AS Sertifitseerimiskeskus – Certification Practice Statement for KLASS3-SK 2010

Version 1.0
1 July 2016

Version and Changes		
Date	**Version**	**Changes**
1 July 2016	1.0	Approved version -Chapter 1.0 – Added ETSI EN 319 411-2 Policy: QCP-l; -Chapter 1.0 - Added that e-Seal Certificates are also issued under ETSI EN 319 411-2 Policy: QCP-l; -Chapter 1.6 – added acronym gTLD; -Chapter 2.2 – Added URLs for revoked and expired certificates; -Chapter 3.1.2 – Added value in the Common Name field; -Chapter 3.2.2.1 – Specified issuance of e-Seal Certificates; -Chapter 3.2.2.2 – Added verification of Commonly Recognised Name; -Chapter 3.2.5 – Specified verification of right of representation; -Chapter 4.1.2 – Added requirements on the Secure Cryptographic Device; -Chapter 4.1.2.1 – Added requirements for the Certificate application; -Chapter 4.2 – Specified the scope of dual control; -Chapter 4.2.1 – Specified the grounds on which SK can change value in Certificate fields; -Chapter 4.3.1 – Added possibility to issue e-Seal Certificate on Secure Cryptographic Device; -Chapter 4.6 – Specified notification of the Subscriber of the Certificate expiry; -Chapter 4.9 – Added identification of the person filing revocation application. Added statement that revoked Certificate can not be reinstated. -Chapter 4.9.15 – Specified procedure for suspension request; -Chapter 4.9.19 – Added submission of application for termination of suspension and identification of the person filing application for termination of suspension. Added statement on the obligation to submit an application for revocation. -Chapter 4.10.1 – Added that URLs of the CDP is included in

		the certificates issued until 1 July 2016. -Chapter 5.6 – Added information on key changeover; -Chapter 6.1.1 - Added specification on Secure Cryptographic Device; -Chapter 6.2.1 – Specified Cryptographic Module Standards and Controls; -Chapter 6.2.6 – Added Secure Cryptographic Device; -Chapter 6.4.1 – Added requirements on activation codes.
1 April 2016	0.1	Draft of version 1.0

1. INTRODUCTION

AS Sertifitseerimiskeskus (SK) was founded on March 26th 2001. The owners of the limited liability company are AS Swedbank, AS SEB Pank and Telia Eesti AS. The principal activities of SK are offering trust services and related technical solutions in the Baltic region. These services guarantee secure and verified electronic communication with public institutions as well as businesses in everyday life.

The CPS is a complete redesign of the previous “AS Sertifitseerimiskeskus - Certification Practice Statement” and “Certification Policy for Organisation Certificates.” Redesign of the named documents in accordance with the IETF RFC 3647 [1] and enforcement of this CPS do not substantially change provision of the respective certification service.

Inspired by the ETSI EN 319 400 series, SK has divided its documentation into three parts:

- SK Trust Services Practice Statement (SK PS) describes general practices common to all trust services;
- Certification Practice Statements and Time-Stamping Practice Statements describe parts that are specific to each Subordinate CA or Time-Stamping Unit;
- Technical Profiles are in separate documents.

Pursuant to the IETF RFC 3647 [1] this CPS is divided into nine parts. To preserve the outline specified by RFC 3647 [1], section headings that do not apply have the statement **"Not applicable"**. Each first-level chapter includes reference to the corresponding chapter in ETSI EN 319 411-1 [13]. References to Baseline Requirements [8] are not included since both documents follow the structure of IETF RFC 3647 [1] and each reference would be to the section with the same number. References to SK PS and Certificate Profile documents are included where applicable.

1.1 Overview

This CPS describes the practices used to comply with “AS Sertifitseerimiskeskus - Certificate Policy for Organisation Certificates” [2] (CP) and “AS Sertifitseerimiskeskus – Certificate Policy for TLS Server Certificates” [3] (CP for TLS Server Certificates).

