified Electronic Signature are not published in the LDAP directory service. CA Certificates are not published in the LDAP directory service.

The service is available free of charge for Subscribers, Relying Parties and others. Usage of the service is subject to specific Terms and Conditions [ZE TC-ID1].

2.1.3 OCSP service

The service is available free of charge for Subscribers, Relying Parties and others. Usage of the service is subject to specific Terms and Conditions [ZE TC-ID1].

2.1.4 CRL service

The service is available free of charge for Subscribers, Relying Parties and others. Usage of the service is subject to specific Terms and Conditions [ZE TC-ID1].

2.1.5 Test eID Cards service

Test eID Cards need to be purchased separately. All services for Test eID Cards are out of scope for the eID CPS. Usage of the service is subject to specific Terms and Conditions [ZE TC-ID1-TEST].

2.2 Publication of certification information

2.2.1 Publication and Notification Policies

The availability of the CA's repository, the CA Certificate archive and the CRL repository is 99%, where 100% is defined as 24 hours per day, seven days per week. In case of unavailability of one or more of the services due to an act of God, failure of infrastructure outside the control of the QTSP or any other reason, the QTSP shall make best effort to reinstate availability of the service within 1 day.

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

- Links to the PBGB Certificate Policy documents [PBGB CP-ID1-ROOT] and [PBGB CP-ID1-EID].
- Trust Services Practice Statement [ZE TSPS-ID1]
- Root Certification Practice Statement [ZE CPS-ID1-ROOT-CA];
- eID Certification Practice Statement [ZE CPS-ID1-EID-CA];
- PKI Disclosure Statement [ZE PDS-ID1];
- Certificate Profiles [ZE PROFILES];
- the Subscriber Terms & Conditions [ZE TC-ID1-SUB] for the use of a Document with Subscriber Certificates
- the Relying Party Agreement and Terms & Conditions [ZE TC-ID1] for the reliance on and the use of the OCSP service, the CRL service, the LDAP directory service and the revocation portal service.

Any changes to the practice statements [ZE CPS-ID1-ROOT-CA], [ZE CPS-ID1-EID-CA] and [ZE TSPS-ID1], to the Certificate Profiles [ZE PROFILES] and to the Terms and Conditions [ZE TC-ID1] and [ZE TC-ID1-SUB] shall be approved by the PMA and by the PBGB Policy Administrator prior to publishing.

2.2.2 Items not published in the Certification Practice Statement

Information about service levels, fees and technical details laid down in mutual agreements between the CA, the RA and the Card Manufacturer are not published. Internal procedures of the PBGB, the MFA, the CA, the RAs (including PBGB's contract partners in a RA role), or the Card Manufacturer are not published.

2.3 Time or frequency of publication

Documents such as Practice Statements, Certificate Profiles and Terms & Conditions shall be published at least 30 calendar days before the enforcement date, unless there are special circumstances, which require a faster publication and enforcement date.

CA Certificates shall be published at least 30 calendar days before the first usage date.

Under normal operational conditions Subscriber Certificates for authentication are published in the LDAP repository within 30 minutes of activation of the Certificate.

For CA Certificate status publication via CRL see [ZE CPS-ID1-ROOT-CA].

For Subscriber Certificate status publication via CRL and OCSP see [ZE CPS-ID1-EID-CA].

2.4 Access controls on repositories

Only authorized staff and internal trusted systems of the QTSP have access rights to update, delete or create new objects in these repositories.

Subscribers and Relying Parties have read-only access via the internet to all the repository services. Information in the repositories is public information and is feely accessible online without access control or registration.

The QTSP reserves the right to control excessive use to protect the repositories and to ensure equal and fair availability for all users.

The QTSP will take reasonable measures to counter abuse of the repository services, in particular the OCSP service and CRL service, in the interest of giving all parties equal and unhindered access.

Restrictions on access to services provided by the repository include reasonable protection measures against abuse or denial-of-service attempts.

The QTSP reserves the right to reduce or refuse services to parties who make excessive use of the services to the extent that it would deprive other parties fair use of the services.

The QTSP reserves the right to charge for the services in mutual agreement with parties that require special service levels.

3 IDENTIFICATION AND AUTHENTICATION

3.1 Naming

3.1.1 Types of names

See the corresponding section in [ZE CPS-ID1-ROOT-CA] and [ZE CPS-ID1-EID-CA].

3.1.2 Need for names to be meaningful

See the corresponding section in [ZE CPS-ID1-ROOT-CA] and [ZE CPS-ID1-EID-CA].

3.1.3 Anonymity or pseudonymity of subscribers

See the corresponding section in [ZE CPS-ID1-ROOT-CA] and [ZE CPS-ID1-EID-CA].

3.1.4 Rules for interpreting various name forms

See the corresponding section in [ZE CPS-ID1-ROOT-CA] and [ZE CPS-ID1-EID-CA].

3.1.5 Uniqueness of names

See the corresponding section in [ZE CPS-ID1-ROOT-CA] and [ZE CPS-ID1-EID-CA].

3.1.6 Recognition, authentication, and role of trademarks

See the corresponding section in [ZE CPS-ID1-ROOT-CA] and [ZE CPS-ID1-EID-CA].

3.2 Initial identity validation

3.2.1 Method to prove possession of private key

See the corresponding section in [ZE CPS-ID1-ROOT-CA] and [ZE CPS-ID1-EID-CA].

3.2.2 Authentication of organization identity

See the corresponding section in [ZE CPS-ID1-ROOT-CA] and [ZE CPS-ID1-EID-CA].

3.2.3 Authentication of individual identity

See the corresponding section in [ZE CPS-ID1-ROOT-CA] and [ZE CPS-ID1-EID-CA].

3.2.4 Non-verified subscriber information

See the corresponding section in [ZE CPS-ID1-ROOT-CA] and [ZE CPS-ID1-EID-CA].

3.2.5 Validation of authority

See the corresponding section in [ZE CPS-ID1-ROOT-CA] and [ZE CPS-ID1-EID-CA].

3.2.6 Criteria for interoperation

See the corresponding section in [ZE CPS-ID1-ROOT-CA] and [ZE CPS-ID1-EID-CA].

3.3 Identification and authentication for re-key requests

3.3.1 Identification and authentication for routine re-key

See the corresponding section in [ZE CPS-ID1-ROOT-CA] and [ZE CPS-ID1-EID-CA].

3.3.2 Identification and authentication for re-key after revocation

See the corresponding section in [ZE CPS-ID1-ROOT-CA] and [ZE CPS-ID1-EID-CA].

3.4 Identification and authentication for revocation requests

See the corresponding section in [ZE CPS-ID1-ROOT-CA] and [ZE CPS-ID1-EID-CA].

4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 Certificate application

4.1.1 Who can submit a Certificate application

See the corresponding section in [ZE CPS-ID1-ROOT-CA] and [ZE CPS-ID1-EID-CA].

4.1.2 Enrolment process and responsibilities

See the corresponding section in [ZE CPS-ID1-ROOT-CA] and [ZE CPS-ID1-EID-CA].

4.2 Certificate application processing

4.2.1 Performing identification and authentication functions

See the corresponding section in [ZE CPS-ID1-ROOT-CA] and [ZE CPS-ID1-EID-CA].

4.2.2 Approval or rejection of Certificate applications

See the corresponding section in [ZE CPS-ID1-ROOT-CA] and [ZE CPS-ID1-EID-CA].

4.2.3 Time to process Certificate applications

See the corresponding section in [ZE CPS-ID1-ROOT-CA] and [ZE CPS-ID1-EID-CA].

4.3 Certificate Issuance

4.3.1 CA actions during Certificate issuance

See the corresponding section in [ZE CPS-ID1-ROOT-CA] and [ZE CPS-ID1-EID-CA].

4.3.2 Notification to subscriber by the CA of issuance of Certificate

See the corresponding section in [ZE CPS-ID1-ROOT-CA] and [ZE CPS-ID1-EID-CA].

4.4 Certificate acceptance

4.4.1 Conduct constituting Certificate acceptance

See the corresponding section in [ZE CPS-ID1-ROOT-CA] and [ZE CPS-ID1-EID-CA].

4.4.2 Publication of the Certificate by the CA

See the corresponding section in [ZE CPS-ID1-ROOT-CA] and [ZE CPS-ID1-EID-CA].

4.4.3 Notification of Certificate issuance by the CA to other entities

See the corresponding section in [ZE CPS-ID1-ROOT-CA] and [ZE CPS-ID1-EID-CA].

4.5 Key pair and Certificate usage

4.5.1 Subscriber private key and Certificate usage

See the corresponding section in [ZE CPS-ID1-ROOT-CA] and [ZE CPS-ID1-EID-CA].

4.5.2 Relying party public key and Certificate usage

See the corresponding section in [ZE CPS-ID1-ROOT-CA] and [ZE CPS-ID1-EID-CA].

4.6 Certificate renewal

4.6.1 Circumstance for Certificate renewal

See the corresponding section in [ZE CPS-ID1-ROOT-CA] and [ZE CPS-ID1-EID-CA].

4.6.2 Who may request renewal

See the corresponding section in [ZE CPS-ID1-ROOT-CA] and [ZE CPS-ID1-EID-CA].

4.6.3 Processing Certificate renewal requests

See the corresponding section in [ZE CPS-ID1-ROOT-CA] and [ZE CPS-ID1-EID-CA].

