Title:	**Zetes Estonia OÜ – Certification Practice Statement for the Intermediate CAs for ID-1 Documents of the Republic of Estonia**
Label:	**[ZE CPS- ID1-EID-CA]**
Document OID:	**[1.3.6.1.4.1.47718.3.11].02**
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	The update brings the CPS in line with the updated eID CP v2.0 document. Condition on the quality check was added for the public key in 6.1.6; Archival period was stated in 6.3.1; Reference to applicable law was added in 9.15; Numbering was corrected at 9.11 onwards; Linguistic corrections were done.
1.3	Updated chapter 9.8. 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. Adaptations after review Cycle. Chapter 4.9.13, added more information on conditions for certificate suspension. Chapter 6.2.1 added a statement that ZE monitors the EU list of QSCD. Updated chapter 9.8.
1.1	For internal use only, no public effect, for pre-production context only. Adaptations after audit. Chapter 1.3.5 and 6.2.1.
1.0	For internal use only, no public effect, for pre-production context only. Approved version for the first phase of the 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 Certification Practice Statement (hereafter CPS) covers the common practices applied by ZE as QTSP for the Intermediate CAs delivering Subscriber Certificates for ID-1 format identity documents of the Republic of Estonia (hereinafter Documents). This CPS adheres to the Certificate Policy (hereafter referred to as [PBGB CP-ID1-EID]) that is defined by the Police and Boarder Guard Board (hereafter PBGB).

This CPS relates to the practices ZE, acting as Certification Authority (CA), employs in issuing Subscriber Certificates.

Two types of Subscriber Certificates for Documents pursuant to the Identity Documents Act [EST ID ACT] are issued and managed by the Intermediate CA:

- NCP+ compliant Subscriber Certificates for authentication and encryption,
- QCP-n-qscd compliance Subscriber Certificates for Qualified Electronic Signatures (hereafter QES),

NCP+ Subscriber Certificates for authentication and encryption shall include the following OIDs:

- 0.4.0.2042.1.2 according to [ETSI EN 319 411-1] clause 5.3 b),
- eID CP OID specified in [PBGB CP-ID1-EID-CA].

QCP-n-qscd Subscriber Certificates for QES shall include the following OIDs:

- 0.4.0.194112.1.2 according to [ETSI EN 319 411-2] clause 5.3 c),
- eID CP OID specified in [PBGB CP-ID1-EID-CA].

The PBGB or the Ministry of Foreign Affairs (MFA) are the issuing authority of Documents in the Republic of Estonia. The PBGB is the issuing authority of the following Documents: identity card, e-resident's digital identity card, residence permit card. The MFA is the issuing authority of diplomatic identity cards.

Pursuant to the IETF RFC 3647 [3], the present CPS document is divided into nine parts. To preserve the outline specified by IETF RFC 3647 [3], clause headings that do not apply have the statement "Not applicable".

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 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 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]	General Policy 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.

The diagram below illustrates the complete CA hierarchy and related services. The elements of the diagram marked in blue are within the scope of this CPS. In the schema below “Intermediate CA” represents the qualified CA that issues the Subscriber Certificates.

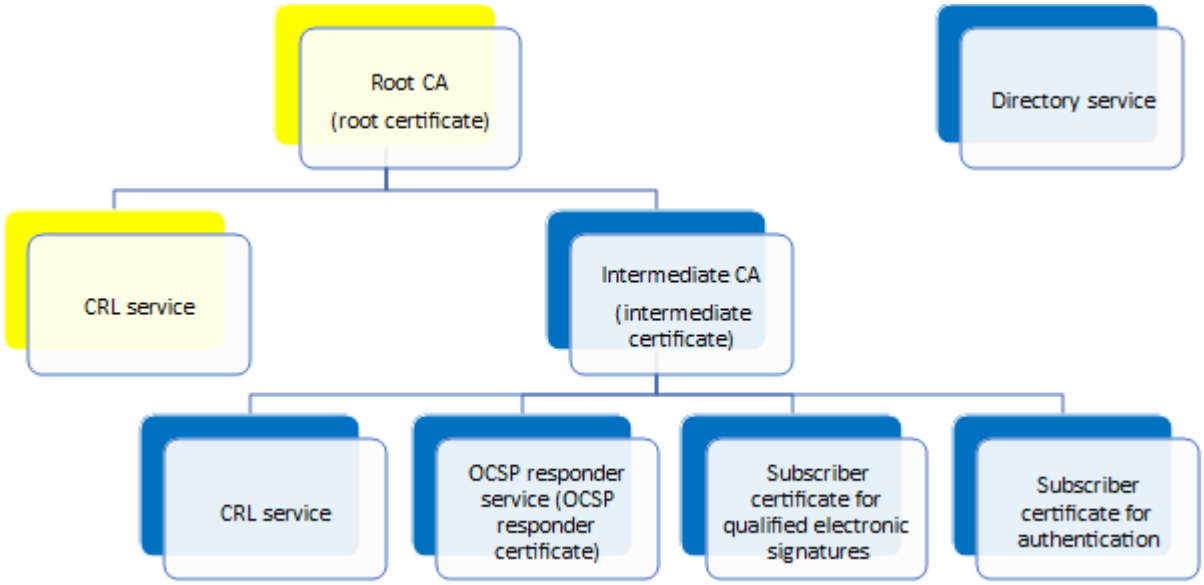

Figure 1. The CA hierarchy and related services for the Republic of Estonia.

The CA hierarchy for the Documents is a 2-level hierarchy comprising a self-signed Root Certification Authority (Root CA) and one or more Intermediate CA issuing Subscriber Certificates for Documents.

The present document pertains to the Intermediate CA for issuing Certificates to citizens, residents and e-residents or diplomatic identity card holders, collectively referred to as the Subscribers.

The Subject's keys and Certificates are stored in a secure chip on the Subject's personal Document. The chip embedded in the Document is a Qualified Signature Creation Device (hereafter QSCD) compliant with the conditions defined in the Commission Implementing Decision [EU 650/2016 QSCD], which sets the standards for the security assessment of QSCD pursuant to [EU 910/2014 EIDAS].

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 CAs issue:

- Subscriber Certificates for Documents
- CRLs for validating the Subscriber Certificates
- Certificates for the OCSP service for validating the Subscriber Certificates

An Intermediate CA shall have a qualified status in accordance with [EU 910/2014 EIDAS] and shall be included in the Trusted List of the Republic of Estonia.

Public Certificate repositories

All 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.

Other documents governing the provision and use of Subscriber Certificates

The certification services rely on a common set of practices described in the ZE Trust Services Practice Statement [ZE TSPS-ID1]. This CPS must be read in conjunction with [ZE TSPS-ID1] and [PBGB CP-ID1-EID-CA]. The declaration of practices in [ZE TSPS-ID1] is endorsed in the present CPS by reference.

1.2 Document name and identification

See the table on the cover page of this document.

In particular, the present document covers Subscriber Certificates issued under the following Certificate Policies:

Certificate Policy OID	Issuer	Document Type	Usage
1.3.6.1.4.1.51361.2.1.1 0.4.0.2042.1.2	PBGB	Identity card of Estonian citizens	Authentication Certificate for authentication, encryption, secure e-mail
1.3.6.1.4.1.51361.2.1.1 0.4.0.194112.1.2	PBGB	Identity card of Estonian citizens	Qualified Electronic Signature Certificate for creating eIDAS compliant Qualified Electronic Signatures
1.3.6.1.4.1.51361.2.1.2 0.4.0.2042.1.2	PBGB	Identity card of European Union citizens	Authentication Certificate for authentication, encryption, secure e-mail
1.3.6.1.4.1.51361.2.1.2 0.4.0.194112.1.2	PBGB	Identity card of European Union citizens	Qualified Electronic Signature Certificate for creating eIDAS compliant Qualified Electronic Signatures
1.3.6.1.4.1.51361.2.1.3 0.4.0.2042.1.2	PBGB	Residence permit card for long-term residents	Authentication Certificate for authentication, encryption, secure e-mail
1.3.6.1.4.1.51361.2.1.3 0.4.0.194112.1.2	PBGB	Residence permit card for long-term residents	Qualified Electronic Signature Certificate for creating eIDAS compliant Qualified Electronic Signatures
1.3.6.1.4.1.51361.2.1.4 0.4.0.2042.1.2	PBGB	Residence permit card for temporary residents	Authentication Certificate for authentication, encryption, secure e-mail
1.3.6.1.4.1.51361.2.1.4 0.4.0.194112.1.2	PBGB	Residence permit card for temporary residents	Qualified Electronic Signature Certificate for creating eIDAS compliant Qualified Electronic Signatures
1.3.6.1.4.1.51361.2.1.5 0.4.0.2042.1.2	PBGB	Residence permit card for family members of EU and UK citizens	Authentication Certificate for authentication, encryption, secure e-mail
1.3.6.1.4.1.51361.2.1.5 0.4.0.194112.1.2	PBGB	Residence permit card for family members of EU and UK citizens	Qualified Electronic Signature Certificate for creating eIDAS compliant Qualified Electronic Signatures
1.3.6.1.4.1.51361.2.1.6 0.4.0.2042.1.2	PBGB	Digital identity card of e-residents	Authentication Certificate for authentication, encryption, secure e-mail
1.3.6.1.4.1.51361.2.1.6 0.4.0.194112.1.2	PBGB	Digital identity card of e-residents	Qualified Electronic Signature Certificate for creating eIDAS compliant Qualified Electronic Signatures
1.3.6.1.4.1.51455.2.1.1 0.4.0.2042.1.2	MFA	Diplomatic identity card	Authentication Certificate for authentication, encryption, secure e-mail
1.3.6.1.4.1.51455.2.1.1 0.4.0.194112.1.2	MFA	Diplomatic identity card	Qualified Electronic Signature Certificate for creating eIDAS compliant Qualified Electronic Signatures

1.3 PKI Participants

1.3.1 Certification Authority (CA)

ZE as the contract partner of the PBGB shall fulfil the role of the CA. The CA shall provide certification and qualified trust services including all the procedures related to the lifecycle of the keys, Certificates and related services described in this CPS and the eID CP [PBGB CP-ID1-EID-CA] exclusively for the Republic of Estonia.

1.3.2 Registration Authorities (RA)

The PBGB shall fulfil the role of RA when identifying Subjects/Subscribers and/or their representatives (if allowed for the type of Document), processing the applications, issuing Documents and revoking Subscriber Certificates (except for diplomatic identity card).

Document hand over of e-resident digital identity card is done by PBGB or delegated to MFA. The list of pick-up points is available at https://www.politsei.ee/en/instructions/e-resident-s-digital-id/pick-up-locations. Subscribers can collect their e-resident's digital identity cards at the PBGB service office, at an Estonian embassy or at any mobile pickup point, which periodically organized by both the PBGB and the MFA.

PBGB outsources certain RA tasks to external service providers who are contract partners of the PBGB. These contract partners shall then fulfil the role of RA for identifying the Subscribers or their representatives (if allowed for the type of Document) and handing over the Documents (except diplomatic identity cards) with the Subscriber Certificates.

PBGB delegates certain RA tasks to the MFA. The MFA fulfil the role of RA for identifying the Subscribers or their representatives (if allowed for the type of Document) and for handing over the Documents (except for diplomatic identity cards) on behalf of the PBGB.

For diplomatic identity cards, the MFA is the sole RA, who identifies the Subscribers, processing the applications, handing over diplomatic identity cards and revoking Subscriber Certificates. For diplomatic identity cards the Subscriber cannot be represented by someone else.

The responsibilities of the RAs are laid down in [EST ID ACT] and [EST EIDTSET ACT]. Transfer of functions listed under [EST ID ACT] clause 3^1 may be applied.