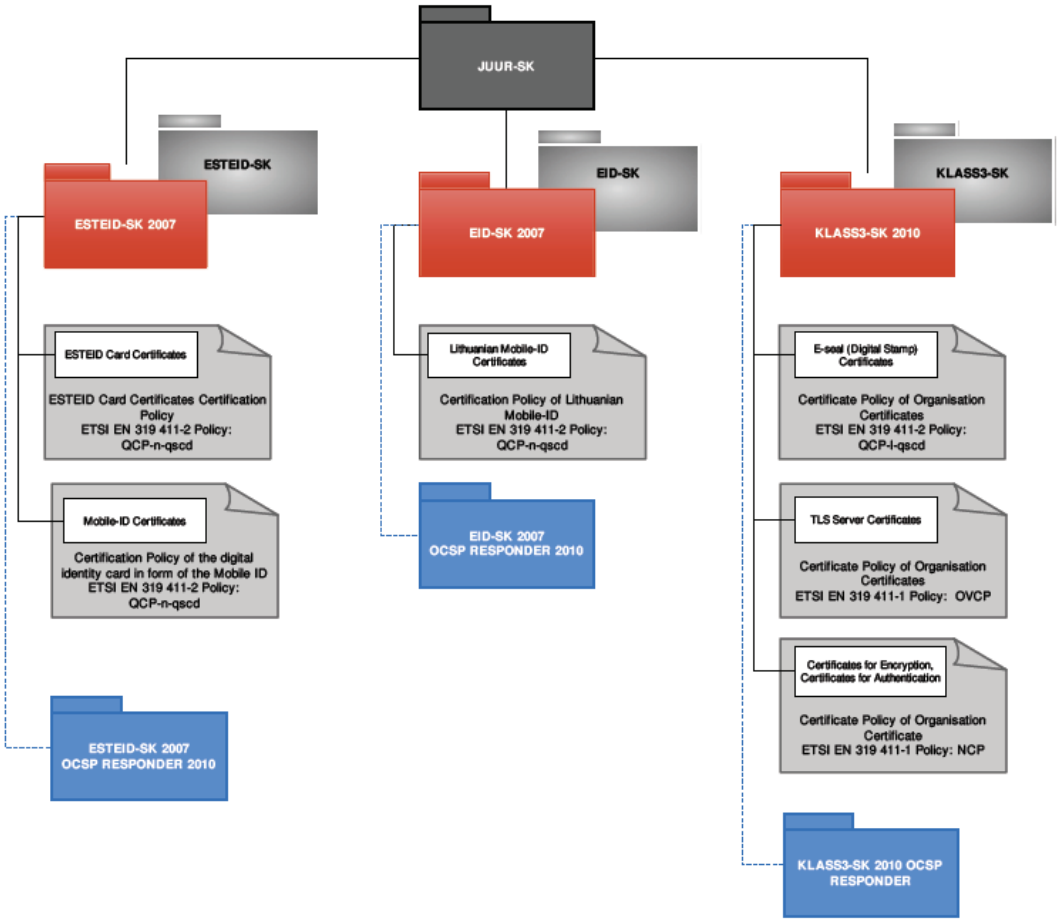
These policies are compliant with ETSI EN 319 411-1 Policies: NCP and OVCP [13] and ETSI EN 319 411-2 Policy: QCP-l-qscd and QCP-l [12]. The OVCP includes CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates [8] (“Baseline Requirements”).

SK also follows the Browser Root Program Requirements from Microsoft, Mozilla and Apple [9] [10] [11].

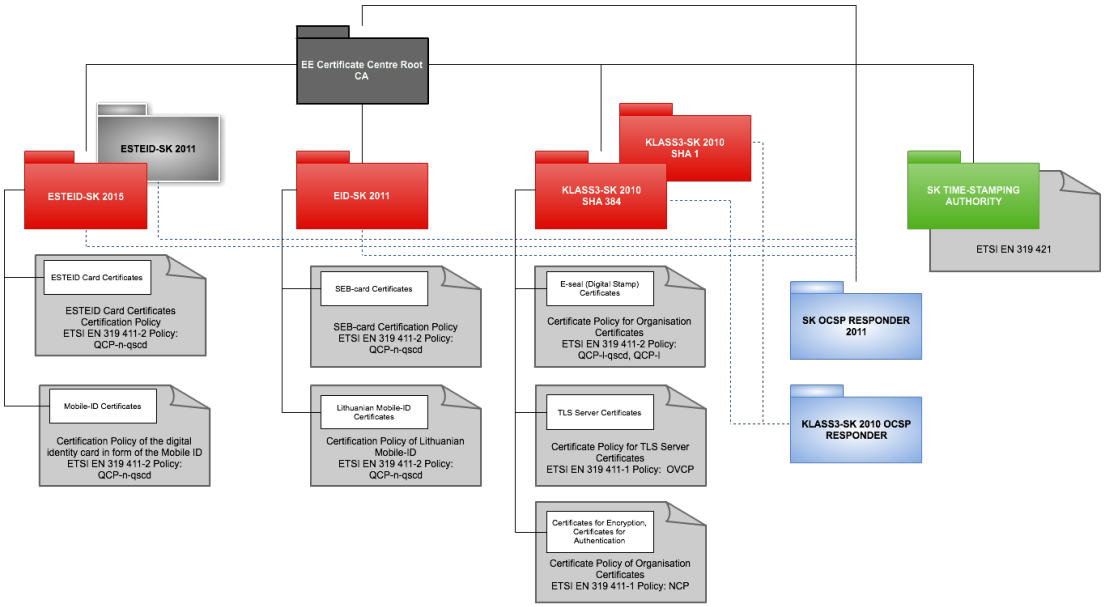
SK is currently using two certificate chains, root certification authorities are “Juur-SK” and “EE Certification Centre Root CA”. Both roots have certified KLASS3-SK 2010. The Root CA certificates and other certificates necessary for PKI operation are available from SK's website at http://www.sk.ee/repository/certs.