4.6.4 Notification of new Certificate issuance to subscriber

See the corresponding section in [ZE CPS-ID1-ROOT-CA] and [ZE CPS-ID1-EID-CA].

4.6.5 Conduct constituting acceptance of a renewal Certificate

See the corresponding section in [ZE CPS-ID1-ROOT-CA] and [ZE CPS-ID1-EID-CA].

4.6.6 Publication of the renewal Certificate by the CA

See the corresponding section in [ZE CPS-ID1-ROOT-CA] and [ZE CPS-ID1-EID-CA].

4.6.7 Notification of Certificate issuance by the CA to other entities

See the corresponding section in [ZE CPS-ID1-ROOT-CA] and [ZE CPS-ID1-EID-CA].

4.7 Certificate re-key

4.7.1 Circumstance for Certificate re-key

See the corresponding section in [ZE CPS-ID1-ROOT-CA] and [ZE CPS-ID1-EID-CA].

4.7.2 Who may request certification of a new public key

See the corresponding section in [ZE CPS-ID1-ROOT-CA] and [ZE CPS-ID1-EID-CA].

4.7.3 Processing Certificate re-keying requests

See the corresponding section in [ZE CPS-ID1-ROOT-CA] and [ZE CPS-ID1-EID-CA].

4.7.4 Notification of new Certificate issuance to subscriber

See the corresponding section in [ZE CPS-ID1-ROOT-CA] and [ZE CPS-ID1-EID-CA].

4.7.5 Conduct constituting acceptance of a re-keyed Certificate

See the corresponding section in [ZE CPS-ID1-ROOT-CA] and [ZE CPS-ID1-EID-CA].

4.7.6 Publication of the re-keyed Certificate by the CA

See the corresponding section in [ZE CPS-ID1-ROOT-CA] and [ZE CPS-ID1-EID-CA].

4.7.7 Notification of Certificate issuance by the CA to other entities

See the corresponding section in [ZE CPS-ID1-ROOT-CA] and [ZE CPS-ID1-EID-CA].

4.8 Certificate modification

4.8.1 Circumstance for Certificate modification

See the corresponding section in [ZE CPS-ID1-ROOT-CA] and [ZE CPS-ID1-EID-CA].

4.8.2 Who may request Certificate modification

See the corresponding section in [ZE CPS-ID1-ROOT-CA] and [ZE CPS-ID1-EID-CA].

4.8.3 Processing Certificate modification requests

See the corresponding section in [ZE CPS-ID1-ROOT-CA] and [ZE CPS-ID1-EID-CA].

4.8.4 Notification of new Certificate issuance to subscriber

See the corresponding section in [ZE CPS-ID1-ROOT-CA] and [ZE CPS-ID1-EID-CA].

4.8.5 Conduct constituting acceptance of modified Certificate

See the corresponding section in [ZE CPS-ID1-ROOT-CA] and [ZE CPS-ID1-EID-CA].

4.8.6 Publication of the modified Certificate by the CA

See the corresponding section in [ZE CPS-ID1-ROOT-CA] and [ZE CPS-ID1-EID-CA].

4.8.7 Notification of Certificate issuance by the CA to other entities

See the corresponding section in [ZE CPS-ID1-ROOT-CA] and [ZE CPS-ID1-EID-CA].

4.9 Certificate revocation and suspension

4.9.1 Circumstances for revocation

See the corresponding section in [ZE CPS-ID1-ROOT-CA] and [ZE CPS-ID1-EID-CA].

4.9.2 Who can request revocation

See the corresponding section in [ZE CPS-ID1-ROOT-CA] and [ZE CPS-ID1-EID-CA].

4.9.3 Procedure for revocation request

See the corresponding section in [ZE CPS-ID1-ROOT-CA] and [ZE CPS-ID1-EID-CA].

4.9.4 Revocation request grace period

See the corresponding section in [ZE CPS-ID1-ROOT-CA] and [ZE CPS-ID1-EID-CA].

4.9.5 Time within which CA must process the revocation request

See the corresponding section in [ZE CPS-ID1-ROOT-CA] and [ZE CPS-ID1-EID-CA].

4.9.6 Revocation checking requirement for Relying Parties

See the corresponding section in [ZE CPS-ID1-ROOT-CA] and [ZE CPS-ID1-EID-CA].

4.9.7 CRL issuance frequency (if applicable)

See the corresponding section in [ZE CPS-ID1-ROOT-CA] and [ZE CPS-ID1-EID-CA].

4.9.8 Maximum latency for CRLs (if applicable)

See the corresponding section in [ZE CPS-ID1-ROOT-CA] and [ZE CPS-ID1-EID-CA].

4.9.9 On-line revocation/status checking availability

See the corresponding section in [ZE CPS-ID1-ROOT-CA] and [ZE CPS-ID1-EID-CA].

4.9.10 On-line revocation checking requirements

See the corresponding section in [ZE CPS-ID1-ROOT-CA] and [ZE CPS-ID1-EID-CA].

4.9.11 Other forms of revocation advertisements available

See the corresponding section in [ZE CPS-ID1-ROOT-CA] and [ZE CPS-ID1-EID-CA].

4.9.12 Special requirements re key compromise

See the corresponding section in [ZE CPS-ID1-ROOT-CA] and [ZE CPS-ID1-EID-CA].

4.9.13 Circumstances for suspension

See the corresponding section in [ZE CPS-ID1-ROOT-CA] and [ZE CPS-ID1-EID-CA].

4.9.14 Who can request suspension

See the corresponding section in [ZE CPS-ID1-ROOT-CA] and [ZE CPS-ID1-EID-CA].

4.9.15 Procedure for suspension request

See the corresponding section in [ZE CPS-ID1-ROOT-CA] and [ZE CPS-ID1-EID-CA].

4.9.16 Limits on suspension period

See the corresponding section in [ZE CPS-ID1-ROOT-CA] and [ZE CPS-ID1-EID-CA].

4.10 Certificate status services

4.10.1 Operational characteristics

See the corresponding section in [ZE CPS-ID1-ROOT-CA] and [ZE CPS-ID1-EID-CA].

4.10.2 Service availability

See the corresponding section in [ZE CPS-ID1-ROOT-CA] and [ZE CPS-ID1-EID-CA].

4.10.3 Optional features

See the corresponding section in [ZE CPS-ID1-ROOT-CA] and [ZE CPS-ID1-EID-CA].

4.11 End of subscription

See the corresponding section in [ZE CPS-ID1-ROOT-CA] and [ZE CPS-ID1-EID-CA].

4.12 Key escrow and key recovery

4.12.1 Key escrow and recovery policy and practices

See the corresponding section in [ZE CPS-ID1-ROOT-CA] and [ZE CPS-ID1-EID-CA].

4.12.2 Session key encapsulation and recovery policy and practices

See the corresponding section in [ZE CPS-ID1-ROOT-CA] and [ZE CPS-ID1-EID-CA].

5 FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

5.1 Physical controls

Physical security measures and environmental controls commensurate with the value and critical nature of the assets they apply to are used. Physical and environmental security is aimed to prevent, deter, detect and delay unauthorized access, loss, theft, damage, compromise, interferences and interruption to business activities. The site operators for the PKI sites and the Card Manufacturer site have internal policies for physical security and environmental controls.

5.1.1 Site location and construction

The critical infrastructure such as the PKI infrastructure and the Card Manufacturer infrastructure is located in buildings that are fit for purpose and are organized, partitioned and segregated into distinct areas with specific physical security measures according to the type and sensitivity of assets and the operations conducted. The primary PKI site is certified [CENELEC EN 50600], [ISO 9001] and [ISO 27001]. The secondary PKI site is certified [ISO 9001] and [ISO 27001].

About site certifications:

[CENELEC EN 50600] covers physical security aspects and availability aspects such as power supply, fuse systems, telecommunications cabling, energy management and climate control, building construction and security systems, as well as criteria for data centre operations.

[ISO 27001] certification refers to an Information Security Management System compliant with the requirements, clauses and controls of ISO 27001 standard to effectively manage information security risks.

[ISO 9001] certification refers to Quality Management System compliant with the requirements of ISO 9001 standard to address customer expectations and to commit to continuous improvement.

Document Personalisation Site of the Card Manufacturer

The Document Personalisation Site is located in Tallinn, Estonia. The Personalisation Site is located on the first floor of an office building. Access to the Personalisation Site is strictly limited and there are no references to the Personalisation Site at this location.

The perimeter of the Personalisation Site is under constant surveillance and guarded by various security measures. The premises of the Personalisation Site are divided into different zones, with appropriate security measures in place to protect data, assets and staff.

The personalisation service provider holds [ISO 9001], [ISO 20000], [ISO 14001], [ISO 27001] and [AQAP 2110] certificates.

5.1.2 Physical access

PKI sites

The PKI infrastructure is hosted in sites that implement extensive security controls, including access control, intrusion detection and CCTV. Access to the sites is limited to authorized personnel. The Trust Service zones within these sites are located in areas appropriate for high-security operations. These areas feature numbered zones and locked rooms, cages, safes, and cabinets.

Physical access is controlled by means of physical access tokens and access control lists to control movement within the building and between zones, where applicable with controls like anti-pass back and anti-tail gating. Physical access system to the PKI infrastructure enforces multifactor authentication for entry and exit, is monitored by motion detectors and CCTV and features controls to prevent tailgating.