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

The following table summarizes the responsibilities of the RAs:

	All Documents (except diplomatic identity cards)	**Diplomatic identity cards**
Identification of the Subscriber or their representative (if allowed for the type of Document)	PBGB, MFA, external service providers in RA role	MFA
Processing applications for Documents and associated Certificates	PBGB	MFA
Packing and logistics of the Documents	PBGB, MFA, external service providers, Card manufacturer	MFA, external service providers, Card manufacturer
Document, including the security code envelope, handover to the Subscriber or their representative (if allowed for the type of Document)	PBGB, MFA, external service providers in RA role	MFA
Subscriber Certificate activation (change the Certificate state from suspended to active)	Initiated by PBGB Activated by CA	Initiated by MFA Activated by CA
Subscriber Certificate revocation request application	PBGB, Subscriber via Revocation portal	MFA, Subscriber via Revocation portal

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

1.3.3 Subjects and Subscribers

The term **Subject** refers to the person to whom a Certificate is issued and who has the usage rights for the Certificate. The Subject is the natural person whose identity is encoded in the Subject name fields in the Certificate.

The term **Subscriber** refers to the person who subscribes to the Trust Service associated with the Certificate.

A Subject and a Subscriber can only be a natural person entitled by [EST ID ACT] (which refers to the Subscriber as "the document holder"). A person can have only one valid Document of a given Document type at any point of time.

Not every Subject is also the Subscriber. For example, for Certificates issued to an underage child, the child is the Subject and the parent or legal guardian of the child is the Subscriber. For Certificates issued to an adult person with active legal capacity, the person is both Subject and Subscriber. In cases where a Subject is considered not having active legal capacity, the Subscriber is an authorized person with a statutory mandate to represent the Subject.

The following applies:

- Minors younger than 15 years old are Subject, not Subscriber
- Minors from 15 to 17 years old are a Subject but are allowed by [EST ID ACT] to perform the procedural acts provided for in [EST ID ACT] independently, i.e. these minors are considered to be the Subscriber and can apply for Documents and Certificates on their own, ratify [ZE TC-ID1-SUB] on their own, and request revocation of their Certificates on their own.
- Parents and legal guardians can act as Subscriber on behalf of a minor, as defined in [EST FAMILY LAW ACT]
- Adults with full legal capacity are always both Subscriber and Subject
- A person with passive legal capacity or restricted legal capacity, as defined in [EST ADMINPROC ACT] and [EST CIVIL CODE ACT] can only be a Subject

Throughout this document, any reference to term Subject must be interpreted as the person whose identity information is encoded in the Subscriber Certificates. Any reference to the term Subscriber must be interpreted as the person who is entitled and expected to act on behalf of the Subject (themselves or someone else) for the purposes of requesting, revoking and otherwise managing the obligations related to the Subscriber Certificates.

1.3.4 Relying Parties

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

1.3.5 Other Participants

The QSCD is managed by the Card Manufacturer, a private company, under the authority and supervision of PBGB and MFA who are mandated by Estonian law to issue the Documents, including the embedded QSCD. PBGB governs and audits the Card Manufacturer service. PBGB ensures that the Card Manufacturer supplies a certified QSCD that is configured in accordance with the QSCD compliance constraints, that Subscribers keys are generated inside the QSCD and that the QSCD is delivered to the Subscriber in accordance with the requirements stated in [ETSI EN 319 411-2].

The Card Manufacturer is under contract with the PBGB and is responsible for:

- designing, manufacturing and certifying the QSCD;
- configuration of the QSCD;
- generation of key pairs for Subscriber Certificates inside the QSCD;
- generation of the Subscriber Certificates request;
- inserting the Subscriber Certificates in the QSCD.
- physical and logical security in the Document personalisation site;
- packing and logistics of the Documents;
- providing a public portal for viewing PUK;
- providing a public portal for re-keying operations (when needed).

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

The MFA is responsible for allocating a correct and unique e-mail address in the eesti.ee domain for the Subject holding a diplomatic identity card.

The QTSPs uses ICT service companies for hosting, for software development and for ICT configuration services.

1.4 Certificate Usage

1.4.1 Appropriate Certificate uses

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

1.4.2 Prohibited Certificate uses

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

See clause 1.5.1 of [ZE TSPS-ID1].

1.5.2 Contact person

See clause 1.5.2 of [ZE TSPS-ID1].

1.5.3 Person determining suitability for the policy

See clause 1.5.3 of [ZE TSPS-ID1].

1.5.4 Approval procedures

See clause 1.5.4 of [ZE TSPS-ID1].

1.6 Definitions and acronyms

1.6.1 Definitions

Subject	A natural person identified in the Certificate name fields for whom a Certificate is issued.
Subscriber	A natural person who subscribes to the trust service. In the context of this CPS, the Subscriber is to be understood as either the Subject or the Subscriber based on instances of legal guardianship or legal representation, in accordance with Estonian legislation (i.e. the Subscriber and Subject may or may not be the same natural person).
Subscriber Certificate	In the context of this CPS this term is a Certificate issued upon the request of the Subscriber in relation to a Document. Each Document contains two Subscriber Certificates: one for authentication and one for electronic signature.

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

1.6.2 Acronyms

See clause 1.6.2 of [ZE TSPS-ID1].

1.6.3 References

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

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

2 PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 Repositories

2.1.1 Overview

See clause 2.1.1 of [ZE TSPS-ID1].

2.1.2 LDAP Directory Service

See clause 2.1.2 of [ZE TSPS-ID1].

2.1.3 OCSP service

See clause 2.1.3 of [ZE TSPS-ID1].

2.1.4 CRL service

See clause 2.1.4 of [ZE TSPS-ID1].

2.1.5 Test eID Cards service

See clause 2.1.5 of [ZE TSPS-ID1].

2.2 Publication of certification information

2.2.1 Publication and Notification Policies

See clause 2.2.1 of [ZE TSPS-ID1].

The status information for a Certificate is maintained on the CRL until the expiration date of the Certificate. For status information on expired certificates please use OCSP instead.

CRLs will be updated and published until all Certificates in the scope of the CRL are either expired or revoked.

CRL termination occurs

- when there are no more valid Certificates in the scope of the CRL,
- when the CRL's signing entity Certificate is about to expire,
- in case of CA compromise or termination,
- in case of QTSP termination.

In case of CRL termination a last and final CRL shall be published. The nextUpdate field in the last and final CRL is set to "99991231235959Z". The availability of this CRL is ensured from the CRL Distribution Point indicated in the Certificates until at least 1 year after the expiration date of the longest lasting Certificate within scope.

In case Certificate Status can no longer be validated in the standard manner due to CA compromise the QTSP will provide alternative means to obtain Certificate Status information e.g. through a web page and/or a web service. The QTSP does not guarantee interoperability of these alternative means with any third party software.

The QTSP provides an OCSP service. The OCSP service is synchronized with the latest Certificate Status information from the Intermediate CA.

The OCSP service for the Intermediate CA is maintained at least until all Certificates issued by the CA have either expired or have been revoked.

OCSP termination occurs

- when there are no more valid Certificates in the scope of the OCSP,
- when the OCSP's signing entity Certificate is about to expire,

- in case of CA compromise or termination,
- in case of QTSP termination.

In case Certificate Status can no longer be validated in the standard manner due to CA compromise the QTSP will provide alternative means to obtain Certificate Status information e.g. through a web page and/or a web service. The QTSP does not guarantee interoperability of these alternative means with any third party software.

2.2.2 Items not published in the Certification Practice Statement

See clause 2.2.2 of [ZE TSPS-ID1].

2.3 Time or frequency of publication

See clause 2.3 of [ZE TSPS-ID1].

For Subscriber Certificate Status publication via CRL or OCSP see clauses 4.10.7, 4.10.8 and 4.11. The OCSP service is synchronized with the latest status of the Certificates and always provides the most up to date Certificate Status information service.

2.4 Access controls on repositories

See clause 2.4 of [ZE TSPS-ID1].

3 IDENTIFICATION AND AUTHENTICATION

3.1 Naming

3.1.1 Types of names

Type of names and encoding of names for the Subject is described in [ZE PROFILES].

3.1.2 Need for names to be meaningful

The names used in the Certificates are the official given names and surnames of the Subject.

The meaning of the Subject name fields is described in [ZE PROFILES].

3.1.3 Anonymity or pseudonymity of Subjects

Not applicable.

3.1.4 Rules for interpreting various name forms

See clause 3.1.4 of [PBGB CP-ID1-EID-CA].

3.1.5 Uniqueness of names

See clause 3.1.5 of [PBGB CP-ID1-EID-CA].

3.1.6 Recognition, authentication, and role of trademarks

Not applicable.

3.2 Initial identity validation

3.2.1 Method to prove possession of private key

The private keys for the Subject are generated by the Card Manufacturer.

Key generation is done on-board the QSCD.

The QSCD is designed

- to generate key pairs,
- to guard the secrecy of the private key,
- to prevent use of the private key prior to handover,
- to prevent use of the private key without explicit consent of the Subject after handover.

The Card Manufacturer has the necessary controls, procedures and checks in place to ensure that keys are always generated on-board the QSCD and the keys, Documents and Subject data are matched throughout the Document personalization process and the Document re-keying process.

3.2.2 Authentication of organization identity

Not applicable.

3.2.3 Authentication of individual identity

See clause 3.2.3 of [PBGB CP-ID1-EID-CA].

At application and prior to Document handover PBGB and MFA do identification and identity proofing of the Subscriber and/or their representative (if allowed for the type of Document) as prescribed by the official procedure for identification and identity verification in [EST PROCIDVERIF REG] and [EST ID ACT] and exceptions for e-residents in §20^{12} in [EST ID ACT].

For RA contractors PBGB imposes specific requirements for the process of issuing a Document, including identification, set out in the technical description of the contract with the RA contractor.

For the diplomatic identity card, MFA does identification and identity proofing of the Subscriber as prescribed by the official procedure for identification and identity verification in [EST PROCIDVERIF REG], [EST DIPLCARD REG] and in accordance with [EST ID ACT], with specifications for the diplomatic identity card in §20[15] in [EST ID ACT]. Diplomatic identity cards are issued at the MFA in Tallinn and in select embassies.

3.2.4 Non-verified Subject information

The Subscriber Certificates does not contain non-verified Subject information.

3.2.5 Validation of authority

See clause 3.2.5 of [PBGB CP-ID1-EID-CA].

3.2.6 Criteria for interoperation

Not applicable.

3.3 Identification and authentication for re-key requests

3.3.1 Identification and authentication for routine re-key

Counts as re-key:

Re-keying is defined as the creation of a new key pair and the related Certificate to replace an existing key pair for an active Certificate on a QSCD after the QSCD was handed over to the Subscriber.

Re-keying is only allowed for active Certificates. Re-keying is not allowed for a Certificate that has expired or was already revoked before to the re-keying request.

The Card Manufacturer may perform re-key operations only after the Document is handed to the Subscriber and if explicitly authorized by PBGB as part of a controlled and exceptional re-keying campaign for all or a group of Documents. For each Document a re-key is only allowed if the Subject name and identifier fields remained the same.

Re-key for a Document requires that the Subscriber is authenticated by means of the Document itself either in person (physical presence) by an authorized RA operator or online via the re-key portal of the Card Manufacturer. The existing Certificate is revoked when requesting the new Certificate.

The identification and authentication of the Subscriber requesting the re-keying must be done according to the procedures specified by the RA.

Re-key requests are initiated by the RA either in the physical presence of the Subscriber or remotely under condition that the Subscriber was authenticated through the State Authentication Service (TARA) by an authentication means with assurance level “high”. The remote re-key process itself is executed via a re-key portal of the Card Manufacturer.

Key generation for re-keying is also executed on-board the QSCD. Key import into the QSCD is not allowed.

See also clause 3.2.3.

Does not count as re-key:

Creation of a new key pair and the related Certificate to replace an existing key pair for a suspended or permanently revoked Certificate on a QSCD before the QSCD was handed over to the Subscriber, does not count as re-key.