Their relations between Root CAs, Subordinate CAs and the CPs are shown on the following figures:

1) Juur-SK



2) EE Certification Centre Root CA



The certification service for e-Seal Certificates described in this CPS has qualified status in the Trusted List of Estonia.

The Root CA Certificates are included in Microsoft, Mozilla and Apple browsers [9] [10] [11].

In case of conflicts the documents are considered in the following order (prevailing ones first):

- Browser root program requirements (only for TLS Server Certificates);
- Baseline Requirements (only for TLS Server Certificates);
- ETSI Policies NCP, QCP-l-qscd, QCP-l or OVCP;
- CP or CP for TLS Server Certificates;
- This CPS.

1.2 Document Name and Identification

This document is called “AS Sertifitseerimiskeskus – Certification Practice Statement for KLASS3-SK 2010.” This is the first version of this document.

1.3 PKI Participants

1.3.1 Certification Authorities

SK operates as a CA.

The Certificates are issued by the intermediate CA KLASS3-SK 2010 that is identified by the following certificate:

Certificate:
Data:
Version: 3 (0x2)
Serial Number:
0a:19:b7:e3:1f:1a:87:70:55:70:57:9d:96:cd:9c:da
Signature Algorithm: sha384WithRSAEncryption
Issuer: C=EE, O=AS Sertifitseerimiskeskus, CN=EE Certification Centre Root CA/emailAddress=pki@sk.ee
Validity
Not Before: Jun 4 13:50:21 2015 GMT
Not After: Mar 17 22:00:00 2024 GMT
Subject: C=EE, O=AS Sertifitseerimiskeskus, OU=Sertifitseerimisteenused, CN=KLASS3-SK 2010
Subject Public Key Info:
Public Key Algorithm: rsaEncryption
Public-Key: (2048 bit)
Modulus:
00:ab:95:a6:11:5f:6b:fc:f6:4f:07:77:40:03:68:
e7:e7:51:c2:27:ee:23:3a:68:e5:e4:01:1f:a3:a7:
9f:36:ed:98:43:a8:3c:8d:75:d1:7d:65:4a:01:80:
f8:21:18:d2:2b:90:76:c7:ee:ac:1e:c7:7f:58:9c:
8d:24:6b:6e:25:0a:37:30:10:cb:d0:30:f6:f2:3e:
75:ff:6b:84:72:27:ec:04:66:db:66:8c:19:7e:f8:
57:eb:64:ae:78:2f:eb:c3:ec:3c:b2:e1:86:01:d0:
e8:3d:92:d0:78:aa:9b:6c:0c:18:fe:82:28:af:fc:
c1:8f:78:67:8d:b3:74:da:70:97:4d:6f:bf:b7:b2:
99:53:3e:d3:ca:94:37:eb:b9:fb:ea:e0:7e:a3:34:
eb:fd:4b:d6:c2:fa:3d:95:55:8f:6e:08:55:d4:ae:
8f:00:03:78:68:38:42:89:75:28:e5:a5:80:9a:e7:
53:7c:28:62:d5:25:84:6e:73:f2:bc:d7:1a:a2:d3:
9e:09:cf:e0:b2:fc:76:3f:01:c5:e4:93:62:64:c6:
5a:49:a0:45:e6:72:e4:e4:c6:33:bf:40:4f:d7:6d:
df:a6:44:91:e7:ab:af:87:ba:b3:a2:29:cc:4a:c1:
90:8f:01:af:9d:f9:db:d1:3e:46:f2:ab:da:21:31:
71:fd
Exponent: 65537 (0x10001)
X509v3 extensions:
X509v3 Basic Constraints: critical
CA:TRUE, pathlen:0
X509v3 Key Usage: critical
Digital Signature, Non Repudiation, Certificate Sign, CRL Sign
X509v3 Certificate Policies:
Policy: 1.3.6.1.4.1.10015.100.1.1.1
CPS: https://www.sk.ee/cps
User Notice:
Explicit Text:

X509v3 Subject Key Identifier:
5D:75:14:11:8C:F4:A5:8E:42:8F:7B:B2:40:44:A3:EE:D6:7A:3B:72

X509v3 Authority Key Identifier:
keyid:12:F2:5A:3E:EA:56:1C:BF:CD:06:AC:F1:F1:25:C9:A9:4B:D4:14:99

Authority Information Access:
OCSP - URI:http://ocsp.sk.ee/CA
CA Issuers - URI:http://www.sk.ee/certs/EE_Certification_Centre_Root_CA.der.crt

X509v3 CRL Distribution Points:

Full Name:
URI:http://www.sk.ee/repository/crls/eeccrca.crl

Signature Algorithm: sha384WithRSAEncryption
78:ff:44:cb:5d:db:4c:4e:7c:e5:f1:9f:35:d2:54:77:a4:44:
82:ab:ab:9e:41:1b:c6:3c:f9:76:8a:c1:9e:de:57:40:f4:f8:
4a:67:b8:fa:df:6d:e2:7c:8d:a5:74:e7:4c:79:4d:76:81:de:
29:ce:e1:d7:89:e1:42:d5:88:6c:c2:a5:c2:47:58:6e:2c:db:
b5:28:0f:0f:46:18:31:74:e0:50:d5:eb:51:4a:46:53:21:fb:
4c:84:18:29:c6:8b:76:4e:ee:06:db:12:90:ef:07:de:b5:da:
a7:ad:44:3f:bb:ef:81:b8:08:6e:1c:0d:b1:b2:66:b6:df:a7:
90:ef:3d:e2:ce:8c:42:39:27:3e:14:ca:50:4f:f4:98:f4:db:
ca:b5:99:66:14:43:f2:73:16:71:bb:4b:96:09:0b:41:6f:1f:
9b:fc:c0:18:2a:0a:b6:fe:f3:2f:2c:ee:25:c9:1a:a4:79:24:
6e:2c:c6:53:e0:00:38:d8:78:20:81:4c:0b:ee:15:a2:c1:e7:
72:12:ab:f0:ab:44:a0:dd:ef:76:17:6c:01:7d:ff:97:6a:1f:
d6:79:90:62:a3:1b:a5:d5:34:6d:cc:57:20:7b:a0:53:7c:5d:
92:d1:17:5b:69:a3:96:79:7b:1b:35:a0:3f:6b:36:78:5a:b3:
63:d4:24:ef

1.3.2 Registration Authorities

SK operates as an RA.

1.3.2.1 Customer Service Point

SK operates as a Customer Service Point.

Contact information:

Pärnu mnt 141, 11314 Tallinn, Estonia
(Mon-Fri 9.00 a.m. - 6.00 p.m. Eastern European Time)
Tel +372 610 1880
Email: info@sk.ee

Revocation and Suspension requests are accepted 24/7 at:

Tel +372 610 1880
Email: revoke@sk.ee

The most recent information on Customer Service Point and its contact details is available on SK's website: https://sk.ee/en/kontakt/.

1.3.3 Subscribers

Refer to clause 1.3.3 of the CP [2] and clause 1.3.3 of the CP for TLS Server Certificates [3].

1.3.4 Relying Parties

A Relying Party is a natural or legal person who takes a decision relying on the Certificate issued by SK.

1.3.5 Other Participants

Not applicable.

1.4 Certificate Usage

Refer to clause 1.4 of the CP [2] and clause 1.4 of the CP for TLS Server Certificates [3].

1.5 Policy Administration

1.5.1 Organisation Administering the Document

This CPS is administered by SK.

AS Sertifitseerimiskeskus
Registry code 10747013
Pärnu mnt 141, 11314 Tallinn
Tel +372 610 1880
Fax +372 610 1881
Email: info@sk.ee
http://www.sk.ee/en/

1.5.2 Contact Person

Business Development Manager
Email: info@sk.ee

1.5.3 Person Determining CPS Suitability for the Policy

Not applicable.

1.5.4 CPS Approval Procedures

Amendments which do not change the meaning of the CPS, such as corrections of misspellings, translation and updating of contact details, are documented in the Versions and Changes section of the present document and the fraction part of the document version number is enlarged.

In case the CP [2] and/or the CP for TLS Server Certificates [3] are amended, the CPS is reviewed as well in order to verify the need for its amendments.

In case of substantial changes, the new CPS version is clearly distinguishable from the previous ones. The new version bears a serial number enlarged by one. The amended CPS along with the enforcement date, which cannot be earlier than 90 days after publication, is published electronically on SK's website.

Within 30 days of amendment publication, the Subscriber has the chance to provide reasoned comments followed by maximum 30-day period for comment analysis by SK. 60 days after the amendment publication, the new version of CPS is published electronically on SK's website, otherwise the amendment is withdrawn.

All amendments are to be approved by the business development manager and the amended CPS is enforced by the CEO.

1.6 Definitions and Acronyms

1.6.1 Terminology

In this CPS the following terms have the following meaning.

Term	Definition
Authentication	Unique identification of a person by checking his/her alleged identity.
Certificate Policy	A set of rules that indicates the applicability of a named certificate to particular community and/or PKI implementation with common security requirements.
Certification Practice Statement	One of several documents forming the governance framework in which certificates are created, issued, managed, and used.
Certificate Profile	Document that determines the profile and minimum requirements for the Certificate.
Certificate Revocation List	A list of invalid (revoked, suspended) certificates.
Certification Service	Issuing certificates, managing suspension, termination of suspension, revocation, modification and re-key.