Doors to secured areas are equipped with electromechanical or magnetic locks. The security door to the server room or col-location hall are highly fire-resistant multi-walled steel doors in a fire-resistant steel door frame. The doors have secure locking bolts and an emergency release, a door closing delay, door monitoring system, door signal contact and bolt mechanism monitoring.

The building and/or secure areas inside the building have intrusion detection.

Equipment racks are located in a dedicated server room or in a security cage within a co-location server room. Equipment racks can only be opened by means of a personal access code. Controls are put in place for emergency access to the racks in case of flood or fire.

Document Personalisation Site of the Card Manufacturer

The Personalisation Site is divided into different zones, such as the general office area and High Security Area (HSA). HSA consist of a Document personalisation area, a PIN/PUK printing room, a Document destruction room, an IT admin room, a server room, a vault, a shipping room and a loading bay area.

The HSA windows are covered with security film, blackout film, and metal bars. All rooms in HSA can only be accessed by authorised personnel with access badges. Access to the server room and vault is permitted only under dual control.

Sluices and "man traps" are used to control movement in and out of HSA. The loading bay area is separated from the rest to facilitate Document handover to the security couriers. The area functions as a vehicle man-trap to ensure there is no direct physical interaction between the couriers and personalisation staff. A goods sluice system is used to hand over packages containing Documents and an intercom system along with cameras is used to control and communicate with the couriers in the loading bay area. All areas are monitored with sensors and cameras, and all movements in and out of the areas are logged.

5.1.3 Power and air conditioning

The PKI infrastructure is hosted in state-of-the-art server rooms with redundant power supply and redundant cooling systems. Essential IT components are powered with multiple and independent sources of power allowing their maintenance and replacement without total shutdown.

Primary PKI Site

The site is connected to multiple electricity grid connections for high availability of the power supply. The site has redundant UPS system, on-site redundant emergency generators. On-site fuel supplies are sufficient for several days of operations. The site has Class 1 lightning protection.

The site has state-of-the art data center climate control hot aisle compartment design, CAH (Custom Air Handler) units located outside the server hall, cold aisle temperature and pressure controls and independent redundant humidification and dehumidification systems.

All power and climate control systems are checked and tested periodically.

Secondary PKI Site

The site has redundant electrical distribution panels, for two separate power supplies to achieve TIER III protection level.

The site has redundant UPS system, on-site redundant emergency generators on opposite sides of the building and connections for additional external generators. When one of the generators is operational, the facility management is immediately informed, to monitor fuel levels and replenish fuel accordingly. The autonomy of each generators is at least 8 hours running time. Continuous fuel supply is covered by a contract for 24/7 fuel delivery.

The emergency generator is fuel powered, filled at regular intervals, and is tested monthly for its operational capability. The flow of energy is measured annually by simulating a power failure.

Document Personalisation Site of the Card Manufacturer

The electricity connection to the Personalisation Site is fully isolated from the rest of the building. In addition, in the server room, there is a stationary UPS that provides power in case of power outages to servers and network equipment, personalisation machines, garage doors, man-trap. There is also a standby in case a backup generator needs to be connected in the event of a longer power outage.

The access system to the Personalisation Site has its own power batteries in case of power failure. The video surveillance system has a separate UPS system.

All HSA rooms are equipped with forced ventilation, air conditioners and the capacity to ensure optimum air humidity. The server room air conditioner also has an additional back-up unit and installed temperature sensors connected to the alarm system.

5.1.4 Water exposures

The PKI infrastructure is hosted in state-of-the-art server rooms that have physical protection measures against water leakage or water intrusion originating from internal and external sources.

Primary PKI site

Data centre concept and design support all the possible mitigation measures against risks of water leakage to critical infrastructure or to client equipment. All the water pipes in data centre are routed around the critical areas with the racks and cabinets that house the servers, storage, and network gear, hot- and cold-aisle containment systems, and power distribution equipment, without crossing or passing over the room itself. The air handling units are in a separated technical room. Technical rooms are equipped with waterproof epoxy coating, emergency floor drainage systems and leak detection sensors in proximity of areas with potential leak risk. Sensors are integrated to BMS monitoring system.

Risk analysis, as the foundation for design, considers water leakage risks from various external sources such as rainfall, groundwater, flooding, and surface water caused by excessive rainfall or melting snow. Flooding risk is mitigated already in location selection phase by having plot height approximately 45 meters above the sea level and by being situated on higher ground compared to the surrounding area. The foundation and underground part of the facility are externally hydro-isolated. Additionally, the inground drainage system with redundant pumps is installed around and below the facility.

The rainwater system on the rooftop has been designed to avoid piping above server rooms or other critical infrastructure rooms. Specific stainless steel leak detection fabric is mounted between the layers of SBS roofing material. Leak detection system together with testing equipment allows to detect smaller than millimetre damages to the roofing material. Semi-annual inspections take place based on service agreement.

Secondary PKI Site

The secure area is dust and watertight to IP65 and has protection against standing water for 72 hours up to a water level of 40cm.

Document Personalisation Site of the Card Manufacturer

Server room, vault and production area have water leakage sensors installed and connected to the alarm system. No plumbing of any kind in the server room. Generally, the risk of water exposure in the HSA is deemed low (no main water pipes going over the ceiling which could have significant impact to the personalisation service or related infrastructure).

5.1.5 Fire prevention and protection

PKI office spaces have fire detection and fire extinguishing systems typical for modern office spaces.

The PKI infrastructure is hosted in state-of-the-art server rooms with systems and protocols for the prevention, detection and extinguishing of fires. Server rooms have systems to extinguish fires using inert gases.

Fire prevention, detection and extinguish systems are installed and maintained by accredited organizations and adhere to EU and national regulation.

Primary PKI Site

All rooms are built as separate fire-protection zones with a minimum EI-60 fire rating. Since adjacent service areas have close to zero combustion load and neighbouring server rooms have their own EI-60 fire-rated walls, the practical fire resistance is EI-120 with buffer zones between server rooms. Fire-resistant doors, walls, and fire-rated cable and pipeline penetrations are in place. Commonly used cable penetrations are of the re-sealable type.

The facility fire safety installation is designed and built according to the local fire code and to the fire safety requirements of EN 50600 standard.

All areas are equipped with corresponding smoke detection systems (conventional smoke sensors, precision sensors for high air velocity areas, temperature sensor cables, optical beam smoke detectors, aspirating smoke detection systems etc.), smoke extraction and fresh air compensation systems.

The battery rooms have their own dedicated hydrogen detection systems integrated to Battery Management System. Based on parameters the system alarms when reaching certain setpoint, activates dedicated hydrogen extraction ventilation system and/or intervenes UPS battery charging process.

Integration between fire safety, intrusion detection and CCTV systems allows monitoring centre to see instant corresponding live feed from any fire safety or security incident.

In server rooms and supporting technical rooms, an oxygen reduction system is used for fire prevention. Local oxygen extraction generator provides hypoxic air to the protected rooms, taking care of fresh air and overpressure of the server rooms at the same time. Oxygen levels are kept around 15% maintaining the non-combustible environment while still being safe for working in the room. For extra safety measures, while working alone in hypoxic room, a portable radio panic button is used with “man-down” functionality. In case of a health & safety incident corresponding room alarm with CCTV feed will be visible in monitoring centre.

Battery rooms and medium voltage switchgear rooms are equipped with automatic gas suppression system.

Numerous fire safety procedures and rules are implemented and following the rules is regularly monitored.

Data centre staff is attending on regular fire safety trainings.

All nearby fire departments have been organized to visit the site for training and familiarizing purposes.

The combustion load in the servers is kept to a minimum by prohibiting unnecessary materials and equipment unpacking in server rooms.

Secondary PKI Site

The server room is fireproof, class R60D, EN1047-2, has a fire detection panel and optical smoke detectors, in both the ceiling and in the false floor. The security door consists of a highly fire-resistant multi-walled steel door panel, a steel door frame and a fire-sealed flap. The server room has smoke detection in the ceiling and the false floors and a fire extinguishing system with inert gas to reduce the oxygen levels when a fire is detected. The server room has fire protection valves with an electric drive system (ventilation) for closing the ventilation and air-conditioning openings and with a pneumatic motor, for overpressure relief and for exhausting flue gases.

Document Personalisation Site of the Card Manufacturer

All rooms in the HSA has smoke detection in the ceiling (and the false ceilings) and a fire extinguishing system with inert gas to reduce the oxygen levels when a fire is detected. The ventilation system has fire protection valves with an electric drive system for closing the ventilation and openings for an overpressure relief. The doors between the specified fire-protection zones are of class EI60 and the walls of class EI120. Fire prevention, detection and extinguish systems is installed and regularly maintained by accredited company adhere to EU and Estonian regulation.

5.1.6 Media storage

Media are stored securely. Backup data are also stored in a location separate from the source and is physically secured and protected from fire and water damages. Media containing security critical data is stored in a safe and/or in a vault in a secured area.

5.1.7 Waste disposal

To prevent unwanted disclosure of sensitive data, paper waste and electronic waste is disposed of in a secure manner.

Documents and Document Activation data (PIN letters) are destroyed in a separate destruction room in the Personalisation Site with cross-cut shredder machine. Removable media is destroyed in the same destruction room using a dedicated shredder. Destruction activities are done under dual control and are logged.