As part of the personalization and delivery process of the Document the Card Manufacturer may generate multiple key instances for one or more Documents before the final Document is handed to the Subscriber, without doing a new identification and authentication of the Subscriber, provided that the Subject name and identifier fields remained the same. The CA ensures that any obsoleted associated Certificates are revoked immediately when a Certificate for the new key is requested.

3.3.2 Identification and authentication for re-key after revocation

See clause 3.3.1 for the identification and authentication for the allowed re-key scenarios.

3.4 Identification and authentication for revocation requests

The person requesting the revocation of Certificates will be identified and authenticated by one of the following duly authorized parties:

- service points operated by PBGB
- the online revocation portal of ZE,
- service points operated by MFA in case of the diplomatic identity card;

For identification and authentication at the service points, see clause 3.2.3.

The online revocation portal of ZE uses TARA for authentication with one of the following recognized Estonian eID means: an identity card, residence permit card, diplomatic identity card, e-resident's digital identity card, Mobile-ID and Smart-ID. TARA identifies and authenticates the Subscriber and links the Subject's identity with – if any - active Document and Certificates.

Authenticated Subscribers can request revocation of their own Certificates or for Certificates of Subjects for which the Subscriber has a statutory mandate or is otherwise legally allowed to represent. The mandate or representation rights are checked and confirmed by the PBGB or in case of the diplomatic identity card, the MFA.

For Subscribers/Subjects who do not dispose of one of the above-mentioned authentication means in TARA, a One-Time Password will be provided through the Subscriber's e-mail address.

4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 Certificate application

4.1.1 Who can submit a Certificate application

See clause 4.1.1 of [PBGB CP-ID1-EID-CA].

Certificate Application is defined as the entire process a Subscriber goes through to apply for Certificates for a Document.

Certificate Application is part of the issuance processes and lifecycle management processes for the Documents. The initiative to apply for a new Document or new Certificates for an existing Document always originates with the Subscriber and is facilitated by the Document issuer and the Card Manufacturer. Subscribers may apply for a new Document on their own initiative or upon invitation of the Document issuer. The actual Certificate request data received by the CA is in all cases generated by and channelled through systems of the PBGB and generated by the Document Issuer and the Card Manufacturer.

A Certificate request is a data set that contains information and instructions for the CA to create a Certificate.

The Card Manufacturer may generate multiple Certificate requests within the scope of a single Certificate Application. Normally only a single request is needed per Document application.

However, if the Document is rejected prior to handover to the Subscriber then multiple requests may occur, e.g. in case of an error during QSCD personalization, a defect or quality problem, the Card Manufacturer may need to generate multiple key instances for a Document and/or may need to replace the Document and generate Certificate Requests for this replacement Document. Therefor multiple request may occur within the scope of issuing a Document with Certificates to a Subject. This scenario is called a “re-print”.

If the Document is rejected at handover to the Subscriber then the Card Manufacturer is authorised to make another Document. Therefor multiple request may occur within the scope of issuing a Document with Certificates to a Subject. This scenario is called a “re-make”.

Subscribers/Subjects can find the most up to date information on the public http://www.politsei.ee website.

For first-time application of a Document and Certificates, Subscribers/Subjects can apply either in a PBGB service point or in an embassy abroad. If the Subject is a minor, for whom a parent or legal guardian acts as the Subscriber, then the first-time application is also allowed via other channels that are normally only allowed for applying for second and following Document and Certificates.

For replacement of a Document (e.g. before expiration, after expiration, lost, stolen, damaged, changes in personal data), Subscribers/Subjects can apply in-person at the PBGB service point or an embassy, via self-service, or in exceptional cases by letter or e-mail.

Subscribers/Subjects are reminded via the Subject’s e-mail address to replace their Document before expiration.

Depending on the Document type, 1 or 2 reminders are sent before expiration of the Document and its Certificates.

For ID-cards and residence permit cards 2 reminders are sent to the Subjects official eesti.ee e-mail address assigned by the Republic of Estonia respectively 60 days and 30 days before expiration of a Document.

For an e-resident card, 1 reminder is sent 90 days before expiration to the e-mail address provided by the Subscriber on their last application.

For diplomatic ID cards, 1 reminder is sent 60 days before expiration to the e-mail address provided by the Subscriber on their last application.

4.1.2 Enrolment process and responsibilities

See clause 4.1.2 of the [PBGB CP-ID1-EID-CA].

See clause 3.3.1.

Subscribers/Subjects cannot apply for Certificates directly from the CA nor submit Certificate request data directly to the CA.

The enrolment process for Certificates is always an integral part of the enrolment process for a Document. The enrolment process is entirely managed by the PBGB or the MFA in their role as RA.

The RAs are responsible for

- the identity proofing process of the Subscribers/Subjects
- the authorization checking process of the Subscribers/Subjects, a.o. whether the Subject is authorized to represent themselves as Subscriber or that another person needs to act as Subscriber
- for defining the type and content of the Certificates.

The processes and checks done by an RA and the responsibilities of the Subscribers/Subjects are described in [EST ID ACT], in the [PBGB CP-ID1-EID-CA] or information otherwise provided to the Subscriber by each RA.

The Card Manufacturer operates under the mandate of the RAs to create the Certificate request data which is sent to the CA through a central system of the PBGB. This central system of the PBGB is the only channel through which the CA receives and processes Certificate creation requests.

The CA considers a Certificate request as implicit evidence that the Subscriber have been vetted and have been lawfully enrolled by the RA and that the Document issuer approved the issuance of Certificates for a specified Document for the Subject.

4.2 Certificate application processing

4.2.1 Performing identification and authentication functions

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

See clause 3.2.3.

For re-keying via the re-key portal of the Card Manufacturer, identification and authentication of the Subscriber is done via TARA.

4.2.2 Approval or rejection of Certificate Applications

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

Certificate Application may be rejected by the CA or by the RA. For the re-key scenario, the Card Manufacturer may reject the Certificate Application in case the Document has already expired or in case a re-key for the Document was not authorized by the RA.

4.2.3 Time to process Certificate Applications

The time to process Certificate Applications may vary by Document type, by the chosen delivery method and delivery location for the Document and by the RAs involved in the process.

PBGB and MFA shall process applications for a Document with Subscriber Certificates within 30 calendar days from the day of the acceptance of the application or the day of the removal of the deficiencies in the application.

Applications for expedited delivery of the Identity card or residence permit card take 2 working days. Subscribers have 6 months to collect the Document from the service points. PBGB and MFA have the right to recover and destroy Documents that are not collected within this period, as stated in [EST ID ACT].

Regular checks are done at all RA locations (embassies, RA service points) for Documents that were not collected and that need to be returned to either PBGB or MFA for destruction, depending on the Document type.

The CA processes Certificate requests immediately. For the Subscriber, the Certificate creation process has no impact on the overall time it takes to complete a Certificate Application procedure.

4.3 Certificate Issuance

4.3.1 CA actions during Certificate issuance

The RA and the Card Manufacturer are collectively responsible for the pertinence, legitimacy, completeness, accuracy and veracity of each Certificate request.

The CA validates the authenticity and integrity of the message contains the Certificate request it receives through X-tee from PBGB and the Card Manufacturer and checks the format and syntax of the data. The CA also checks the uniqueness of the public key for which a Certificate is requested. The CA matches the information in the request with the pre-defined Document types, with pre-existing Subject information if available and the Subject's pre-existing Document(s). The CA checks that the DN is unique, i.e. that the same DN is not already associated with an active or suspended Certificate at the time of the request. The CA checks that the business conditions for issuing the Certificate are met.

If the Certificate can be issued then the CA provides the Certificate through X-tee to PBGB and the Card Manufacturer who stores the Certificate in the designated QSCD in the Document for the Subject as part of the Certificate issuing process for a new Document or as part of the Certificate re-keying process for existing Documents.

4.3.2 Notification to Subscriber by the CA of issuance of Certificate

Certificates are delivered to the Subscriber or their representative (if allowed for the type of Document) on the Document itself as part of the Document issuance process, or the Document re-key process. Subjects will receive an e-mail notification from ZE on their official eesti.ee e-mail address assigned by the Republic of Estonia when the Certificates are activated during the Document handover. The notification e-mail pertains to both Certificates issued for the Subject's Document.

4.4 Certificate acceptance

4.4.1 Conduct constituting Certificate acceptance

When applying for a Document the Subscriber must accept [ZE TC-ID1-SUB] and can register a representative to pick up the Document and the security code envelope. The Subscriber or the registered representative, must confirm receipt and integrity of the Document and the security code envelope, at the time of Document hand over. This confirmation of receiving the Document and the security code envelope, constitutes acceptance of the Subscriber Certificates. At the time of the handover, the Subscriber Certificates can be rejected by rejecting the Document.

Subscribers can at any time request revocation of their Certificates after handover either via the revocation portal of ZE or at a service point of the PBGB or the MFA. In case the Subscriber registered a representative for the pickup, the Subscriber must check the integrity of the security code envelope. If the security code envelope is opened or otherwise tampered with, the Subscriber must request revocation of the Subscriber Certificates and notify the Document issuer, either PBGB or MFA, of the incident.

For Documents issued by PBGB:

For applications submitted via the self-service system, the Subscribers can click a link to show the [ZE TC-ID1-SUB] and must check a box to ratify agreement with [ZE TC-ID1-SUB] in order to complete the application process.

For applications submitted via a paper application form at the service point or via letter, the Subscriber is requested to sign for agreement with the [ZE TC-ID1-SUB].

For applications submitted via e-mail, the Subscriber must sign the digital application with a valid QES for agreement with [ZE TC-ID1-SUB].

After handover of the Document, the Subscribers can request revocation of the Subscriber Certificates either via the revocation portal of ZE or via a service point. The Document itself remains valid even with revoked Subscriber Certificates except for the e-resident identity card.

For Documents issued by MFA:

Applications can only be submitted via a paper application form at the service point or via letter, the Subscriber is requested to sign for agreement with the [ZE TC-ID1-SUB]. Subscribers can request revocation of Subscriber Certificates which in this case also lead to the revocation of the Document.

4.4.2 Publication of the Certificate by the CA

See clause 4.4.2 of [PBGB CP-ID1-EID-CA].

Active authentication Certificates are published in a public LDAP repository, see clause 2 in [ZE TSPS-ID1].

Subscriber Certificates for signature are not published.

4.4.3 Notification of Certificate issuance by the CA to other entities

See clause 4.4.3 of [PBGB CP-ID1-EID-CA].

4.5 Key pair and Certificate usage

4.5.1 Subject private key and certificate usage

The Subscriber must ensure that the Certificates are exclusively used for the purposes as described in clause 6.1.7.

Subscribers who are responsible for a Subject under their care, i.e. parents or legal guardians, are responsible for the correct use of the QSCD issued to a Subject under their care.

Two types of Certificates are issued, each having its specific use. The authentication and encryption Certificate is intended for authentication to online services and for encrypting files or messages and should not be used to create electronic signatures. The Qualified Electronic Signature Certificate is intended to create qualified electronic signatures.

Once the QSCD is handed over, the Subscriber is responsible for correct use of the keys and the Certificates, i.e. the Subscriber must ensure that the QSCD and PIN codes are used in adherence to the intended use as encoded in the Certificates.

The keys are generated by and stored in a QSCD from which the private key cannot be extracted and which ensure sole control of the private keys.

The Subscriber must ensure that the QSCD and the associated PIN code are protected against loss, theft, disclosure, or compromise.

The Subscriber has the following obligations:

- safe and controlled storage of the QSCD
- not share the QSCD with another person
- keep the PIN and PUK codes secret from other people
- choose a non-obvious PIN code
- in case of loss or theft immediately report it to a revocation official (the issuer of the Document or through the online revocation portal)
- refrain from using a QSCD for which the Certificates are expired or have been revoked

4.5.2 Relying Party public key and Certificate usage

The Relying Party must validate a Certificate using at least one of the Certificate Status information services. The Relying Party will trust a Certificate only if it has not been suspended or revoked and may not rely on a Certificate if the Certificate Status cannot be established.