Directory Service	Certificate validity information publication service.
Distinguished Name	Unique subject name in the infrastructure of certificates.
Encrypting	Information treatment method changing the information unreadable for those who do not have necessary skills or rights.
Integrity	A characteristic of an array: information has not been changed after the array was created.
OID	An identifier used to name an object (OID).
Certificate	e-Seal Certificate, TLS Server Certificate, Certificate for Encryption and Certificate for Authentication. Within the meaning of this CPS, the term “Certificate” encompasses all the previously listed certificates.
Private Key	The key of a key pair that is kept secret by the holder of the key pair, and that is used to create digital signatures and/or to decrypt electronic records or files that were encrypted with the corresponding public key.
Public Key	The key pair that may be publicly disclosed by the holder of corresponding private key and that is used by Relying Party to verify digital signatures created with the holder’s corresponding private key and/or to encrypt messages so that they can be decrypted only with the holder’s corresponding private key.
Qualified Electronic Signature/Seal Creation Device	A secure signature creation device that meets the requirements laid down in eIDAS regulation [14].
Relying Party	Entity that relies upon either the information contained within a certificate.
Registration Authority	Entity that is responsible for identification and authentication of subjects of certificates. Additionally, an RA may accept certificate applications, check the applications and/or forward the applications to the CA.
Secure Cryptographic Device	Device that holds the user's Private Key, protects this key against compromise and performs signing or decryption functions on behalf of the user.
Subscriber	Legal person bound by agreement with CA to any subscriber obligations.
TLS Server Certificate	Certificate issued to TLS server (HTTPS, IMAPS, FTPS, etc.) for proof of authenticity of TLS server owner.
Terms and Conditions	Document that describes the obligations and responsibilities of the Subscriber while using the Certificate. The Subscriber must be familiar with the document and accept the terms and conditions described within when receiving the Certificate.

1.6.2 Acronyms

Acronym	Definition
CA	Certification Authority
CAA Record	The Certification Authority Authorization (CAA) DNS Resource Record that, according to RFC 6844, allows a DNS domain name holder to specify the Certification Authorities authorized to issue certificates for that domain.
CP	Certificate Policy for Organisation Certificates [2]
CP for TLS Server Certificates	Certificate Policy for TLS Server Certificates [3]
CPS	Certification Practice Statement for KLASS3-SK 2010
CRL	Certificate Revocation List
CSR	Certificate Signing Request
DNS	Domain Name System according to RFC 3467 (http://tools.ietf.org/html/rfc3467)
eIDAS	Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC [14].
gTLD	generic Top Level Domain
IANA	The Internet Assigned Numbers Authority is an organisation, which oversees global IP address allocation, autonomous system number allocation, root zone management in the Domain Name System, media types, and other Internet Protocol-related symbols and numbers.
HSM	Hardware Security Module
QSCD	Qualified electronic Signature/Seal Creation Device
OID	Object Identifier, a unique object identification code
RA	Registration Authority
SK	AS Sertifitseerimiskeskus, provider of the certification services
SK PS	AS Sertifitseerimiskeskus Trust Services Practice Statement [7]
URI	Unified Resource Identifier

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 Repositories

Refer to clause 2.1 of AS Sertifitseerimiskeskus Trust Services Practice Statement [7] (SK PS).

2.2 Publication of Certification Information

Refer to clause 2.2 of SK PS [7].

2.2.1 Publication and Notification Policies

This CPS is published on SK's website: https://sk.ee/en/repository/CPS/.

This CPS and referred documents – the CP [2], the CP for TLS Server Certificates [3] and the "Certificate, CRL and OCSP Profile for Organisation Certificates Issued by SK" [5] (Certificate Profile) as well as the Terms and Conditions [4] with the enforcement dates are published no less than 90 days prior to taking effect.

A valid TLS Server Certificate issued per this CPS can be viewed on SK's website: https://sk.ee/. SK has example pages with revoked certificate at https://revoked.tls.sk.ee/ and expired certificate at https://expired.tls.sk.ee/.

2.2.2 Items not Published in the Certification Practice Statement

Refer to clause 9.3.1 of SK PS [7].

2.3 Time or Frequency of Publication

Refer to clause 2.2.1 of this CPS.

2.3.1 Directory Service

Refer to clause 2.3.3 of SK PS [7].

2.4 Access Controls on Repositories

Refer to clause 2.4 of SK PS [7].

3. IDENTIFICATION AND AUTHENTICATION

3.1 Naming

Types of names assigned to the Subscriber are described in the Certificate Profile [5].

3.1.1 Types of Names

Refer to clause 3.1.1 of the CP [2] and clause 3.1.1 of the CP for TLS Server Certificates [3].

3.1.2 Need for Names to be Meaningful

Names are meaningful for the following fields of e-Seal Certificate, Certificate for Encryption and Certificate for Authentication:

- Organisation (O): Legal name of the Subscriber;
- Common Name (CN): Legal or Commonly Recognised name of the Subscriber, optionally followed by intended usage for the certificate;
- OrganizationIdentifier: Pursuant to syntax described in the CP [2], identifier of the registry used, followed by registration number of the Subscriber.

Names are meaningful on the following fields of TLS Server Certificate:

- Organisation (O): Legal name of the Subscriber;
- Common Name (CN): the Fully Qualified Domain Name or IP Address of the server for which the certificate is issued;
- Subject Alternative Name (SAN): the Fully Qualified Domain Name or IP Address of the server for which the certificate is issued.