5.1.8 Off-site backup

For the PKI infrastructure the QTSP uses two sites. Each site is used as the other’s site backup location. In case of an adverse situation as a natural disaster, fire, act of terrorism or war, the QTSP has implemented the necessary measures to recover and continue the critical trust services in accordance with its legal and contractual requirements.

The Card Manufacturer stores its off-site backups in other buildings owned by the Card Manufacturer and in a secure 3rd party storage service.

5.2 Procedural controls

5.2.1 Trusted roles

The QTSP follows personnel and management practices that provide reasonable assurance of the trustworthiness and competence of the members of the staff and of the satisfactory performance of their duties.

All members of the staff intervening in the key management operations (administrators, security officers, system auditors) or in any other operations that materially affect such operations are considered as serving in a trusted position.

Trusted roles are used for activities conducted to operate, maintain, monitor, review and communicate about PKI activities. Trusted roles are allocated to duly identified persons by the PMA.

Trusted roles are listed and defined and include:

- PKI Manager
- PKI Administrator
- PKI Operator
- System Administrator
- Security Officer
- Compliance Officer
- System Auditor
- CISO
- Key Custodians
- Registration and Revocation Officers

The QTSP conducts or delegates an initial investigation of all members of staff and external contractors who are candidates to serve in trusted roles in the PKI infrastructure before they are admitted in their function. The QTSP ensures that these people have the necessary expertise, reliability, experience, and qualifications and that they receive training when needed. The QTSP ensures that these people have the necessary awareness regarding security and personal data protection rules as appropriate for the offered services and the role.

The Card Manufacturer has a separate policy to clearly define all trusted roles within the Card Manufacturer organization that are related to Document personalization. Trusted roles in relation to key generation on the Document's QSCD chip and PIN letters are the production coordinator and card specialists/operators.

5.2.2 Number of persons required per task

Critical PKI assets and Card Manufacturer assets and operations such as key management operations are protected by means of dual control or multiple controls. At least two trusted roles need to combine their respective assets and/or (split) knowledge to be able to perform critical operations.

Generic ICT administration, operations and maintenance can be performed by internal or external resources. For all security critical cases a segregation of duties and dual-control or supervision is applied.

The Card Manufacturer applies dual control for inventory count and for destruction of Documents.

See also the corresponding clause in PBGB Certificate Policies [PBGB CP-ID1-ROOT].

5.2.3 Identification and authentication for each role

Each person acting in a trusted role is identified and authenticated to access the infrastructure to conduct his role either using multi-factor authentication, dual control and/or supervision.

5.2.4 Roles requiring separation of duties

All actions with respect to the CA can be attributed to the components of the CA and the member of the CA staff that has performed the action.

The QTSP ensures separation of duties for PKI operations between:

- PKI staff

- IT staff
- Security staff
- Audit staff

The Card Manufacturer ensures separation of duties for Document personalisation and delivery between:

- Document personalisation operators
- PIN letter personalisation operators
- Quality control staff
- Logistic staff
- IT staff
- Security staff
- Other staff

5.3 Personnel security controls

5.3.1 Qualifications, experience, and clearance requirements

Practices are implemented that provide reasonable assurance regarding trustworthiness and competence of the members of its own staff and contractor's staff. Qualification and experience are derived from learning and training records, professional experience, feedback from previous employers, trusted employee's recommendations, diploma's and Certificates delivered by recognized authorities.

5.3.2 Background check procedures

Background checks are conducted on prospective and existing employees who are involved in security critical operations on regular basis.

The background checks include:

- identity
- criminal record
- misrepresentations by the candidate
- appropriateness of references
- any clearances as deemed appropriate

Background checks concern employees of the QTSP and employees of other parties involved in the provision of certification service components and their respective subcontractors.

Background checks are carried out by an authorized and competent authority or third party in accordance with laws and regulations of the place of employment, with principles of ethics and with specific contractual requirements. The checks are proportional to the role and tasks of the person, the classification of the information to be accessed, and the potential risks.

5.3.3 Training requirements

The QTSP and the Card Manufacturer provide relevant internal and external training for its staff. Training, credentials and actual experience include security practices. Trainings are repeated periodically depending on the needs e.g. evolutions in technology, standards, compliance or other.

5.3.4 Retraining frequency and requirements

Periodic training updates will be carried out to establish continuity and updates in the knowledge of the personnel and procedures. This shall include (at least every 12 months) updates on new threats and current security practices.

Training plans are adapted to individual and role-specific requirements. For all members of staff, a training plan and training record is maintained.

5.3.5 Job rotation frequency and sequence

Due to the segregation of roles job rotation is generally not applied. Changes in roles are managed through training and competences management with respect of segregation of roles where applicable.

5.3.6 Sanctions for unauthorized actions

Personnel shall be accountable for their actions. The QTSP and the Card Manufacturer sanctions its respective personnel for unauthorized actions or violation of security procedures. Sanctions may include – but are not limited to – administrative or disciplinary action, revocation of privileges, dismissal, temporary suspension as well as civil or criminal proceedings. In case the unauthorized action was performed by an employee of subcontractor this may lead to the disqualification of the subcontractor.

5.3.7 Independent contractor requirements

The QTSP and other parties involved in the provision of certification service components will select their respective independent contractors or subcontractors based on evidences of trustworthiness and competences.

Independent contractors and subcontractors will be contractually required to implement measures that provide reasonable assurance regarding protection of privacy and confidentiality.

Independent contractors and subcontractor's employees involved in security critical operations will be subjected to background checks as specified in section 5.3.2 above.

For the delivery of Documents from the Personalisation Site of the Card Manufacturer to Document distribution points or issuance points, the Card Manufacturer maintains a list of individually approved couriers.

5.3.8 Documentation supplied to personnel

Personnel receives the necessary documentation available during initial training, retraining, or as part of operational activities. Documentation is supplied on a need to know basis.

5.4 Audit logging procedures

5.4.1 Types of events recorded

For all events related to the PKI key operations, records will be kept that include all information related to that event that can be useful for auditing purposes. Audit logs records contain date, time, user (or process) and type of the event as well as a link to or the identification of the implicated Document and Certificate, if applicable.

Extensive security logging and monitoring is performed at various levels including (non-exhaustive):

- the physical level (including equipment cabinet access)
- the network level
- the operating system level
- the application level

The QTSP PKI systems record events that include:

- Issuance of a Certificate: request, approval or rejection (with reason) of request, registration information, Identification of the RA approving or processing the request, Certificate generation/activation.
- Revocation of a Certificate: revocation request, approval or rejection (with reason) of request, Identification of the RA approving or processing the request, Identification of the requestor.
- Publishing of a CRL

The Card Manufacturer systems record events that include:

- Order Validation
- Document Application

- Document personalisation
- QSCD configuration and key generation events
- Certificate creation requests
- Certificate revocation requests
- Certificate re-key requests
- Document and PIN letter transport and delivery
- Document and PIN letter destruction
- Quality Assurance

Additionally, audit logs of relevant events in the ICT and HSM infrastructure are maintained that include:

- Log in and log out of administrative interfaces.
- Start and stop of servers.
- Outages and major problems.
- Physical access of personnel and other persons to sensitive parts of the PKI site.
- Backup and restore.
- Report of disaster recovery tests.
- Audit inspections.
- Upgrades and changes to systems, software and infrastructure.
- Security intrusions and attempts at intrusion.

5.4.2 Frequency of processing log

The QTSP regularly monitor security related events. Information about critical events is forwarded to the appropriate department for immediate attention. Reports that are generated from the audit logs are reviewed by internal auditors.

5.4.3 Retention period for audit log

Ordinary system logs used for system monitoring and diagnostics are retained for 18 months. CA and OCSP audit logs regarding Certificate lifecycle management and OCSP have a longer retention period, see section 5.5.2.

5.4.4 Protection of audit log

The QTSP audit logs are time stamped. CA audit logs are also signed. The log signature key is protected by an HSM. Consolidated logs are kept on secure storage systems or media and stored in a secure location.

5.4.5 Audit log backup procedures

Automated audit data is generated and recorded at the application, network and operating system level. Manually generated audit data is recorded by designated roles. For Key Ceremonies, a relevant extract of the audit log is made and stored separately.

5.4.6 Audit collection system (internal vs. external)

The PKI audit collection system is internal.

5.4.7 Notification to event-causing subject

Audit logs are aggregated and monitored continuously in a centralized system. Events that require attention are automatically flagged and notified to relevant staff by means of dashboards and various messaging systems.

5.4.8 Vulnerability assessments

The entire infrastructure is subject of a vulnerability assessment and penetration testing at least once a year and ad-hoc if a critical part of the infrastructure is affected. The assessment covers the ICT infrastructure, the special cryptographic

equipment, the physical environment, data storage, software, personnel, processes and procedures and communication.

Vulnerability assessment of the audit log is part of the risk assessment and risk management program documented internally.

5.5 Records archival

5.5.1 Types of records archived

See section 5.4.1 and 5.5.2.

5.5.2 Retention period for archive

The CA retains audit logs with event records regarding CA and OCSP key generation events, CA and OCSP Certificate issuance events and CA and OCSP Certificate life-cycle events for at least 10 years after the event.

The CA retains audit logs with event records regarding Subscriber Certificate issuance events and Subscriber Certificate life-cycle events for at least 10 years after the event.

The CA retains audit logs with event records regarding Certificate status validation services (CRL and OCSP) for at least 10 years after the event.