The Relying Party will rely on Certificates only for the purpose as set forth in the present CPS and in the policy information and key usage information encoded in the Certificate itself.

The Relying Party is entirely responsible for the interpretation of the relevance and consequences of the date and time associated with a signature in conjunction with the Certificate Status at the date and time of the creation of the signature and at the date and time of each validation of the signature.

The Relying Party is entirely responsible for the interpretation of the relevance and consequences of the date and time associated with a signature in conjunction with the Certificate expiration date and time versus the date and time of the creation of the signature and at the date and time of each validation of the signature.

The Relying Party will not trust or use a Certificate for authentication purposes or encryption purposes if the Certificate is expired, suspended or revoked.

4.6 Certificate renewal

4.6.1 Circumstance for Certificate renewal

Not applicable.

4.6.2 Who may request renewal

Not applicable.

4.6.3 Processing Certificate renewal requests

Not applicable.

4.6.4 Notification of new Certificate issuance to Subscriber

Not applicable.

4.6.5 Conduct constituting acceptance of a renewal Certificate

Not applicable.

4.6.6 Publication of the renewal Certificate by the CA

Not applicable.

4.6.7 Notification of Certificate issuance by the CA to other entities

Not applicable.

4.7 Certificate re-key

4.7.1 Circumstance for Certificate re-key

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

See clause 3.3.1.

Certificate re-key can originate from the Subscriber or the RA. Re-keying comprises the creation of a new key pair and creation of a new Certificate to replace an existing key pair and Certificate.

Re-key is only possible for Certificates that have already been activated but only in the context of a re-keying operations for all or a group of Documents. Reasons for such re-key operations are to correct errors or security issues with Documents that are already in use. The preceding Certificates are revoked when the new Certificates are requested.

4.7.2 Who may request certification of a new public key

Re-key campaigns are exceptional and are orchestrated by the Document issuer in collaboration with the Card Manufacturer and the QTSP. Subscribers/Subjects will be informed and invited to perform an online re-key process on a re-key portal provided by the Card Manufacturer.

4.7.3 Processing Certificate re-keying requests

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

See clause 3.3.1.

4.7.4 Notification of new Certificate issuance to Subscriber

The Subscriber will be invited to perform the re-key operations either through the re-key portal or at a PBGB or MFA service point. In the re-key portal the Subscriber must authenticate via TARA by means of an eID with assurance level “high” and receives information as to the reason and the impact of the re-key operations.

Subscribers/Subjects can request re-key for their own Subscriber Certificates and for Subscriber Certificates of someone under their legal custody.

The Certificates are issued in active state and the Subjects receive confirmation of the issuance via their official eesti.ee e-mail address assigned by the Republic of Estonia.

4.7.5 Conduct constituting acceptance of a re-keyed Certificate

The act of going to the re-key portal online or to the service point in person combined with the act of accepting [ZE TC-ID1-SUB] by clicking / checking a box or signing a paper form constitutes acceptance of the re-keyed Certificates.

4.7.6 Publication of the re-keyed Certificate by the CA

The re-keyed Certificates are issued directly in active state. Other aspects of publication are as described in clause 4.4.2.

4.7.7 Notification of Certificate issuance by the CA to other entities

The Card Manufacturer receives the Certificate in response to a Certificate request, which is an implicit notification of the issuance of the Certificate.

4.8 Certificate modification

4.8.1 Circumstance for Certificate modification

Not applicable.

4.8.2 Who may request Certificate modification

Not applicable.

4.8.3 Processing Certificate modification requests

Not applicable.

4.8.4 Notification of new Certificate issuance to Subscriber

Not applicable.

4.8.5 Conduct constituting acceptance of modified Certificate

Not applicable.

4.8.6 Publication of the modified Certificate by the CA

Not applicable.

4.8.7 Notification of Certificate issuance by the CA to other entities

Not applicable.

4.9 Certificate revocation and suspension

4.9.1 Circumstances for revocation

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

4.9.2 Who can request revocation

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

4.9.3 Procedure for revocation request

4.9.3.1 Identity card, digital identity card and residence permit card

Certificate revocation is regulated by provisions and procedures for the revocation of identity documents in [EST ID ACT].

A Subscriber may request revocation of their own Certificates or for another person over which they have legal custody. The revocation request must be submitted either in person at a PBGB service point or via the online revocation portal.

At the PBGB service point, the Subscriber is identified by the PBGB service point officer and the revocation request must be signed by the Subscriber. The PBGB service point officer verifies the person filing for revocation in accordance with the PBGB identity verification procedures and also checks the legality to request revocation.

In the online revocation portal, the Subscriber is authenticated electronically using an Estonian eID with assurance level high using TARA. The revocation portal also checks the Ministry of the Interior's Population Registry via an X-tee query whether the Subscriber is also a legal guardian of another person and can revoke the Certificates on behalf of someone else.

Vetted revocation requests are forwarded to the CA via the X-tee secure authenticated channel between PBGB and ZE. The CA authenticates and executes the request automatically and immediately.

Designated governmental authorities within the meaning of [EST ID ACT] must request revocation of Certificates via PBGB.

If a designated governmental authority within the meaning of [EST ID ACT], requests revocation of Certificates, the request must be approved and delivered by PBGB. The CA verifies the authenticity of the request it receives from PBGB.

Each revocation request is processed within 24 hours from receipt. The compliance of the application for revocation with [PBGB CP-ID1-EID-CA] is verified. If the request is accepted it is executed without delay. The Certificate's revoked status will be included in the next CRL (see clause 4.9.7) and is immediately made available on the OCSP service.

For Certificates that were active, the Subscriber receives a formal confirmation of the revocation via the Subject's official e-mail address.

4.9.3.2 Diplomatic identity card

Certificate revocation is regulated by provisions and procedures of revocation of identity document in [EST ID ACT]. Submitted revocation request may require revocation at a future date (e.g. Subscriber's planned cessation from his/her duties at a certain date).

Foreign representation or international organisation submits an application for Diplomatic identity card to MFA service point.

Alternatively, the Subscriber submits a signed application for revocation to MFA service point.

The revocation request is registered by an employee of MFA service point.

If the Subscriber requests revocation of the Certificates, an employee of MFA service point verifies the person filing an application for revocation in accordance with internal identity verification procedures and establishes the legality to request revocation.

If revocation of the Certificates is requested by foreign representation or international organisation, an employee of the MFA service point verifies the legality of the request.

The MFA service point forwards the request for revocation via PBGB to the CA.

4.9.4 Revocation request grace period

The Subscriber is required to request revocation immediately after detecting the loss or theft of the Document or it becoming unusable or any suspicion of compromise of the Document.

4.9.5 Time within which CA must process the revocation request

The time between the validation of the revocation request by the RA and the modification of the Certificate Status will not exceed 24 hours. The CA will process a request without delay upon receipt from the RA.

4.9.6 Revocation checking requirement for relying parties

See clause 4.5.1 and clause 4.5.2.

When using or relying on a Certificate, the Relying Party must first always verify the Certificate Status using at least one of the public Certificate Status information services. Relying Parties that rely on CRLs must take into account the periodicity of the CRL. The Relying Parties must evaluate whether this periodicity is of consequence for them or not.

4.9.7 CRL issuance frequency

The CRL is refreshed at least every 10 hours. At the discretion of the QTSP a CRL may be updated at any time before normal expiration.

4.9.8 Maximum latency for CRLs

The QTSP strives for a delay of less than 10 minutes between the creation of the CRL and its availability to relying parties via the CRL distribution point.

4.9.9 On-line revocation/status checking availability

The OCSP service contains the most up to date Certificate Status information and is available to Relying Parties free of charge and subject to Terms and Conditions, see [ZE TC-ID1].

4.9.10 On-line revocation checking requirements

The OCSP service supports request with and without nonce. The OCSP service supports requests pertaining to a single Certificate. Users of the OCSP service must take into account all the information encoded in the OCSP response, especially in case the requester uses local OCSP caching.

4.9.11 Other forms of revocation advertisements available

Not applicable.

4.9.12 Special requirements regarding key compromise

No stipulations.

4.9.13 Circumstances for suspension

For creating a new Document, the Subscriber Certificates are immediately suspended upon creation and remain suspended until the Certificates are either activated when the Document is handed to the Subscriber and/or their representative, or until the Certificates are revoked when the Document is recovered and destroyed by PBGB or MFA (in case the Document was never collected).

For re-keying an existing Document, Subscriber Certificates are immediately suspended upon creation and remain suspended until the preceding Certificates for the Document are successfully revoked.

No other reasons for suspension are allowed.

4.9.14 Who can request suspension

Only the CA can request suspension.

4.9.15 Procedure for suspension request

Suspension is automatic upon creation of the Subscriber Certificates. No other procedure is allowed.

4.9.16 Limits on suspension period

Subscriber Certificates remain suspended until the Document is either collected by the Subscriber and/or their representative or recovered and destroyed by PBGB or MFA in case the Document was never collected.

The CA does not enforce a limitation on the suspension period.

PBGB will request revocation of the Subscriber Certificate for uncollected Documents.

The CA will automatically revoke Subscriber Certificates for re-print cases and re-make cases.

4.9.17 Circumstances for Termination of Suspension

See clause 4.9.16.

4.9.18 Who can Request Termination of Suspension

See clause 4.9.16.

4.9.19 Procedure for Termination of Suspension

For creating a new Document, only the RAs can request the CA for termination of suspension of the Subscriber Certificates as part of their Document handover process and their Document recovery and destruction process.

For re-keying an existing Document, the CA automatically terminates the suspension if the preceding Certificates for the Document were successfully revoked.

4.10 Certificate Status Services

4.10.1 Operational characteristics

The CRL and OCSP services

The CA provides Certificate Status verification services, including CRLs, OCSP service, and appropriate web interfaces.

CRLs

For maximum interoperability with 3rd party software

- the CRL adheres to the RFC 5280 standard
- the Certificate to be checked contains the URI for the CRL
- the CRL are signed by the CA itself
- the QTSP does not use another trusted authority to sign the CRL
- the CRL files can be downloaded via HTTP and HTTPS

The QTSP will generate a last and final CRL when all the Certificates within the scope of the CRL have either expired or have been revoked. See chapter 2.2.1.

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

Most CRLs are several MB in size. Relying Parties may consider caching CRLs in their own environment for faster processing and for reducing their network traffic.

OCSP service

For maximum interoperability with 3rd party software

- the OCSP format adheres to the RFC 6960 standard.
- the Certificate to be checked contains the URI for the OCSP service (authority information access extension)
- the CA delegates OCSP signing authority to multiple OCSP instances
- the OCSP service supports the use of a nonce in requestExtension
- the OCSP service is available via HTTP and HTTPS
- OCSP requests must include only 1 (one) certificate serial number

Relying Parties who wish to use local caching of OCSP responses for faster processing and for reducing their network traffic cannot use nonces in the OCSP request.

Retention period for Certificate Status Information after expiration for qualified Certificates

Certificate Status information in CRLs and the OCSP service shall be updated at least until all Certificates that were issued by the respective CA have either expired or have been revoked.

The Certificate Status for revoked Subscriber Certificates shall remain in the CRLs until the expiration date of the Certificate.

4.10.2 Service availability

The QTSP operates two active sites to provide a 24/7 service for the automated Certificate Status information services based on CRL and OCSP.

The CRL download service availability level is minimum 99.0% excluding planned maintenance periods.

The OCSP service availability level is 99.0% excluding planned maintenance periods.