3.1.3 Anonymity or Pseudonymity of Subscribers

Not applicable.

3.1.4 Rules for Interpreting Various Name Forms

Rules for interpreting various name forms are described in the Certificate Profile [5].

3.1.5 Uniqueness of Names

In order to assure that the Certificate with an identical Subscriber's distinguished name is not issued to another Subscriber, the Subscriber's name in the Organization (O) field is checked by SK according to clause 3.2 of this CPS. Only Legal Names of Subscribers are allowed on the Organization (O) field.

3.1.6 Recognition, Authentication, and Role of Trademarks

The Subscriber must prove its entitlement to use all trademarks that are requested for inclusion into the certificate.

3.2 Initial Identity Validation

Refer to clause 3.2 of the CP [2] and clause 3.2 of the CP for TLS Server Certificates [3].

3.2.1 Method to Prove Possession of Private Key

In order to apply for the Certificate, the Subscriber can electronically submit a CSR in PKCS#10 [6] format, which contains the Public Key of the legal person and is signed with the

corresponding Private Key. The integrity of the signing request allows SK to presume that the corresponding Private Key is in the legal person's possession.

If SK has granted the authority to generate the Public and Private Key for the Subscriber, the conformity is guaranteed by the internal procedures of SK and the Subscriber does not have to electronically submit the CSR.

3.2.2 Authentication of Organisation and Domain Identity

3.2.2.1 Identity

SK verifies that the Subscriber, as identified by the Organization (O) and OrganizationIdentifier fields on the application, is registered in:

- the Estonian Business Register (https://ariregister.rik.ee/); or
- the Estonian Non-Profit Associations and Foundations Register; or
- the Estonian Register of State and Local Government Organisations.

The Estonian Business Register and the Estonian Non-Profit Associations and Foundations Register are accessible at: http://register.fin.ee/register/index.php.

If the request is for Certificate for Encryption or Authentication or TLS Server Certificate, the Subscriber can also be registered in the Latvian, Lithuanian, Finnish or Swedish Business Register and be discoverable from the European Business Register (accessible through https://ariregister.rik.ee).

E-Seal Certificates are issued only to Subscribers registered in the Estonian Business Register or the Estonian Non-Profit Associations and Foundations Register or the Estonian Register of State and Local Government Organisations.

SK verifies that the Subscriber is not bankrupt or in the process of liquidation and its activities are not suspended or in other similar state in accordance with legislation of its country of origin.

3.2.2.2 DBA/Tradename

In case any value on the Certificate field is uncommon or unidentified from the registries listed in clause 3.2.2 of this CPS, SK verifies if the value is a trademark by submitting a query to the Trade marks database of the Estonian Patent Office (http://www2.epa.ee/Patent/mark.nsf/SearchEngl?OpenForm).

If necessary, SK requires the Subscriber to present a copy of the trademark certificate.

Commonly Recognised Name is verified by professional skills of the Customer Service Point employee.

3.2.2.3 Verification of Country

SK verifies that the CountryName field in the Certificate request matches the registry listed in clause 3.2.2.1 of this CPS in which the Subscriber is registered.

3.2.2.4 Authorization by Domain Name Registrant

The Subscriber's control over the domain listed in the application is checked from IANA's registry, available at: https://www.iana.org/whois. If the answer points to a regional registry (ARIN, RIPE, etc.), a subsequent query to that registry is performed until authoritative answer is found.

3.2.2.5 Authentication for an IP Address

The Subscriber's control over the IP address listed in the application is checked from IANA's registry, available at: https://www.iana.org/whois. If the answer points to a regional registry (ARIN, RIPE, etc.), a subsequent query to that registry is performed.

If the Subscriber applies for the Certificate for an IP address, the Subscriber is required to ascertain that during the certificate's validity period, the IP will not be resolvable in the Public DNS system.

SK does not issue IPv4 or IPv6 addresses marked as "reserved" by IANA.

3.2.2.6 Wildcard Domain Validation

Not applicable.

3.2.2.7 Data Source Accuracy

All the registries listed in chapter 3.2 are considered a Reliable Data Source in the meaning of Baseline Requirements [8].

3.2.3 Authentication of Individual Identity

Not applicable.

3.2.4 Non-Verified Subscriber Information

Refer to clause 3.2.4 of the CP [2] and clause 3.2.4 of the CP for TLS Server Certificates [3].

3.2.5 Validation of Authority

As the application for the Certificate is submitted and signed electronically with an Advanced or Qualified Signature compliant to eIDAS [14], physical presence of the Subscriber's legal representative or authorised person is not required.

For Estonian organizations the right of representation of the Subscriber's legal representative is checked by reviewing the Subscriber's registry card data in the Estonian Business Register or the Estonian Non-Profit Associations and Foundations Register. The right of representation of the Subscriber's legal representative is also checked by reviewing relevant laws, statutes of the state and local government organisation and decrees issued by the signatory of the state and local government organisation.