The CA retains records (copies) of all generated CA Certificates, OCSP Certificates and Subscriber Certificates for at least 10 years after the Certificate valid from date.

The RA and Card Manufacturer retain audit logs with event records regarding registration events, key generation events, Certificate request events and Certificate life-cycle events for at least 10 years after the event.

The PKI audit log retention periods for the various services are:

The RA retains information supporting the issuance and life-cycle management of the Subscriber Certificates for a period of at least 10 years after the Certificate ceased to be valid.

PBGB paper records are archived centrally at PBGB (this includes paper records from RA service points operated by contractors and embassies and include issuance notices, applications submitted at embassies). The record retention for Certificate related evidences are retained for the required duration as set in [EST EUTS ACT] and the requirements of [EU 910/2014 EIDAS].

PBGB electronic records are retained based on the database regulations which exceed eIDAS requirements and are laid down in the [EST ITDAK REG], [EST ABISDB REG] and [EST ARCHIVES ACT]. Electronic records held by the contractors of the RA are held by the contractors and are then transferred to PBGB.

MFA paper records are archived by the MFA. The record retention for Certificate related evidences are retained for the required duration as set in [EST EUTS ACT] and the requirements of [EU 910/2014 EIDAS].

MFA electronic records are retained based on the database regulations which exceed eIDAS requirements and are laid down in the [EST VEISDB REG].

The Card Manufacturer retains information supporting the issuance and post-issuance update of the Documents and Certificates for a period of at least 10 years after the Certificate ceased to be valid.

5.5.3 Protection of archives

Archives are protected against manipulation or wilful destruction. Where possible archives will be retained and protected in electronic form. Paper-based records are archived and under control of the respective roles that process them. Paper-based archive may be stored on multiple locations. Subject's registration information will be securely stored to provide reasonable assurance regarding confidentiality, integrity and availability.

5.5.4 Archive backup procedures

Backup copies of the relevant electronic system logs and electronic audit logs are stored in multiple locations. Back-up copies benefit from protection measures similar to the level of protection of the backed-up data (see 5.4.4 above).

Paper archives are not backed up.

5.5.5 Requirements for time-stamping of records

The date and time source for audit logs created by the core Trust Service components are synchronised with UTC using dedicated NTP equipment.

5.5.6 Archive collection system

Archives are collected and maintained by each participant entity separately. The PKI operator, the governmental RA operators and the Card Manufacturer each have their own archive collection systems. Information across the archives is correlated by unique identifiers for Documents, Certificates, Document personalisation orders and the time stamping on the records.

5.5.7 Procedures to obtain and verify archive information

Authorized personnel of the QTSP can access and extract archive information. Access to an archive by authorized personnel must be motivated (e.g. internal audit, external audit, in case of incident investigation, to test the “retrieval" procedure, obligations by law or court order, etc.).

Archive information disclosure to external parties is possible in the context of an authorized audit, investigation, or obligation by law or explicitly by court order or in the context of legal proceedings

PBGB and MFA as contracting authority can request archived information from the QTSP as part of the supervision of the contract with the QTSP for the provision of certification and qualified trust services as well as for termination or transfer of the Trust Services.

For requests from Subscribers, the QTSP shall promptly and without undue delay notify PBGB or MFA. Where the requests from the data subject are manifestly unfounded or excessive, in particular because of their repetitive character, the QTSP reserves the right to charge a compensation to cover the expenses of the retrieval of the information from the archives or refuse to act on a request

5.6 Key changeover

Key changeover for CA keys are exceptional events. New CAs will be announced in a coordinated communication campaign by the QTSP and by the authorities of the Republic of Estonia, specifically PBGB, MFA and RIA.

The QTSP will announce new CAs on its web site and via a subscription channels for Relying Parties. However, the main information channel for CA key changeovers will be the official web sites and other communication channels of PBGB, MFA and RIA. Subscribers may be informed through direct mails to the official e-mail address of Subscribers.

CA Certificates are published through one of the following methods:

- on the QSCD itself in the form of a complete Certificate chain
- in the QTSP online Certificate download repository
- in the Trust List of the Republic of Estonia

New CA Certificates will be made available as soon as possible through the Trusted List and the QTSP web site before the first Subscriber Certificates under the new CA will be issued.

Timing limitations may however apply to align with the Supervisory Body’s need to publish the CA Certificate on the Trust List of the Republic of Estonia.

In the case of a planned CA key changeover that does not affect existing Subscribers, the QTSP will announce the changeover at least 6 months before the first Subscriber Certificates under the new CA will be issued. The key changeover is coordinated with the issuance of identity Documents that will contain Subscriber Certificates from the new CA.

In the case of a CA key changeover that does affect existing Subscribers, typically involving a re-key operation for existing Subscribers, a different timing may apply.

In both cases, to the extent possible, the QTSP and Estonian government agencies such as PBGB, MFA and RIA will provide information, development tools, end user tools, test cards with test certificates and public test services a.o. a fake OCSP responder for developers and system integrators.

5.7 Compromise and disaster recovery

5.7.1 Incident and compromise handling procedures

The QTSP has an incident management procedure including incident reporting and handling procedure.

These procedures are established to ensure a quick, effective and orderly response to (information) security incidents providing knowledge to reduce the likelihood and impact of recurring incident. Incident records and gained knowledge are reviewed during the risk assessment exercise and participate from the risk management procedure.

The specific cases of key compromises are dealt in section 5.7.3.

5.7.2 Computing resources, software and/or data are corrupted

The QTSP establishes the necessary measures to ensure full and where possible automated recovery of CA services in case of a disaster, corrupted servers, software or data.

Computing resources, software and data are replicated in a second location. Backup copies of software and data are kept on regular base and available on both sites.

The distance between both locations is sufficient in case of a local natural disaster. The communication infrastructure and services between the two sites is sufficiently fast and secure to ensure data integrity and effective recovery point.

Disaster recovery infrastructure and procedures are to be fully tested at least once a year.

5.7.3 Entity private key compromise procedures

In case of a key compromise pertaining to a critical Trust Service component, the QTSP will

- document the incident
- notify the PMA
- notify PBGB
- notify the Supervisory Body
- decommission the compromised key
- notify impacted parties
- revoke the Certificates impacted by the corrupted CA
- assess the relevance to revoke all Certificates (this depends amongst other on the time of compromise)
- inform the relevant authorities as required by contract or legislation

By decision of the PMA and providing that the cause of compromise has been discarded, the QTSP may generate a new key and Certificates to resume service.

In case of a key compromise pertaining to a Subscriber, the Subscriber's Certificates will be revoked and may be replaced. The Subscriber has to notify the QTSP of any compromise or suspicion of compromise of their private key. Case-specific obligations for all PKI participants with respect to key compromise are stated in the applicable CPS and CP and the applicable Terms & Conditions for the PKI participant.

5.7.4 Business continuity capabilities after a disaster

A Business Continuity Plan is in effect to ensure business continuity following a natural or other disaster.

The QTSP establishes the necessary measures for full recovery of the on-line services in case of a disaster, corrupted servers, software or data.

Recovery of off-line Root CAs is ensured by the activation of the Root CA's backup at the secondary site. Resources and secrets are distributed across several sites to ensure that all the needed resources and secrets to continue the service will still be available in case one site is completely and definitely destroyed.

The PMA will assess the measures to be taken regarding the protection of resources and information on the disabled site, the need to revoke the CA's impacted by the disaster (as the protection of disabled site cannot be ensured) and the setup of a third site.

5.8 CA or RA Termination

Terminating a Trust Service and as a result terminating, when applicable, the CA(s) and other PKI component services is an event as important as their initiation. Both require planning of the physical, logical, operational, procedural and human aspects. Security of information and reputation is at risk. Furthermore, specific contractual requirements and legal requirements apply.

For clarification, the case of cessation of the issuance of new Certificates while all other services such as revocation services, Certificate status information services (e.g. CRLs, OCSP) or the controlled transfer of services and components to another QTSP or transfer from an old CA to a new CA are not considered as termination.

The Termination Plan covers the procedures to be completed in a situation where all services associated with Qualified Certificates are terminated. The following is a summary of the minimum procedures that are applicable in such a case.

In the context of a planned normal termination:

- Cessation of the issuance of any new Qualified Certificate
- Termination notification to the national Supervisory Body, the Subscribers and Relying Parties within 3 months and no later than 2 months before the effective termination
- Dissemination of relevant information
- Preservation and transfer of auditing and archival records to the arranged custodian
- Revocation of unexpired and unrevoked Certificates
- Creation of the last and final CRL
- When applicable, decommissioning of the CA keys

In the context of an unplanned termination:

As far as it is possible, the plan for planned termination as described in section above will be followed with the following potential significant differences:

- Shorter or no delay for the notification of the interested parties
- Shorter or no delay for the revocation of Certificates

After the termination the CA will hand over records and other relevant data to PBGB as specified by contract between the QTSP and PBGB.

PBGB and MFA as the RAs are permanent institutions established by the government of Republic of Estonia. As such, they are intended to operate indefinitely and continuously fulfil their mandated functions.

PBGB and MFA are responsible for termination plans with contractors in RA roles. For contractors in RA roles with subcontractors fulfilling some or all of those RA duties, the contractor is responsible for having a termination plan for their subcontractor.