The scheduled maintenance tasks shall be planned outside the business hours. In case the scheduled maintenance affects the usage of Documents electronically (OCSP service, CRL service, LDAP directory service, servicing the Subscriber Certificates), it shall be scheduled between 23:00 (EET/EEST) and 07.00 (EET/EEST) next day. A maximum of 2 (two) scheduled maintenance tasks can be scheduled per calendar month. Scheduled maintenance does not necessarily take place on the same days or time slots each month.

Planned maintenance periods that cause an interruption of service will be announced on status.eidpki.ee at least 72 hours in advance and via a notification service.

In case of unavailability due to an act of God, failure of infrastructure outside the control of the QTSP or any other reason, the QTSP shall make best efforts to reinstate availability of the service as soon as possible.

The QTSP cannot be held liable for the availability of any part of the Subscriber's environment or any part of the Relying Party's environment or for the availability of the internet.

4.10.3 Optional features

Not applicable.

4.11 End of subscription

Expiration or revocation of a Certificate effectively ends the subscription for that Certificate.

4.12 Key escrow and key recovery

4.12.1 Key escrow and recovery policy and practices

Not applicable.

4.12.2 Session key encapsulation and recovery policy and practices

Not applicable.

5 FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

This document covers the aspects related to Subject keys and Subscriber Certificates. This chapter is not relevant for the Subject/Subscriber's user environment but is present in this document to maintain conformance with the chapter structure as prescribed by [IETF RFC 3647].

Please refer to corresponding clause in the [ZE TSPS-ID1] for a description of the facilities, management and operational controls applicable to the QTSP PKI components (CA, OCSP service, HSMs and other PKI component services) and for information about the provisions in case of compromise, disaster recovery and termination of all or parts of the QTSP activities.

5.1 Physical controls

Not applicable for the Subject/Subscriber user environment.

For the PKI environment, see the corresponding clause in [ZE TSPS-ID1].

5.1.1 Site location and construction

Not applicable for the Subject/Subscriber user environment.

For the PKI environment, see the corresponding clause in [ZE TSPS-ID1].

5.1.2 Physical access

Not applicable for the Subject/Subscriber user environment.

For the PKI environment, see the corresponding clause in [ZE TSPS-ID1].

5.1.3 Power and air conditioning

Not applicable for the Subject/Subscriber user environment.

For the PKI environment, see the corresponding clause in [ZE TSPS-ID1].

5.1.4 Water exposures

Not applicable for the Subject/Subscriber user environment.

For the PKI environment, see the corresponding clause in [ZE TSPS-ID1].

5.1.5 Fire prevention and protection

Not applicable for the Subject/Subscriber user environment.

For the PKI environment, see the corresponding clause in [ZE TSPS-ID1].

5.1.6 Media storage

Not applicable for the Subject/Subscriber user environment.

For the PKI environment, see the corresponding clause in [ZE TSPS-ID1].

5.1.7 Waste disposal

Not applicable for the Subject/Subscriber user environment.

For the PKI environment, see the corresponding clause in [ZE TSPS-ID1].

5.1.8 Off-site backup

Not applicable for the Subject/Subscriber user environment.

For the PKI environment, see the corresponding clause in [ZE TSPS-ID1].

5.2 Procedural controls

5.2.1 Trusted roles

Not applicable for the Subject/Subscriber user environment.

For the PKI environment, see the corresponding clause in [ZE TSPS-ID1].

5.2.2 Number of persons required per task

Not applicable for the Subject/Subscriber user environment.

For the PKI environment, see the corresponding clause in [ZE TSPS-ID1].

5.2.3 Identification and authentication for each role

Not applicable for the Subject/Subscriber user environment.

For the PKI environment, see the corresponding clause in [ZE TSPS-ID1].

5.2.4 Roles requiring separation of duties

Not applicable for the Subject/Subscriber user environment.

For the PKI environment, see the corresponding clause in [ZE TSPS-ID1].

5.3 Personnel security controls

5.3.1 Qualifications, experience, and clearance requirements

Not applicable for the Subject/Subscriber user environment.

For the PKI environment, see the corresponding clause in [ZE TSPS-ID1].

5.3.2 Background check procedures

Not applicable for the Subject/Subscriber user environment.

For the PKI environment, see the corresponding clause in [ZE TSPS-ID1].

5.3.3 Training requirements

5.3.4 Retraining frequency and requirements

Not applicable for the Subject/Subscriber user environment.

For the PKI environment, see the corresponding clause in [ZE TSPS-ID1].

5.3.5 Job rotation frequency and sequence

Not applicable for the Subject/Subscriber user environment.

For the PKI environment, see the corresponding clause in [ZE TSPS-ID1].

5.3.6 Sanctions for unauthorized actions

Not applicable for the Subject/Subscriber user environment.

For the PKI environment, see the corresponding clause in [ZE TSPS-ID1].

5.3.7 Independent contractor requirements

Not applicable for the Subject/Subscriber user environment.

For the PKI environment, see the corresponding clause in [ZE TSPS-ID1].

5.3.8 Documentation supplied to personnel

Not applicable for the Subject/Subscriber user environment.

For the PKI environment, see the corresponding clause in [ZE TSPS-ID1].

5.4 Audit logging procedures

5.4.1 Types of events recorded

Not applicable for the Subject/Subscriber user environment.

For the PKI environment, see the corresponding clause in [ZE TSPS-ID1].

5.4.2 Frequency of processing log

Not applicable for the Subject/Subscriber user environment.

For the PKI environment, see the corresponding clause in [ZE TSPS-ID1].

5.4.3 Retention period for audit log

Not applicable for the Subject/Subscriber user environment.

For the PKI environment, see the corresponding clause in [ZE TSPS-ID1].

5.4.4 Protection of audit log

Not applicable for the Subject/Subscriber user environment.

For the PKI environment, see the corresponding clause in [ZE TSPS-ID1].

5.4.5 Audit log backup procedures

Not applicable for the Subject/Subscriber user environment.

For the PKI environment, see the corresponding clause in [ZE TSPS-ID1].

5.4.6 Audit collection system (internal vs. external)

Not applicable for the Subject/Subscriber user environment.

For the PKI environment, see the corresponding clause in [ZE TSPS-ID1].

5.4.7 Notification to event-causing Subject

Not applicable for the Subject/Subscriber user environment.

For the PKI environment, see the corresponding clause in [ZE TSPS-ID1].

5.4.8 Vulnerability assessments

Not applicable for the Subject/Subscriber user environment.

For the PKI environment, see the corresponding clause in [ZE TSPS-ID1].

5.5 Records archival

5.5.1 Types of records archived

Not applicable for the Subject/Subscriber user environment.

For the PKI environment, see the corresponding clause in [ZE TSPS-ID1].

5.5.2 Retention period for archive

Not applicable for the Subject/Subscriber user environment.

For the PKI environment, see the corresponding clause in [ZE TSPS-ID1].

5.5.3 Protection of archives

Not applicable for the Subject/Subscriber user environment.

For the PKI environment, see the corresponding clause in [ZE TSPS-ID1].

5.5.4 Archive backup procedures

Not applicable for the Subject/Subscriber user environment.

For the PKI environment, see the corresponding clause in [ZE TSPS-ID1].

5.5.5 Requirements for time-stamping of records

Not applicable for the Subject/Subscriber user environment.

For the PKI environment, see the corresponding clause in [ZE TSPS-ID1].

5.5.6 Archive collection system

Not applicable for the Subject/Subscriber user environment.

For the PKI environment, see the corresponding clause in [ZE TSPS-ID1].

5.5.7 Procedures to obtain and verify archive information

Not applicable for the Subject/Subscriber user environment.

For the PKI environment, see the corresponding clause in [ZE TSPS-ID1].

5.6 Key changeover

Not applicable for the Subject/Subscriber user environment.

For the PKI environment, see the corresponding clause in [ZE TSPS-ID1].

5.7 Compromise and disaster recovery

5.7.1 Incident and compromise handling procedures

Not applicable for the Subject/Subscriber user environment.

For the PKI environment, see the corresponding clause in [ZE TSPS-ID1].

5.7.2 Computing resources, software and/or data are corrupted

Not applicable for the Subject/Subscriber user environment.

For the PKI environment, see the corresponding clause in [ZE TSPS-ID1].

5.7.3 Entity private key compromise procedures

Not applicable for the Subject/Subscriber user environment.

For the PKI environment, see the corresponding clause in [ZE TSPS-ID1].

5.7.4 Business continuity capabilities after a disaster

Not applicable for the Subject/Subscriber user environment.

For the PKI environment, see the corresponding clause in [ZE TSPS-ID1].

5.8 CA or RA Termination

Not applicable for the Subject/Subscriber user environment.

For the PKI environment, see the corresponding clause in [ZE TSPS-ID1].

6 TECHNICAL SECURITY CONTROLS

This document covers the aspects related to Subject keys and Subscriber Certificates.

Please refer to corresponding clause in [ZE TSPS-ID1] for a description of the technical security controls applicable to the QTSP PKI components (CA, OCSP service, HSMs and other PKI component services)

6.1 Key pair generation and installation

6.1.1 Key pair generation

The key pairs for Certificates are generated by the Card Manufacturer on board the QSCD chip of the Document, in one of two controlled environments:

1. the personalisation site operated by the Card Manufacturer
2. the re-key portal operated by the Card Manufacturer.

The QSCD chip has integrated access control, device lifecycle management and key lifecycle management under the exclusive control of the Card Manufacturer. The processes for key pair generation, public key extraction and installation of a Certificate can only be initiated under control of the Card Manufacturer on request of and/or authorized by PBGB and MFA.

6.1.2 Private key delivery to Subscriber

The Subject receives the private key and public key (in the form of a Certificate) pre-installed on a new Document or generated anew on the Subject's existing Document during a re-key process. In both cases key delivery process is controlled by the Card Manufacturer and the RA.

Delivery of the key and the public key Certificate is part of an initial key generation process or of a re-key process.

For a new Document, the key is generated on the QSCD chip as part of the Document personalization process in the Personalisation Site of the Card Manufacturer. Delivery of the key coincides with the physical delivery of the Document to the Subscriber or their representative. This is the typical scenario for the majority of Documents that are delivered through the RAs including PBGB contract partners.

For the re-key process via the re-key portal of the Card Manufacturer, the private key is generated on the QSCD chip as part of the re-key process, using the Subscriber's own computer or on a designated computer system in a service point.

6.1.3 Public key delivery to Certificate issuer

The CA receives the public key from the Card Manufacturer through the government-operated X-tee data exchange system of the Republic of Estonia.

6.1.4 CA public key delivery to Relying Parties

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

6.1.5 Key sizes

See the applicable Certificate Profiles [ZE PROFILES].

6.1.6 Public key parameters generation and quality checking

The quality of public keys is guaranteed by generating the keys on the QSCD chip. The QSCD chip is certified device and the certification scope includes the chip's built-in random number generator of the chip and key generation algorithms.

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

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

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

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic module standards and controls

QSCD list

The cryptographic module of the Document is officially notified as a QSCD and as such listed on the European Commission compilation of QSCD devices which can be consulted at the following URL: https://eidas.ec.europa.eu/efda/browse/notification/qscd-sscd.

List of QSCD used:

QSCD Operating system: MultiApp V5.1

- CC Certificate (ANSSI-CC-2023/31)
  https://commoncriteriaportal.org/nfs/ccpfiles/files/epfiles/ANSSI-CC-2023_31fr.pdf
- CC Certification report (ANSSI-CC-2023/31
  https://commoncriteriaportal.org/nfs/ccpfiles/files/epfiles/ANSSI-CC-2023_31fr.pdf
- CC Maintenance report (ANSSI-CC-2023/31-M01)
  https://commoncriteriaportal.org/nfs/ccpfiles/files/epfiles/ANSSI-CC-2023_31-M01fr.pdf

QSCD application: IAS Classic V5.2.1 with MOC Server v3.1 (version 5.2.1.A.O)

- CC Certificate (ANSSI-CC-2023/42
  https://commoncriteriaportal.org/nfs/ccpfiles/files/epfiles/Certificat-CC-2023_42fr.pdf
- CC Certification report (ANSSI-CC-2023/42
  https://commoncriteriaportal.org/nfs/ccpfiles/files/epfiles/ANSSI-CC-2023_42fr.pdf
- CC Maintenance report (ANSSI-CC-2023/42-M01)
  https://commoncriteriaportal.org/nfs/ccpfiles/files/epfiles/ANSSI-CC-2023_42-M01fr.pdf

The QSCD is a device that is embedded in Documents issued by the Republic of Estonia. The processes for Certificate issuance and Certificate activation are integrated into the processes for issuing the Documents.