If a TLS Server Certificate, Certificate for Encryption or Certificate for Authentication is requested by a foreign Subscriber, the right of representation is checked from the European Business Register.

The validity of letter of attorney of the Subscriber's authorised person is verified by checking the substance of the letter of attorney and the right of representation of the Subscriber's legal representative. Letters of attorney can be submitted electronically or delivered in person to the Customer Service Point.

The contact person listed in the domain registrant's records is considered to have the right of representation.

3.2.6 Criteria for Interoperation

Not applicable.

3.3 Identification and Authentication for Re-Key Requests

3.3.1 Identification and Authentication for Routine Re-Key

Refer to clause 3.2.2 of this CPS.

3.3.2 Identification and Authentication for Re-Key after Revocation

Refer to clause 3.2.2 of this CPS.

3.4 Identification and Authentication for Revocation Request

If the revocation request is submitted by the Subscriber, a Supervisory Body or court, the request is authenticated as described in clause 3.2.2 of this CPS.

For suspension, the requester is identified and the validity of the request is verified using professional skills of Customer Service Point employee.

4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 Certificate Application

4.1.1 Who Can Submit a Certificate Application

Any person with access to public Internet can submit an application for the Certificate to SK.

4.1.2 Enrolment Process and Responsibilities

The Subscriber files an application for the requested Certificate on SK's website at https://www.sk.ee/en/services/. The application is signed with an Advanced or Qualified Electronic Signature compliant with eIDAS [14] by the legal person's representative or authorised person.

Upon submitting an application for the Certificate, the Subscriber confirms the correctness and integrity of the information presented to SK.

Upon submitting an application for the Certificate, the Subscriber confirms agreement to the Terms and Conditions [4].

In case of an e-Seal Certificate issued on QSCD issued under policy QCP-l-qscd application based on the CSR, the Subscriber confirms that the private key is stored on a QSCD and it has possession over the device.

In case of an e-Seal Certificate issued on Secure Cryptographic Device under policy QCP-l, the Subscriber confirms that the private key is stored on:

- Federal Information Processing Standards Publication 140-2 level 2 (FIPS 140-2 Level 2) or higher; or
- Common Criteria (CC) (Standard EN 419 211, Protection Profiles for Secure Signature Creation and other related devices).

SK checks the correctness and integrity of the information provided in the application.

SK checks the validity of a Common Criteria Certificate issued for a QSCD in accordance with clause 4.1.2.2 of this CPS.

SK is entitled to adopt additional checks prior to the issuance of the Certificate if the Subscriber does not have the ability to electronically sign the application.

One application suffices for multiple Certificates to be issued simultaneously to the same Subscriber.

SK does not apply the aging and updating requirement of contact information in the meaning of Baseline Requirements [8].

4.1.2.1 Submission of Application for Certificates

An application includes the following information:

- Information about the Subscriber (name, registry code, VAT No, phone, e-mail for notifications, country, city, postal code, address, invoice e-mail);
- Information on the legal person's representative or authorised person or person who signed the application (first name, last name, personal identification code, phone, e-mail, authorization document);
- The distinguished name and validity period of the requested Certificate.

The application for TLS Server Certificate contains CSR in PKCS#10 format.

The application for e-Seal, Certificate for Authentication or Encryption contains:

- CSR in PKCS#10 [6] format; and
- Information on a QSCD (device type, firmware version, serial number of the device, name of the QSCD provider, valid Common Criteria Certificate issued for the device or guidance on how to verify the validity of a Common Criteria Certificate); or
- Proof that SCD is compliant with the requirements listed in clause 4.1.2 of this CPS; or
- Permission for SK to generate the Private Keys on behalf of the Subscriber.

The Subscriber immediately notifies SK of withdrawal of a Common Criteria Certificate issued for a QSCD.

4.1.2.2 Annual Control of QSCD

SK carries out annual verification of QSCD on which an e-Seal Certificate has been loaded.

SK asks the Subscriber to provide the following:

- Information on the legal person listed in clause 4.1.2.1 of this CPS;
- Updated contacts and information about authorised persons of the Subscriber;
- Information listed in clause 4.1.2.1 of this CPS about the QSCD in use.

The information provided by the Subscriber to SK has to be signed by the Subscriber's legal representative or authorised person who also confirms the correctness and integrity of the information.

SK verifies the following:

- Authority of the Subscriber's representative or authorised person pursuant to clause 3.2.5 of this CPS;
- Validity of Common Criteria Certificate issued for the QSCD;
- Whether the QSCD is the same device that was used when applying for the Certificate.

If the QSCD has changed, SK asks for proof that the Subscriber has performed the transfer of keys in a properly secured way. If the Subscriber is unable to present the necessary information, SK revokes the e-Seal Certificate on QSCD.

Notification of the results of QSCD verification is sent by e-mail to the Subscriber.