PBGB is the Contracting Authority towards the QTSP and other Parties involved in the issuance of Certificates and Documents. PBGB has a Termination Plan Guidance document to manage termination of activities. PBGB conducts an annual risk assessment to determine if any of the activities are scheduled or at risk of termination. When a decision to termination is taken, a concrete Termination Plan will be created based on the Termination Plan Guidance document.

6 TECHNICAL SECURITY CONTROLS

6.1 Key pair generation and installation

6.1.1 Key pair generation

Key pair generation for CAs

The key pairs for CAs are generated on-board an HSM, under the authority of and with the explicit consent of the PMA. The key pair generation is performed under the supervision of a Security Officer, under at least dual control and as part of a Key Ceremony in the presence of representatives of the PBGB and invited witnesses.

Key pair generation for the OCSP service

The key pairs for the OCSP service components are generated on-board an HSM, under the authority of the PMA. New OCSP keys and Certificates are generated under supervision of a Security Officer, under dual control and as part of a formal Key Ceremony. Key and Certificate renewal may be an automated scheduled process.

Key pair generation for Subscribers of the Intermediate CAs

The key pairs for Subscribers of the Intermediate CAs are generated on-board a QSCD in the Document of the Subscriber.

6.1.2 Private key delivery to Subscriber or Subject

For PKI components the private key delivery is an implicit consequence of the key generation process in the HSM.

The private keys for Subscribers are delivered on the QSCD for the Subscriber of the Intermediate CAs as part of the Document delivery and handover to the Subscriber.

6.1.3 Public key delivery to Certificate issuer

Public Key delivery to the offline Root CA

The Root CA is an offline CA. Certificate requests (that include the public key of the requester) are transferred by means of a secure storage medium. The storage medium's technical characteristic protects the data content against unauthorized manipulation. The transfer is done in a single Key Ceremony, in the presence of witnesses, and with a direct transfer of the public key following the generation of the key pair.

This applies for public keys of the Intermediate CAs. The procedures, the Key Ceremony, the tools used and the environment in which the key pair is generated and the public key extracted, ensure the requester is in possession of the private key for which the Certificate is requested.

Public Key delivery to the Intermediate CA

Delivery of the public key for OCSP Certificates:

The Intermediate CA has a secure internal network connection to internal systems for Certificate revocation and for generating Certificates. Public keys are transferred via secure system to system connections (e.g. for automated renewal) or are manually uploaded to the CA by an authorized PKI Administrator (e.g. for initial Certificate creation).

The procedures, the Key Ceremony, the tools used and the environment in which the key pair is generated and the public key extracted, ensure the requester is in possession of the private key for which the Certificate is requested.

Delivery of public key for Subscriber Certificate requests

Certificate requests are transferred by means of a secure network connection between the RA and the CA.

For keys generated on QSCDs the following method is supported:

- the public key is extracted from the QSCD as part of the initial personalisation process or a post-issuance personalisation process under the control of the Document issuer (either the PBGB or the MFA) and the Card Manufacturer under contract of the PBGB

- a Certificate request message that incorporates the public key along with all the required metadata relevant to the Subscriber and the Document, is forwarded from the Card Manufacturer to the CA via the PBGB using the X-tee data exchange system
- the CA's X-tee security server validates the authenticity of the message, extracts the data from the message and forwards it to the CA, the CA generates the Subscriber Certificate and returns it to the Card Manufacturer via the PBGB using the X-tee data exchange system
- the Card Manufacturer installs the Subscriber Certificates in the QSCD as part of an initial personalization process or a post-issuance personalization process

6.1.4 CA public key delivery to Relying Parties

CA public keys are made available to Relying Parties in the form of X.509 Certificates that shall be published on a publicly available website. See clause 2.1.

Relying Parties shall be able to authenticate the website by means of the SSL/TLS server authentication Certificate which is issued by a public CA that is external to the CA hierarchy.

Relying Parties shall be able to authenticate a CA Certificate by means of the Certificate "thumbprint" that shall be published in a signed document in ASICE format.

Relying Parties may contact ZE to receive confirmation of the "thumbprint" of a CA Certificate by means of an out-of-band channel such as a telephone call, e-mail or letter.

The CA Certificates are also distributed as part of the full Certificate chain which is stored in the secure memory of the QSCD in the Document. Some applications can extract the complete Certificate chain from the QSCD and embed the CA Certificates in the transaction or document for receipt and validation by Relying Parties. These applications are not controlled by the CA.

6.1.5 Key sizes

See [ZE PROFILES].

The QTSP is not in any way held to continue using the current algorithms, protocols or key lengths should the QTSP decide that the current algorithms, protocols or key lengths provide insufficient assurance and security for the intended purpose and the intended use period.

6.1.6 Public key parameters generation and quality checking

CA and OCSP keys are generated on-board certified HSM. NIST Elliptic Curve keys are generated in accordance with [NIST 186]. Brainpool-curve keys are generated in accordance with the [RFC 5639] standard or the [ECC BP] standard to ensure the quality of the keys. 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)

The QTSP ensures that the key usage properties encoded in the Certificates correspond with the intended use of the Certificates. The key usage properties are encoded in the Certificates as Key Usage and Extended Key Usage fields that correspond with the intended use of the Certificates as defined in [ETSI EN 319 411] part 1 and 2 and in [ETSI EN 319 412] part 1, 2 and 5. For details about the encoded key usage, see Certificate Profiles [ZE PROFILES].

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic module standards and controls

The HSM infrastructure for the CA and OCSP infrastructure complies with the Common Criteria security certification scheme as mentioned in [ETSI EN 319 411-1] and in [ETSI EN 319 411-2].

The HSM for the CA infrastructure are CC-certified with assurance level "EAL4 augmented with AVA_VAN.5 Advanced Methodical Vulnerability Analysis (EAL4+ conformant)". The HSM for the OCSP infrastructure are CC-certified with

assurance level “EAL4 augmented with AVA_VAN.5 Advanced Methodical Vulnerability Analysis and ALC_FLR.3 (EAL4+ conformant)”.

Physical access to the HSM is limited to authorised personnel only. The HSM equipment is installed in a secure environment. Operational use of the HSM equipment is controlled by activation assets (e.g. smartcards, key activation keys) and/or activation data (e.g. PIN codes, passphrases, etc.). Activation assets and activation data are assigned to multiple custodians and are stored in a secure location. The separation of activation assets and activation data is organized such that no single custodian can exercise control over the protected key material.

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

The activation and/or use of the private keys in the HSM infrastructure that hold the private keys for the PKI is controlled by access control procedures and activation mechanisms that require 2 or more custodians to be involved in the process. The activation assets or activation data needed for the activation and/or use of the HSMs is under control of yet more trusted roles and are not directly accessible to the custodians. Custodians require prior approval by the authorized Security Officer to be allowed access to the activation assets or activation data under their care.

6.2.3 Private key escrow

Not applicable.

6.2.4 Private key backup

Private keys on an HSM for CA and OCSP are generated on-board the HSM and are backed up in encrypted format during the key ceremony. The backups are exclusively used to:

- restore for recovery in case of failure of the HSM
- restore in case of replacement of an HSM
- initialize additional HSMs

The backup of the keys is encrypted inside the HSM. The encrypted key backups are exported from the HSM into a backup file set. The backup encryption key is itself generated inside the HSM during the installation and initialization of HSM and is secured by means of a set of HSM backup cards.

Backup and restore or transfer of private keys requires a quorum of m-out-of-n HSM backup cards. Each card has an activation code which is independent from the other cards.

The key backups, the activation assets and the activation data are assigned to multiple custodians and are stored in separate locations.

6.2.5 Private key archival

Private keys are not archived.

6.2.6 Private key transfer into or from a cryptographic module

PKI CA and OCSP keys are generated on-board the HSM and can be transferred to another HSM. Transfer of private keys to another HSM requires multi-person control using a quorum of HSM assets.

6.2.7 Private key storage on cryptographic module

Keys inside an HSM are protected by the HSM-specific security mechanisms including access conditions and conditions for key extraction formats e.g. for backup, and usage conditions for other purposes.

Keys are stored in a special memory area of the HSM which is connected to the sensory controller of the HSM. The sensory controller can, in a case of an alarm, delete or render useless the key material in the HSM. The implementation specifics may vary between HSM makes and models.

6.2.8 Method of activating private keys

Activating and authorizing the private keys for the Root CA a is restricted by a dual control mechanism.

Private keys for 24/7 services such as Intermediate CAs and OCSP are automatically activated in case of a controlled reboot to guarantee continuity of service. A reboot of the HSM requires the reauthorization of the signing key(s).

Access to the control interface for importing or exporting a key is restricted by a dual control mechanism.

6.2.9 Method of deactivating private key

Keys in HSMs are deactivated either by a manual operation by an authorized operator or by shutting down/resetting the computer that holds the HSM.

6.2.10 Method of destroying private key

The HSM's internal mechanism for reset to factory or for zeroize is used to render useless all keys stored in the HSM and thus effectively destroying all the private keys in that HSM. This procedure is applied when an HSM is to be removed for repair, replacement or decommissioning or when the HSM needs to be re-initialized.

Private keys can be selectively destroyed if the key assignment is deleted in the configuration of the CA or PKI component. When a key in the HSM is deleted, the relevant record in the HSM's internal key database is marked as deleted which immediately deactivates the key and makes it unavailable. The key will also be zeroized and deleted from the HSM memory.