The Card Manufacturer under contract with PBGB is responsible for the certification, the security surveillance and re-certification of the QSCD. The Card Manufacturer informs PBGB as soon as planned changes that effect the technical use or the certification status of the QSCD are known. The Card Manufacturer is obligated to inform PBGB immediately in case of any unforeseen (potential) change or issue regarding the security, reliability, usability or certification status of the QSCD. PBGB is responsible for monitoring the certification status of the QSCD with the Card Manufacturer and for ensuring that all use of the QSCD meets the conditions of the QSCD certifications. PBGB informs the QTSP in full and without delay.

ZE as QTSP will monitor the QSCD certificate status using the list of QSCD that is published by the European Commission.

The QTSP will decide on the appropriate action in response to the information available and that state of affairs in case a change (potentially) impacts Subscriber Certificates. The QTSP will select the appropriate measures and the timing of those measures depending on the situation at hand.

The QTSP can take any combination of the following actions:

- Revocation of Certificates
- Pause creation of new Certificates
- Pause activation of Certificates at Document handover
- Delayed activation of Certificates after Document handover
- Re-key and issuance of new Certificates
- Continue operations without change

Communication on the status of the QSCD and the impact on Subscriber Certificates to Subscribers, Relying Parties or the Supervisory Body will be coordinated with PBGB and MFA.

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

Not applicable. The QSCD private keys of the Document are exclusively assigned to the Subject. Only the Subject is entitled to use the private key and has sole control over the private key by means of a personal PIN code.

6.2.3 Private key escrow

Not applicable. The private key cannot be extracted from the QSCD.

6.2.4 Private key backup

Not applicable. The Card Manufacture's product and personalisation procedure ensures that the private key cannot be extracted from the QSCD.

6.2.5 Private key archival

Not applicable. The Card Manufacture's product and personalisation procedure ensures that the private key cannot be extracted from the QSCD.

6.2.6 Private key transfer into or from a cryptographic module

The private key is generated on the QSCD by the Card Manufacturer. The private key cannot be extracted from the QSCD.

6.2.7 Private key storage on cryptographic module

The private key is generated on the QSCD, cannot be extracted from the QSCD and can only be used for cryptographic operations inside the QSCD. Private keys are stored in dedicated key containers on the QSCD, the key containers are protected against logical and physical attacks to extract keys. The protection mechanism has been evaluated as part of the QSCD's Common Criteria certification.

6.2.8 Method of activating private keys

The Subject activates a private key by means of a PIN code.

PIN1 (authentication PIN) protects the usage of authentication key. PIN1 is also required for a re-key operation. The private key intended for authentication and encryption purposes can be used multiple times without requiring repeated PIN entry. This is deliberate for user convenience and compatibility with how popular browsers handle TLS client authentication.

PIN2 (signature PIN) protects the usage of signature key and dedicated only for that purpose. The private key intended for QES purposes can be used for a single cryptographic operation per PIN entry. The private keys do not have a usage limit counter.

The Subject can change PIN1 and PIN2 values e.g. using the DigiDoc application. To change a PIN, it is required to enter the correct current value of the corresponding PIN.

The PUK (PIN unblocking key) is used to unblock PIN1/PIN2 codes when these were locked after 3 unsuccessful PIN verifications. The PUK value cannot be changed. The PUK itself will also be locked after 3 unsuccessful PUK verifications. Once locked the PUK cannot be unlocked and the Document will have to be replaced.

6.2.9 Method of deactivating private key

The private key is deactivated when

- the Document is pulled out of the reader,
- the QSCD chip is powered down,
- application software or driver software deliberately deactivates the key.

For the QES key, the key is automatically deactivated after each signature operation. In case the contactless interface is used, the key is deactivated also if the PIN entry is followed by any non-authorized command sequence.

6.2.10 Method of destroying private key

The QSCD is in the hands of the Subject. Destruction of the private key after its designated usage period can therefore not be guaranteed. Key destruction can only be done when the Document is used in a re-key operation (by overwriting the original key object in the QSCD) or when the QSCD is physically destroyed, either by the Subject or by the PBGB or MFA when uncollected cards are recovered and destroyed.

6.2.11 Cryptographic Module Rating

The QSCD meets the requirements laid down in the European standards for QSCD at the time of certification.

See [ZE PROFILES] for the actual key types and key lengths that are used.

6.3 Other aspects of key pair management

6.3.1 Public key archival

The QTSP does not maintain a dedicated archive of all public keys. Public keys are only stored as part of the Certificates that are kept in the database of the CA. Retention period shall be in accordance with [EU 910/2014 EIDAS], [EST EUTS ACT] and applicable standards.

The Card Manufacturer deletes the public keys no later than five days after personalization of a Document.

6.3.2 Certificate operational periods and key pair usage periods

The key usage period is presumed to equal the Certificate usage period which may be shorter than the original Certificate expiration date due to early revocation of the Certificate. See [ZE PROFILES] for the applied Certificate operational periods. The key pair usage period may or may not be explicitly mentioned in the Certificates.

6.4 Activation data

6.4.1 Activation data generation and installation

The activation data in the form of 2 PIN codes and a PUK code is provided to the Subject in a tamper-evident PIN/PUK-letter (also called the security code envelope).

The Document, together with the security code envelope, is delivered to the Subscriber through the RAs, including contract partners of the PBGB in a RA role.

The Subject can change the PIN codes or unblock the PIN codes using the PUK code by means of the DigiDoc software provided by the Information System Authority (RIA) which is available to all Subjects without limitation and at no charge.

In case the Subject has lost the PUK code, the Subscriber can apply in person at a PBGB service points for the existing PUK code or the Subject can connect to the portal of the Card Manufacturer after strong authentication through other accepted electronic identification means to view the PUK code.

If the PUK code is blocked then the Subscriber can apply for a new Document.

6.4.2 Activation data protection

The activation data is delivered in the form of printed PIN and PUK codes in a tamper-evident PIN/PUK-letter. Attempts to open the PIN/PUK-letter leaves visible physical signs. The PIN/PUK-letter has „tear parts“ on 3 sides and all three must be fully opened to see the PIN/PUK, i.e. it is clearly visible to the Subscriber or their representative (if allowed for the type of Document) and to the officer at the service point if a PIN/PUK-letter was (partially) opened or tampered with.

PIN/PUK-letters are printed with a regular office printer which is connected to secure pressure seal folding device. Printing is managed through the Card Manufacturer personalization system. Operator check the integrity of the sealed PIN/PUK-letter before shipping. The PIN/PUK-letters are put in a tamper evident sealed package and delivered to PBGB or MFA via a secure courier.

Assigned officers of the PBGB and MFA are instructed to check if the PIN/PUK-letters have been properly closed, have any signs of tampering before handing them out.

The Subscriber or their representative (if allowed for the type of Document) has also been informed to check the integrity of the PIN/PUK-letter. The Subscriber or their representative (if allowed for the type of Document) must sign a form to confirm that the PIN/PUK-letter was intact or must reject the Document in case the PIN/PUK-letter was tampered with.

The Subject is encouraged to change the PIN at home using the Digidoc software on their personal computer.

6.4.3 Other aspects of activation data

No stipulations.

6.5 Computer security controls

6.5.1 Specific computer security technical requirements

The Subscriber is responsible to ensure that the environment in which the private keys will be used is deemed trustworthy, secure and fit for purpose.

6.5.2 Computer security rating

No stipulations.

6.6 Life cycle technical controls

6.6.1 System development controls

No stipulations.

6.6.2 Security management controls

The Subscriber is responsible to keep the operating system software, anti-virus software, network security software and DigiDoc software on every device used to interface with the Document up to date.

The Subscriber is responsible to ensure that the environment and the computing device which the Document will interface with is deemed trustworthy, secure and fit for purpose. If in doubt, the Subject should not interface the Document with the computing device.

6.6.3 Life cycle security controls

No stipulations.

6.7 Network security controls

The Subscriber is responsible for applying reasonable protection on the device where the private keys are used. The Subject is recommended to use firewall software on every device used to interface with the Document.

6.8 Time-Stamping

The Subscriber is responsible for setting the correct date and time on the device where the private keys are used. The Subscriber is recommended to configure the operating system of the device to use a public UTC time source to ensure that the device's time is accurate.

7 CERTIFICATE, CRL AND OCSP PROFILES

For internal test and validation purposes the QTSP may issue certificates with a special Policy OID-prefix 2.999 and special content in the Subject and Issuer name fields.

7.1 Certificate profile

See the corresponding section in the Certificate Profiles [ZE PROFILES].

7.2 CRL profile

See the corresponding section in the Certificate Profiles [ZE PROFILES].

7.3 OCSP profile

See the corresponding section in the Certificate Profiles [ZE PROFILES].

8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS

This document covers the aspects related to Subscriber context. Compliance audits and other assessments are not applicable to the Subscriber. Please refer to corresponding clause in [ZE TSPS-ID1] for a description of the compliance audits and other assessments that are applicable to the QTSP.

8.1 Frequency or Circumstances of Assessment

Not applicable for the Subject/Subscriber user environment.

For the PKI environment, see the corresponding clause in [ZE TSPS-ID1].

8.2 Identity/qualifications of assessor

Not applicable for the Subject/Subscriber user environment.

For the PKI environment, see the corresponding clause in [ZE TSPS-ID1].

8.3 Assessor's relationship to assessed entity

Not applicable for the Subject/Subscriber user environment.

For the PKI environment, see the corresponding clause in [ZE TSPS-ID1].

8.4 Topics covered by assessment

Not applicable for the Subject/Subscriber user environment.

For the PKI environment, see the corresponding clause in [ZE TSPS-ID1].

8.5 Actions taken as a result of deficiency

Not applicable for the Subject/Subscriber user environment.

For the PKI environment, see the corresponding clause in [ZE TSPS-ID1].

8.6 Communication of results

Not applicable for the Subject/Subscriber user environment.

For the PKI environment, see the corresponding clause in [ZE TSPS-ID1].

9 OTHER BUSINESS AND LEGAL MATTERS

Chapter 9 in this CPS covers all aspects regarding the issuance of Certificates for Documents. The corresponding chapter in [ZE CPS-ID1-ROOT-CA] and in [ZE TSPS-ID1] therefor contain no stipulations and instead refer to this CPS.

9.1 Fees

9.1.1 Certificate Issuance or Renewal Fees

The fee for the Subscriber Certificates issuance is included in the fee for the review of a Document application, in accordance with the [EST FEES ACT]. The fee for the issuance of the Subscriber Certificates for the diplomatic identity card is covered by the MFA as agreed in the mutual agreement between the MFA and the PBGB. The use of the Subscriber Certificates and the CA-hierarchy Certificates are free of charge.

9.1.2 Certificate Access Fees

The use of the public LDAP service for Subscriber Certificates for authentication and encryption as well as the CA Certificate repository service is free of charge.

In case of misuse or abuse of a service by a Subscriber, a Relying Party or any other party, the QTSP has the duty to take measures to ensure the availability, integrity and responsiveness of the service for other users, either by (temporarily) denying access or (temporarily) limiting the rate of usage for said party.

The QTSP may at its discretion come to commercial agreement with said party in case the party's needs are not met within the standard public service levels of the service.

9.1.3 Revocation or Status Information Access Fees

Revocation of the Subscriber certificates is free of charge. The CRL service and the OCSP service are free of charge.

In case of misuse or abuse of a service by a Subscriber, a Relying Party or any other party, the QTSP has the duty to take measures to ensure the availability, integrity and responsiveness of the service for other users, either by (temporarily) denying access or (temporarily) limiting the rate of usage for said party.

The QTSP may at its discretion come to a commercial agreement with said party in case the party's needs are not met within the standard public service levels of the service.

9.1.4 Fees for other services

The public documents repository service is free of charge.

In case of misuse or abuse of the service by a Subscriber, a Relying Party or any other party, the QTSP has the duty to take measures to ensure the availability, integrity and responsiveness of the service for other users, either by (temporarily) denying access or (temporarily) limiting the rate of usage for said party.

The QTSP may at its discretion come to a commercial agreement with said party in case the party's needs are not met within the standard public service levels of the service.

9.1.5 Refund Policy

The Subscriber is entitled to apply for a refund of the state fee or the review of the Document application in accordance with [EST FEES ACT].

9.2 Financial responsibility

9.2.1 Insurance coverage

The QTSP has a liability insurance as required by Article 13 and Article 24 of [EU 910/2014 EIDAS] and by [EST EUTS ACT]. The QTSP maintains adequate resources and insurance coverage to meet its obligations regarding the provision, use and continuity of its services. ZE publishes the terms of the compulsory insurance policy on the CA repository website.

9.2.2 Other assets

No stipulations.

9.2.3 Insurance or warranty coverage for end-entities

No stipulations.

9.3 Confidentiality of business information

9.3.1 Scope of confidential information

All information that has become known while providing services and that is not intended for publication (e.g. information that had been known to ZE because of operating and providing Trust Services) is confidential. Subscriber has a right to get information from ZE about him/herself according to legal acts.

9.3.2 Information not within the scope of confidential information

The following information is public information and non-confidential:

- Overview of the PKI hierarchy
- Trust Services Practice Statement
- Certification Practice Statements
- Audit results made public on the website
- Conditions for insurance policy
- Root CA Certificates and Intermediate CA Certificates in the CA Certificate repository service
- Subscriber Certificates for authentication in the LDAP directory service
- Certificate Revocation Lists and OCSP responses
- Certificate Profiles
- Terms and Conditions for the use of OCSP service, CRL, LDAP and the documentation repository [ZE TC-ID1]
- Subscriber Agreement and Terms and Conditions
- Privacy Policy including personal data processing principles

Additionally, non-personalised statistical data about ZE's services is also considered public information. ZE may publish non-personalised statistical data about its services.

9.3.3 Responsibility to protect confidential information

Parties that are granted access to confidential information are granted permission on the condition that they use it for the requested purposes, protect it from compromise, and refrain from using it or disclosing it to third parties. These parties are bound to observe personal data privacy rules in accordance with the law.

9.4 Privacy of personal information

9.4.1 Privacy plan

The QTSP does not release nor is it required to release any confidential information without an authenticated and justified request.

The QTSP shall:

- where it processes personal data do so in line with the [EU 679/2016 GDPR] and the [EST EIDTSET ACT], as they refer to the data processor.
- treat all personal data as confidential, unless the Subscriber determines otherwise;

- take adequate technical and organisational measures as a data processor ensuring the security of the processing of personal data in line with the [EU 679/2016 GDPR] and the [EST EIDTSET ACT];

The QTSP warrants that:

- the technical and organisational measures offer an appropriate level of protection in proportion to the risks involved against the accidental or unauthorised destruction, loss, alteration or access to personal data or any other form of unauthorised processing of personal data;
- its personnel shall only have access to personal data insofar the access is necessary for performing their duties;
- its personnel charged with the processing of personal data have been duly informed of the applicable obligations under the [EST PDP ACT] and their obligations under this clause.

9.4.2 Information treated as private

Personal data encoded in the Certificate is deemed private information whilst being processed by the QTSP, the RAs and their contractors in the RA role and the Card Manufacturer. However, the Certificates are intended for public exposure either as part of a signature data structure, as part of an authentication data structure or by virtue of being published in the public LDAP directory for encryption purposes. OCSP usage information pertaining to a Subscriber Certificate is deemed private information.

9.4.3 Information not deemed private

Certificates published in the LDAP service and their visible content is not deemed private.

Certificate Status information published via the CRL service and the OCSP service is not deemed private.

9.4.4 Responsibility to protect private information

See clause 9.4.1.

9.4.5 Notice and consent to use private information

During the Certificate Application process the Subscriber is presented the Subscriber Agreement and Terms & Conditions [ZE TC-ID1-SUB] as notice and the Subscriber expresses consent regarding the use of their private information by opting to include Certificates on the Document, in accordance the [EU 679/2016 GDPR], the [EST ID ACT] and the [EST EIDTSET ACT].

9.4.6 Disclosure pursuant to judicial or administrative process

Information may be disclosed in the course of any judicial or administrative proceeding.

9.4.7 Other information disclosure circumstances

The QTSP is under no obligation to disclose information other than is provided for by a legitimate and lawful judicial order.

9.5 Intellectual property rights

The QTSP owns and reserves all intellectual property rights associated with its own databases, web sites, software, the CA Certificates and any other publication whatsoever originating from the QTSP.

Intellectual property rights in documentation created by or on behalf of the QTSP specifically for the performance of the provision of the qualified trust service in the Republic of Estonia, are transferred to the benefit of the Republic of Estonia or when not transferable the works are made available under license, including the unlimited right to create derivative works based on the work.

9.6 Representations and warranties

9.6.1 CA representations and warranties

To the extent specified in the relevant CPS, the QTSP shall:

- Comply with the Practice Statements as published in the CA's Repository;
- Provide infrastructure and certification services, including the establishment and operation of the CA's Repository and web site for the operation of public certification services;
- Provide Trust mechanisms, including a key generation mechanism, key protection, and secret sharing procedures regarding its own infrastructure;
- Promptly notify the PBGB in case of compromise of its own private key(s);
- Issue Certificates in accordance with this CPS and fulfil its obligations presented herein;
- Publish CRLs and OCSP responses of all suspended and revoked Certificates on a regular basis;
- Comply with [EU 910/2014 EIDAS] and the relevant legislation of the Republic of Estonia.

If the CA becomes aware of or suspects a key compromise, it will immediately notify the PBGB and the Supervisory Body.

When using third party agents, the CA will make best efforts to ensure the proper financial responsibility and liability of such contractor.

The CA is responsible towards Subscribers for the following acts or omissions:

- Issue Certificates with data not corresponding to the data submitted by the RA;
- If a private signing key of the CA is compromised;
- Failure to include revoked or suspended Certificates in a CRL at the time of its creation;
- Incorrect response in the answer of the OCSP to report a Certificate as revoked or suspended;
- Unauthorised disclosure of confidential information or personal data.

The employees of ZE that are relevant to the Trust Services shall not have a valid criminal record for an intentionally committed criminal offence..

ZE has documented agreements and contracts with its subcontracting and outsourcing parties provisioning services. ZE has defined in these agreements and contracts the liability, relevant requirements and right to audit subcontracting and outsourcing parties to be ensured that they are bound to implement any requirements and controls required by ZE.

In accordance with the relevant legislation, ZE does its best to guarantee that all potential service users, especially people with disabilities, can access services provided by ZE on an equal basis. ZE accepts that its services imply at least some sort of qualitative capabilities and legal capacity, but nonetheless truly aspires to provide trust services and related technical solutions in a non-discriminating way.

The warranties delivered by the QTSP are made considering that the QTSP is not responsible for the production, security, transport, secure transfer of data and delivery to the Subjects of the Cards or the chips embedded in the Cards. No responsibility related to these items will be borne by the QTSP.

It is the sole responsibility of the parties accessing information featured in the CA's Repository and web site to assess and rely on information featured therein.

9.6.2 RA representations and warranties

In addition to elsewhere stated in this CPS, the RA will:

- Provide correct and accurate information in their communication with the CA;
- Control the Card Manufacturer to ensure that the public key submitted to the CA by the Card Manufacturer corresponds to the private key generated on the Document
- Control the data exchange between the Card Manufacturer and the CA a.o. for Certificate Requests and Revocation Requests;

- Create Certificate requests through the Card Manufacturer in accordance with the applicable Practice Statement;
- Perform all verification and authenticity actions prescribed by the CA procedures and the applicable Practice Statement;
- Receive, verify and relay to the CA all requests for Certificate Status change of a Certificate in accordance with the CA procedures and the present document;
- Verify the accuracy and authenticity of the information provided by the Subscriber.

According to section 6.1.2 of the [PBGB CP-ID1-EID] and this CPS, the Card Manufacturer and the RA are responsible for the secure storage and logistics of the Document (including its private key) prior issuance and until handover of the Document to the Subscriber or their representative. If the RA becomes aware of or suspects the compromise of a Subject's private keys, it will immediately request revocation of the associated Certificates.

An employee of the RA (including employees of external service providers in a RA role), shall not have been convicted of an intentional crime.

9.6.3 Subscriber representations and warranties

In addition to elsewhere stated in this CPS, the Subscriber's obligations include the following:

- the Subscriber adheres to the requirements provided by ZE in this CPS, the Subscriber Agreement including the Terms and Conditions;
- the Subscriber presents true and correct information to RA while applying for the Document;
- in case of a change of the Subject's name and/or personal code, the Subscriber must notify within one month the RA of the correct details in accordance with the established legislation;
- the Subject uses the private keys solely for the intended purpose as indicated in the Subscriber Certificates;
- the Subject uses the private keys and corresponding Subscriber Certificates solely on a secure cryptographic device integrated in the Document, in the manner prescribed by ZE;
- the Subject uses the private key in accordance with the present document;
- the Subject immediately informs the RA of any suspicion or possibility of unauthorised use of the private key and requests revocation of the Subscriber Certificates;
- the Subscriber immediately requests revocation of the Subscriber Certificates as soon as the Document is stolen, damaged, missing or otherwise no longer under the control of the Subscriber;
- the Subject no longer uses the private keys after the Subscriber Certificates expiration date or after revocation of the Subscriber Certificates or after revocation of the Root CA Certificate and/or the Intermediate CA Certificate;
- the Subscriber is aware that Qualified Electronic Signatures given on the basis of expired, revoked or suspended Certificates are invalid;
- The Subscriber is aware that it is highly recommended to only use the Subscriber Certificate for Qualified Electronic Signature in combination with a Qualified Timestamp.

The Subscriber is not responsible for acts performed with the Document while the Subscriber Certificates were in suspended state prior to the Document handover.

The Subscriber is aware that ZE publishes the valid authentication Subscriber Certificate during their validity period via LDAP directory service.

9.6.4 Relying Party representations and warranties

In addition to elsewhere stated in this CPS, a Relying Party will:

- Be sufficiently informed about the use of Certificates and PKI;
- Receive notice and adhere to the conditions of this CPS and associated conditions for Relying Parties;

- Validate a Certificate by using a CRL or OCSP in accordance with the Certificate path validation procedure;
- Trust a Certificate within its validity period only if it has not been revoked;
- Rely on a Certificate, as may be reasonable under the circumstances.

It is the sole responsibility of the Relying Parties accessing information featured in the CA's Repositories and web site to assess and rely on information featured therein.

If a Relying Party becomes aware of or suspects that a private key has been compromised it will immediately notify the RA.

9.6.5 Representations and warranties of other participants

The Card Manufacturer is responsible for the supply, initialisation, personalisation, secure data transfer and the distribution of the Documents and the embedded QSCD chip.