6.2.11 Cryptographic Module Rating

See chapter 6.2.1.

6.3 Other aspects of key pair management

6.3.1 Public key archival

The QTSP maintains an internal archive of all CA public keys and all public keys certified by the QTSP Qualified CA in the form of the Certificates that contain the public key. See clause 5.5.2 for archival retention periods.

6.3.2 Certificate operational periods and key pair usage periods

A Root CA will not issue Certificates that exceed the Certificate expiration date of the CA Certificate. The Intermediate CA will not issue Certificates that exceed the Certificate expiration date of the CA Certificate. The key usage period of a CA key is aligned with the expiration date / lifetime of the Certificates issued with that key.

See [ZE CPS-ID1-ROOT-CA] for more detail.

6.4 Activation data

6.4.1 Activation data generation and installation

All activation data related to the Root and Intermediate CA key pairs are generated and stored in HSM during Key Ceremony under dual control and the supervision of the Security Officer and witnessed by a representative from PBGB and an auditor.

6.4.2 Activation data protection

All activation data such as PIN codes, passwords and passphrases and activation assets such as smartcards are securely stored in multiple locations.

Activation data and the associated activation assets are assigned to multiple custodians.

Where relevant, activation data such as passwords and passphrases are split in parts and each part is assigned to a different custodian. The length, syntax, structure and guidelines regarding the content of the activation data ensures that the activation data for critical assets is non-trivial and contains sufficient variation.

6.4.3 Other aspects of activation data

No stipulations.

6.5 Computer security controls

6.5.1 Specific computer security technical requirements

The computer security controls are implemented according the technical standard [ETSI EN 319 411]. The Implemented Information Security Management System is [ISO IEC 27001] compliant and includes several controls related to computer security a.o.

- Firewalls to protect the internal network domain from unauthorized access and to prevent all accesses and protocols that are not required for the operation of the TSP
- Control of sensitive data stored on “demobilized” or reusable storage device
- Local network components are kept in a secure environment and their configuration is periodically checked
- Use of multifactor authentication for account capable to issue Certificates
- Enforced access control to modify disseminated information regarding Certificates.
- Enforced access control to modify revocation status information through TLS mutual authentication between the CA and the OCSP server and between CA and the CRL publication infrastructure.
- Access control, intrusion detection system and CCTV monitoring to detect, record and react upon unauthorized physical access to its resources

6.5.2 Computer security rating

No stipulations.

6.6 Life cycle technical controls

All core hardware and software for operating a Trust Service is procured from reputed manufacturers or developed in-house in a manner which will mitigate the risk that any particular component could be tampered with. Equipment for use within the QTSP PKI infrastructure shall be staged, deployed and maintained in a controlled environment under strict change control procedures. System configurations are kept minimalistic and where possible the principle of least privilege is applied.

6.6.1 System development controls

Implemented in compliance with [ETSI EN 319 411-1].

6.6.2 Security management controls

Implemented in compliance with [ETSI EN 319 411-1].

6.6.3 Life cycle security controls

Implemented in compliance with [ETSI EN 319 411-1].

6.7 Network security controls

The QTSP PKI operator with regard to the Trust Services activities ensures the maintenance of a high-level network of systems security including firewalls. Network intrusions are monitored and detected.

Certificate creation and lifecycle management data exchange between the CA, RA and Card Manufacturer is done using the secure data exchange service “X-tee” of the Republic of Estonia.

The network segment for the network-connected Intermediate CAs is protected by firewalls and intrusion detection system and is segregated from other internal network segments.

The network-connected Intermediate CAs use encrypted connections (confidentiality) and strong authentication for access by administrators, operators and for other systems that connect to the CA servers. Strong authentication is implemented by means of Certificates that are issued by the internal management CA of the CA infrastructure itself.

Network equipment configurations are periodically reviewed and updated or patched.

Network penetration tests are periodically performed.

6.8 Time-Stamping

For date and time synchronization the QTSP uses internal NTP infrastructure for its PKI infrastructure to synchronize the system clocks of critical infrastructure with recognized NTP services such as the Royal Observatory of Belgium (UTC(ROB)). The Observatory maintains 4 of the atomic clocks of the worldwide UTC network and disseminates the time via the Network Time Protocol (ntp1.oma.be and ntp2.oma.be).

In the unlikely event that no external UTC time source is available, the NTP infrastructure can maintain accurate time independently by means of high-precision oscillators.

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

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

8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS

eIDAS compliance audit

The eIDAS compliance audit overarches other audits and assessments and is therefore the primary scope of this chapter.

Overall the QTSP applies the policy and security requirements set out in in the European technical standards ETSI EN 319 401, ETSI EN 319 411 – 1 and ETSI EN 319411-2 for Trust Service Providers issuing Certificates. The Certificates, CRL and OCSP services adhere to IETF RFC 6818, RFC 5280 and RFC 8399.

The QTSP operates according to the terms of the eIDAS Regulation [EU 910/2014 EIDAS] that stipulates the legal framework for trust services in the European Union. The QTSP plans compliance audits and other assessments to ensure it meets the legal and technical requirements, the practices and the service levels according to the applicable Practice Statement.

The PKI participants that perform the role of CA, RA and Card Manufacturer all participate in the eIDAS audits for their respective roles.

The findings from eIDAS compliance audits and other assessments are evaluated by the PMA and addressed accordingly.

Other audits and assessments

The PKI participants that perform the role of CA, RA and Card Manufacturer also organize additional audits and assessments for their respective activities in support of the eIDAS compliance audits and their contractual obligations or legal obligations.

8.1 Frequency or Circumstances of Assessment

Compliance with the eIDAS Regulation [EU 910/2014 EIDAS] is audited by an accredited Conformity Assessment Body at least once every two years or whenever a major change is made to the Trust Service operations.

Internal audits for the CA are conducted according an audit plan approved by the PMA and shall be performed at least once every 12 (twelve) months. Internal audits for RA and Card Manufacturer participants are done by each participant independently and according to each participant's respective audit plan.

Under special circumstances (I.e. a security breach) unplanned audits and assessments may be conducted on request of the Supervisory Body, the conformity Assessment Body, the PBGB or the PMA.

8.2 Identity/qualifications of assessor

The eIDAS Regulation [EU 910/2014 EIDAS] establishes the requirements for Trust Services providers (TSP) that offer defined trust services such as the issuance of Certificates to natural persons within the internal market. The qualification of trust service provider is given by the Supervisory Body of Estonia. The qualification is decided on the basis of an audit report issued by an accredited Conformity Assessment Body.

Compliance of the QTSP with the eIDAS Regulation [EU 910/2014 EIDAS] is audited by an accredited Conformity Assessment Body as defined in Regulation (EC) No 2008/765 point 13 of article 2 and in ETSI EN 319 304 Electronic signatures and infrastructures (ESI) - evaluation of trust service providers - Requirements for conformity assessment bodies assessing trust service providers.

The accredited Conformity Assessment Body is:

CAB name:	LSTI
CAB web site:	https://www.lsti-certification.fr/

The Supervisory Body:

The Supervisory Body for the Republic of Estonia resides under the Information System Authority (RIA).

8.3 Assessor's relationship to assessed entity

The eIDAS audits and ISO 27001 audits are carried out by independent auditors who will not be affiliated directly or indirectly in any way with the QTSP or the respective PKI participants.

8.4 Topics covered by assessment

The periodic eIDAS audits cover –but are not limited to – all aspects of the QTSP's operations and related services as specified in the applicable Practice Statements and Policies according to the introduction of section 8. In particular:

- Management of the infrastructure that implements QTSP services;
- Management of the physical site infrastructure;
- Adherence to the Certificate Policies, Certification Practice Statements and Trust Services Practice Statement;
- Adherence to [EU 910/2014 EIDAS];
- Adherence to the applicable ETSI standards;
- Inspection of audit trails, logs and relevant documents;
- Protection of Subscriber data;
- Cause of any failure to comply with the conditions above.

8.5 Actions taken as a result of deficiency

Detected deficiencies and non-conformities found in eIDAS Audits will be reported to the PMA in writing. Additional oral comments and clarifications can be provided by the auditor.

The PMA will assess the severity and the extent of the detected deficiencies. In accordance with the auditor, the PMA will determine the time frame and the actions to be conducted to rectify the deficiencies.

A follow-up audit to verify the effectiveness of the actions conducted can be decided by the PMA to ensure compliance.

In the event of a result showing deficiency in the assessment, the Supervisory Body may require ZE to remedy any failure to fulfil requirements within a time limit (if applicable) set by the Supervisory Body.

8.6 Communication of results

The eIDAS Audit Report and other findings are communicated by the auditor to the audited entities and to the PMA.

The QTSP shall submit the resulting conformity assessment report to the Supervisory Body and the PBGB within the period of three working days after receiving it.

In some circumstances, e.g. suspicion of internal fraud, the auditor will not disclose his findings to the audited entity.

All audit reports are classified as confidential information and are distributed on a need-to-know basis. Conformity assessment attestation letter(s) and Certificate(s) for qualified trust services shall be published on the repository.

9 OTHER BUSINESS AND LEGAL MATTERS

All aspects pertaining to this chapter are grouped in chapter 9 of [ZE CPS-ID1-EID-CA].