In addition to elsewhere stated in this CPS, the Card Manufacturer will:

- Design, manufacture and supply the QSCD;
- Personalize the QSCD including:
    - Initialization and configuration of the QSCD;
    - Generation of key pairs on the QSCD;
    - Generation of certificate requests for the Subscriber Certificates;
    - Loading the CA certificates and the Subscriber Certificates on the QSCD;
    - Loading the identification data of the Subscriber on the QSCD;
    - Creation of the PIN and PUK codes and the PIN/PUK-letter;
- Ensure and maintain the QSCD's certification as QSCD;
- Notify the QTSP of changes, incidents or flaws that may impact the QSCD's security or certification status.

9.7 Disclaimers of warranties

The QTSP explicitly declines all liability towards Relying Parties and Subscribers in all cases where

- a Certificate was used improperly,
- a Certificate was used for any purpose other than the Certificate's intended use,
- the validity of the Certificate was not properly checked at the relevant time,
- an authentication Certificate was used in a private setting between private parties, which is beyond authentication that is required under national law or by administrative practice to access a service provided by a public sector body.

9.8 Limitations of liability

The QTSP limits and excludes its liability towards Subscribers and all Relying Parties as stipulated below.

The limitation to the liability of the QTSP shall apply differently, depending on whether (i) damage may have been caused by the QTSP due to a failure to comply with its obligations under the eIDAS Regulation [EU 910/2014 EIDAS] (see Chapter 9.8.1) or whether (ii) damage is caused by an error or fault that is not a failure to comply with the obligations under the eIDAS Regulation [EU 910/2014 EIDAS] (see Chapter 9.8.2).

9.8.1 For damages caused due to a failure to comply with the obligations under the eIDAS Regulation

The QTSP shall be liable for damage caused intentionally or negligently to any natural or legal person due to a failure to comply with the obligations under the eIDAS Regulation [EU 910/2014 EIDAS]. Any natural or legal person who has

suffered material or non-material damage as a result of an infringement of the eIDAS Regulation [EU 910/2014 EIDAS] by the QTSP shall have the right to seek compensation in accordance with Union and national law.

The intention or negligence of a qualified trust service provider shall be presumed unless that qualified trust service provider proves that the damage referred to in the first paragraph occurred without the intention or negligence of the QTSP.

Without prejudice to the foregoing paragraphs, the following limitations shall apply:

- The QTSP excludes any and all liability for failure of the QSCD since the QSCD is provided by the Card Manufacturer.
- Provided that the QTSP has complied with its obligations under eIDAS Regulation [EU 910/2014 EIDAS], it shall not be liable to Subscribers or Relying Parties for the acts or omissions of other PKI participants.
- The exclusions and limitations iterated under the previous section 9.7 of this CPS shall apply, as a limitation on the use of the services under article 13(2) of the eIDAS Regulation [EU 910/2014 EIDAS].

Exclusion of Certain Elements of Damages

Within the limit set by Estonian Law and not limiting more than what is allowed under article 13 of the eIDAS Regulation [EU 910/2014 EIDAS], as described above, the QTSP shall not be liable for:

- Any loss of profits;
- Any indirect or consequential damage caused by loss of data;
- Any indirect, consequential or punitive damages arising from or in connection with the use, delivery, license, and performance or non-performance of Certificates or digital signatures;
- Any non-compliance or contractual breach by the Card Manufacturer; or
- Any other damages beyond proven direct damages.

If any provision of limitation of liability or exclusion of warranty is declared by an Estonian court to be invalid, illegal or unenforceable under applicable law the remaining provisions shall continue to be in full force and effect.

9.8.2 For damages caused by an error or fault that is not deemed as a failure to comply with the obligations under the eIDAS Regulation

In relation to any damage caused by an error or fault of the QTSP that is not damage caused intentionally or negligently due to a failure to comply with the obligations under the eIDAS Regulation [EU 910/2014 EIDAS], the following limitations of liability shall apply:

- Any and all limitations and exclusions applied under section 9.8.1.
- In addition, in case of liability of the QTSP towards the Subscriber or a Relying Party for proven direct damages, the liability of the QTSP towards any claimant is in any way limited to paying damages amounting up to the upper limit stated in the published insurance information. Such upper limit shall be applied per Certificate that is underlying to the claim and for the full validity period of that Certificate, and per claimant.
- The exclusions as stated hereafter.

Excluded liability

Unless the QTSP intentionally or negligently infringed its obligations under the eIDAS Regulation [EU 910/2014 EIDAS], QTSP shall bear absolutely no liability for any loss whatsoever involving or arising from any one (or more) of the following circumstances or causes:

- If the Certificate held by the claiming party or otherwise the Subscriber involved in the claim has been compromised by the unauthorised disclosure or unauthorised use of the Certificate or any password or activation data used to control access thereto;
- If the Certificate held by the claiming party or otherwise the Subscriber involved in the claim was issued as a result of any misrepresentation, error of fact, identity fraud or omission of the (intended) Subscriber concerned;

- If the Certificate held by the claiming party or otherwise the Subscriber of any claim had expired or been revoked prior to the date of the circumstances giving rise to any claim;
- If the Certificate held by the claiming party or otherwise the Subscriber involved in the claim has been modified or altered in any way or been used otherwise than as permitted by the terms of the [ZE TSPS-ID1], this CPS and/or the relevant Subscriber Agreement and Terms & Conditions [ZE TC-ID1-SUB] or any applicable law or regulation;
- If the private key associated with the Certificate held by the claiming party or otherwise the Subscriber involved in the claim has been compromised;
- If the Certificate held by the claiming party or the signature on which a Relying Party has relied on, has been invalidated after its use without any fault or intention attributable to the QTSP;
- Where the claiming Party relies on a Certificate beyond the validity period of the Certificate or where the claiming party relies on an electronical signature based on such Certificate at a time beyond the validity period of such Certificate without substantial time-stamping evidence the electronical signature was issued within the validity period of the Certificate;
- Computer hardware or software, or mathematical algorithms, are developed that tend to make public key cryptography or asymmetric cryptosystems insecure, provided that the QTSP has taken all necessary measures to increase the quality and security level of the services and supplies in such a way that would preserve a high level of quality and security of equivalent services and goods in the changed circumstances and ensure the continued use of the services and goods for their intended purpose and with a high level of security;
- Power failure, power interruption, or other disturbances to electrical power, provided that the QTSP has taken all necessary measures to increase the quality and security level of the services and supplies in such a way that would preserve a high level of quality and security of equivalent services and goods in the changed circumstances and ensure the continued use of the services and goods for their intended purpose and with a high level of security;
- Failure of one or more computer systems, communications infrastructure, processing, or storage media or mechanisms, or any sub components of the preceding, not under the exclusive control of QTSP and/or its subcontractors or service providers;
- One or more of the following events: a natural disaster or Act of God (including without limitation flood, earthquake, or other natural or weather related cause); a labour disturbance; war, insurrection, or hidden or overt military or geo-political interferences and/or hostilities; earlier unknown crypto algorithms, zero-day cyber hacking or sabotage, adverse or retro-active legislation or governmental action, prohibition, embargo, or boycott; riots or civil disturbances; fire or explosion; catastrophic epidemic; trade embargo; restriction or impediment (including, without limitation, export controls); any lack of telecommunications availability or integrity; legal compulsion including, any judgments of a court of competent jurisdiction to which the QTSP is, or may be, subject; and any event or occurrence or circumstance or set of circumstances that is beyond the control of the QTSP.

If any provision of limitation of liability or exclusion of warranty is held to be invalid, illegal or unenforceable under applicable law the remaining provisions shall continue to be in full force and effect.

9.9 Indemnities

See also clause 9.8. Further indemnity provisions and obligations are contained within relevant contractual documentation.

9.10 Term and termination of the present CPS

9.10.1 Term

The present document becomes effective 30 days after publication in the CA's Repository. Amendments to this document become effective 30 days after publication in the CA's Repository.

9.10.2 Termination

The present document remains in force until notice of the opposite is communicated on the CA's Repository.

9.10.3 Effect of termination and survival

The provisions of this document shall survive the termination or withdrawal of a Subscriber or Relying Party with respect to all actions based upon the use of or reliance upon a Subscriber Certificate or other participation or usage of the Certificates and related services. Any such termination or withdrawal shall not act so as to prejudice or affect any right of action or remedy that may have accrued to any person up to and including the date of withdrawal or termination.

9.11 Individual notices and communications with participants

See clause 1.5.2

9.12 Amendments to the present CPS

9.12.1 Procedure for amendment

Changes are managed by the Policy Management Authority (PMA) of the QTSP. All proposed changes need to be approved by the PMA and PBGB.

9.12.2 Notification mechanism and period

After approval a new version of the document is created and published alongside the former version on the CA's Repository.

9.12.3 Circumstances under which OID must be changed

Minor changes to this CPS do not require a change in the CPS OID or the CPS pointer qualifier (URL) that might be communicated by the CA. Major changes that may materially change the acceptability of Certificates for specific purposes may require corresponding changes to the CPS OID or CPS pointer qualifier (URL).

9.13 Dispute resolution provisions

All disputes associated with this CPS will be resolved according to Estonian Law.

Complaints related to this CPS and the Certificates are addressed to:

See clause 1.5.1 and 1.5.2

Any arbitration shall, unless agreed otherwise between the parties take place in Estonia.

9.14 Governing law

The QTSP is governed by the jurisdictions of the European Union and of the Republic of Estonia.

9.15 Compliance with applicable law

ZE ensures compliance with the legal requirements to meet all applicable statutory requirements for protecting records from loss, destruction and falsification, and the requirements of the following:

- 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 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework [EU 910/2014 EIDAS]
- GDPR - Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [EU 679/2016 GDPR];

- Electronic Identification and Trust Services for Electronic Transactions Act [EST EIDTSET ACT]
- Personal Data Protection Act [EST PDP ACT]
- Identity Documents Act [EST ID ACT]
- Statutory Fees Act [EST FEES ACT]
- Other applicable laws of the Republic of Estonian and the European Union, see the corresponding clause in the PBGB Certificate Policies [PBGB CP-ID1-ROOT]

9.16 Miscellaneous provisions

9.16.1 Entire agreement

Subscribers accept this CPS [ZE CPS-ID1-EID-CA], the Subscriber Agreement and Terms & Conditions [ZE TC-ID1-SUB] as well as associated documents under the Certificate acceptance rules of the Document application and handover process. Relying Parties should only rely on Certificates in line with this CPS. ZE also requires each party using its products and services to enter into an agreement that delineates the terms associated with the product or service. If an agreement has provisions that differ from this CPS, then the agreement with that party prevails, but solely with respect to that party. Third parties may not rely on or bring action to enforce such agreement.

9.16.2 Assignment

Not applicable.

9.16.3 Severability

Any provision of the present CPS document that is determined to be invalid or unenforceable will be ineffective to the extent of such determination without invalidating the remaining provisions of the present CPS document or affecting the validity or enforceability of such remaining provisions.

9.16.4 Enforcement (attorneys' fees and waiver of rights)

The failure or delay of the QTSP to exercise or enforce any right, power, privilege, or remedy whatsoever, howsoever or otherwise conferred upon it by the present CPS document; shall not be deemed to be a waiver of any such right or operate so as to bar the exercise or enforcement thereof at any time or times thereafter, nor shall any single or partial exercise of any such right, power, privilege or remedy preclude any other or further exercise thereof or the exercise of any other right or remedy. No waiver shall be effective unless it is in writing. No right or remedy conferred by any of the provisions of the present CPS document is intended to be exclusive of any other right or remedy, except as expressly provided in the present CPS document, and each and every right or remedy shall be cumulative and shall be in addition to every other right or remedy given hereunder or now or hereafter existing in law or in equity or by statute or otherwise.

9.16.5 Force Majeure

The QTSP accepts no liability for any breach of warranty, delay or failure in performance that results from events beyond its control such as Acts of God, acts of war, acts of terrorism, epidemics, power or telecommunication services failure, fire, and other natural disasters. See also Section 9.8 (Excluded Liability) above.

9.17 Other provisions

Not applicable.

APPENDIX A - REFERENCES

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

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