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

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

A.1 EUROPEAN LEGISLATION

[EU 910/2014 EIDAS] Regulation (EU) 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.
Published https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02014R0910-20241018

[EU 679/2016 GDPR] Regulation (EU) 679/2016 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: http://data.europa.eu/eli/reg/2016/679/oj

[EU 765/2008 ACC] 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: http://data.europa.eu/eli/reg/2008/765/2021-07-16

[EU 1025/2012 STND] Regulation (EU) No 1025/2012 of the European Parliament and of the Council of 25 October 2012 on European standardisation**,** amending Council Directives 89/686/EEC and 93/15/EEC and Directives 94/9/EC, 94/25/EC, 95/16/EC, 97/23/EC, 98/34/EC, 2004/22/EC, 2007/23/EC, 2009/23/EC and 2009/105/EC of the European Parliament and of the Council and repealing Council Decision 87/95/EEC and Decision No 1673/2006/EC of the European Parliament and of the Council Text with EEA relevance.
Published: http://data.europa.eu/eli/reg/2012/1025/oj

[EU 1502/2015] 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: http://data.europa.eu/eli/reg_impl/2015/1502/oj

[EU 650/2016 QSCD] Commission Implementing Decision (EU) 650/2016 of 25 April 2016, which sets the standards for the security assessment of qualified signature creation devices (QSCD) pursuant to the eIDAS Regulation
Published: http://data.europa.eu/eli/dec_impl/2016/650/oj

A.2 REPUBLIC OF ESTONIA LEGISLATION

[EST ABISDB REG] ABIS Database Regulation
Published: https://www.riigiteataja.ee/akt/103102023017?leiaKehtiv

[EST ARCHIVES ACT] Archives Act
Published: https://www.riigiteataja.ee/en/eli/ee/521032019019/consolide/current

[EST CONSULAR ACT] Consular Act, RT I 2009, 29, 175.
Published: https://www.riigiteataja.ee/en/eli/ee/527012016004/consolide/current

[EST CYBERSEC ACT] Cybersecurity Act.
Published: https://www.riigiteataja.ee/en/eli/523052018003/consolide

[EST DIPLCARD REG] Procedure, form, technical specifications and list of data to be entered on the diplomatic identity card and the procedure for registration of non-residents exempt from income tax
Published: https://www.riigiteataja.ee/akt/101022022008?leiaKehtiv

[EST EIDTSET ACT] Electronic Identification and Trust Services for Electronic Transactions Act, RT I, 25.10.2016, 1
Published: https://www.riigiteataja.ee/en/eli/527102016001/consolide/current

[EST E-ITS]	Estonian Information Security Standard Published: https://eits.ria.ee
[EST EMERGENCY ACT]	Emergency Act, RT I, 03.03.2017, 1. Published: https://www.riigiteataja.ee/en/eli/ee/505012018004/consolide/current
[EST FEES ACT]	Statutory Fees Act. Published: https://www.riigiteataja.ee/en/eli/ee/519022016005/consolide/current
[EST ID ACT]	Identity Documents Act, RT I 1999, 25, 365 Published: https://www.riigiteataja.ee/en/eli/ee/521062017003/consolide/current
[EST ITDAK REG]	ITDAK Database Regulation Published: https://riigiteataja.ee/akt/122122015045?leiaKehtiv
[EST PDP ACT]	Personal Data Protection Act RT I, 04.01.2019, 11 Published: https://www.riigiteataja.ee/en/eli/523012019001/consolide
[EST PROCIDVERIF REG]	Procedure for identification and verification of the identity of the applicant for a document Published: https://www.riigiteataja.ee/akt/126082022002?leiaKehtiv
[EST VEISDB REG]	VEIS Database Regulation Published: https://www.riigiteataja.ee/akt/118082017002?leiaKehtiv

A.3 ZETES ESTONIA OÜ DOCUMENTS

[ZE CPS-ID1-ROOT-CA]	Zetes Estonia OÜ - Certification Practice Statement for the Root CA for ID-1 Documents of the Republic of Estonia
[ZE CPS-ID1-EID-CA]	Zetes Estonia OÜ - Certification Practice Statement for the Intermediate CA for ID-1 documents of the Republic of Estonia
[ZE PDS-ID1]	Zetes Estonia OÜ – PKI Disclosure Statement for Subscriber Certificates for ID-1 documents of the Republic of Estonia
[ZE PROFILES]	Zetes Estonia OÜ Technical profile of Certificates, OCSP responses and CRLs
[ZE TSPS-ID1]	Zetes Estonia OÜ - Trust Services Practice Statement for the CA-hierarchy for ID-1 Documents of the Republic of Estonia
[ZE TC-ID1-SUB]	Zetes Estonia OÜ- Terms and Conditions and PKI Disclosure Statement for Subscriber Certificates for ID-1 Documents of the Republic of Estonia.
[ZE TC-ID1]	Zetes Estonia OÜ- Terms and Conditions the OCSP, CRL and LDAP services for Certificates for ID-1 Documents of the Republic of Estonia.
[ZE TC-ID1-TEST]	Zetes Estonia OÜ - Terms & Conditions for Test eID Cards

A.4 PBGB DOCUMENTS

[PBGB CP-ID1-EID-CA]	Certificate Policy for ID-1 format identity documents of the Republic of Estonia" (eID CP), OID: 1.3.6.1.4.1.51361.2 (PBGB) and OID: 1.3.6.1.4.1.51455.2 (MFA) Published **:** https://www.id.ee
[PBGB CP-ID1-ROOT-CA]	Certificate Policy for the root Certification Authority of the Republic of Estonia" (Root CP) OID: 1.3.6.1.4.1.51361.3 Published: https://www.id.ee

A.5 ETSI/CEN/CENELEC NORMS

[ETSI TS 119 615]	ETSI TS 119 615 "Trusted Lists; Procedures for using and interpreting European Union Member States national trusted lists"
[ETSI TS 119 172-4]	ETSI TS 119 119 172-4: "Signature policies; Part 4: Signature applicability rules (validation policy) for European qualified electronic signatures/seals using trusted lists"

[ETSI EN 319 401]	ETSI EN 319 401 "General Policy Requirements for Trust Service Providers"
[ETSI EN 319 403]	ETSI EN 319 403 " Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment - Requirements for conformity assessment bodies assessing Trust Service Providers." Published: https://www.etsi.org/
[ETSI EN 319 411-1]	ETSI EN 319 411-1 "Policy and Security Requirements for Trust Service Providers issuing certificates; Part 1: General requirements"
[ETSI EN 319 411-2]	ETSI EN 319 411-2 "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/
[ETSI EN 319 412-1]	ETSI EN 319 412-1 " Certificate Profiles; Part 1: Overview and common data structures" Published: https://www.etsi.org/
[ETSI EN 319 412-2]	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/
[CEN EN 419 211]	CEN EN 419 211 Protection profiles for secure signature creation device. Published: https://www.cencenelec.eu/
[CENELEC EN 50600]	50600-1:2019 Information technology - Data centre facilities and infrastructures Published: https://www.cencenelec.eu/

A.6 ISO/IEC AND NATO NORMS

[ISO 9001]	ISO/IEC 9001 Quality management systems– Requirements Published: https://www.iso.org
[ISO 14001]	ISO/IEC 14001 Environmental management systems Published: https://www.iso.org
[ISO 20000]	ISO/IEC 20000 Information technology — Service management Published: https://www.iso.org
[ISO 27001]	ISO/IEC 27001 Information technology - Security techniques - Information security management systems – Requirements Published: https://www.iso.org
[ISO 17065]	ISO/IEC 17065 Conformity assessment — Requirements for bodies certifying products, processes and services Published: https://www.iso.org
[AQAP 2110]	NATO AQAP 2110 NATO Quality Assurance Requirements for design, development and production Published: https://nso.nato.int

A.7 IETF - RFC

[IETF RFC 3647]	Internet Engineering Task Force RFC 3647 "Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework" Published: https://www.rfc-editor.org/rfc/rfc3647.html
[IETC RFC 5280]	Internet Engineering Task Force RFC 5280 "X.509 Public Key Infrastructure - Certificate and Certificate Revocation List (CRL) Profile" https://www.rfc-editor.org/rfc/rfc5280.html
[IETF RFC 6960]	Internet Engineering Task Force RFC 6960 "X.509 Public Key Infrastructure - Online Certificate Status Protocol – OCSP" Published: https://www.rfc-editor.org/rfc/rfc6960.html

[IETF RFC 5480] Internet Engineering Task Force RFC 5480 “Elliptic Curve Cryptography Subject Public Key Information”
Published: https://www.rfc-editor.org/rfc/rfc5480.html

[IETF RFC 5639] Internet Engineering Task Force RFC 5639 “Elliptic Curve Cryptography (ECC) Brainpool Standard Curves and Curve Generation”
Published: https://www.rfc-editor.org/rfc/rfc5639.html

A.8 PCI SECURITY STANDARDS COUNCIL

[PCI DSS] PCI Data Security Standard for Information Security
Published: https://www.pcisecuritystandards.org/

A.9 NIST

[NIST 186] **NIST** Recommendations for Discrete Logarithm-based Cryptography: Elliptic Curve Domain Parameters | CSRC)
Published: https://csrc.nist.gov/pubs/sp/800/186/final

A.10 ECC

[ECC BP] ECC Brainpool Standard Curves and Curve Generation, v1.0, 19.10.2005 / ECC
Published: http://www.ecc-brainpool.org/ecc-standard.htm

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