4.2 Certificate Application Processing

At least two employees of SK review if each application for the Certificate is compliant with the clause 4.1 of this CPS before issuance of the Certificate. Special diligence is also applied on verification of Domain ownership and authorisation of the persons representing Subscriber.

4.2.1 Performing Identification and Authentication Functions

Refer to clause 3.2.2 of this CPS.

SK does not apply any additional requirements on processing High Risk Certificates in the meaning of Baseline Requirements [8]. All applications for the Certificates are considered to be equally high risk and same identification and authentication procedures are applied.

In case the application for the Certificate does not contain all the necessary information about the Subscriber, SK obtains the remaining information from the registries listed in clause 3.2.2 of this CPS. SK considers data in the referred registries reliable and accurate and therefore does not confirm obtained information with the Subscriber.

In case the data on an application for the Certificate is missing, contains grammatical errors, contradicts with the Certificate Profile [5] or the data in registries listed in clause 3.2.2 of this CPS then without notifying the Subscriber, SK can change the values in the following fields of Subject information of the Certificate:

Subject Distinguished Name:

- Organizational Unit (OU);
- Common Name (CN);
- Organization (O);
- Locality (L);
- State (S);
- Serial Number;

- Valid from;
- Valid to.

4.2.2 Approval or Rejection of Certificate Applications

The acceptance or rejection of an application for the Certificate is decided by SK.

SK issues a Certificate only to a legal person registered in the registers listed in clause 3.2.2.1 of this CPS.

SK does not issue TLS Server Certificate containing a new gTLD (generic Top Level Domain) under consideration by ICANN.

SK does not issue IPv4 or IPv6 addresses marked as “reserved” by IANA.

SK does not check CAA records when issuing TLS Server Certificates.

The decision to accept or reject the Certificate request is based on checks listed in clauses 3.2 and 4.1.2 of this CPS. If any of the checks fail, the application is rejected.

Notification of rejection of the application together with a reason is sent by e-mail to the Subscriber. Notification process of the issuance of the Certificate is described in clause 4.3.2 of this CPS.

4.2.3 Time to Process Certificate Applications

SK processes the application for the Certificate within 5 working days after receiving the application that is compliant with the requirements listed in clause 4.1 of this CPS.

4.3 Certificate Issuance

4.3.1 CA Actions During Certificate Issuance

Each Certificate is issued using a manual process.

At least two employees of SK review each issued Certificate in order to verify compliance of the Certificate to the application and the Certificate Profile [5] prior to notifying the Subscriber of issuance. The certificate is immediately revoked in case of errors.

The business development manager is automatically notified of the issuance of the Certificate for monitoring purposes.

During issuance of e-Seal Certificate on QSCD issued under policy QCP-l-qscd, SK verifies information on QSCD listed in clause 4.1.2.1 of this CPS. In case SK is not certain that the device used by the Subscriber is QSCD, SK does not issue e-Seal Certificate on QSCD

issued under policy QCP-l-qscd. The Subscriber is offered e-Seal Certificate on Secure Cryptographic Device issued under policy QCP-l.

4.3.2 Notification to Subscriber by the CA of Issuance of Certificate

SK notifies the Subscriber of the issuance of the Certificate by delivering the Certificate (or a reference thereto) to the e-mail address of the Subscriber stated in the application for the Certificate.

4.4 Certificate Acceptance

4.4.1 Conduct Constituting Certificate Acceptance

Refer to Terms and Conditions [4].

4.4.2 Publication of the Certificate by the CA

Certificates are published by SK in LDAP directory at ldap://ldap.sk.ee/ no later than within 1 hour after issuing the certificates. Certificates which are expired, suspended and revoked are not published in LDAP directory.

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

Not applicable.

4.5 Key Pair and Certificate Usage

4.5.1 Subscriber Private Key and Certificate Usage

The Subscriber is required to use the Private Key and the Certificate lawfully and in accordance with this CPS, the CP [2], the CP for TLS Server Certificates [3] and the Terms and Conditions [4].

4.5.2 Relying Party Public Key and Certificate Usage

Relying Party is required to use the Subscriber's Public Key and the Certificate lawfully and in accordance with this CPS, the CP [2], the CP for TLS Server Certificates [3] and the Terms and Conditions [4].

4.6 Certificate Renewal

Renewal of the Certificate is not performed. The Subscriber has to apply for a new Organisation Certificate.

SK sends an email about the Certificate expiry to the Subscriber's contact address:

- 30 days prior to expiry;
- 10 days prior to expiry;
- After the Certificate has expired.

4.7. Certificate Re-Key

The procedure of the re-key of the Certificate is the same as for the initial Certificate issuance.

4.8 Certificate Modification

SK performs modification of the Certificate only to fix the errors in the issued Certificate within 14 days after initial issuance of the Certificate.

Before modification of the Certificate, SK revokes the erroneous Certificate.

Modification of the Certificate can be done based on the initial application for the Certificate.

If modification of the Certificate is requested after 14 days of initial certificate issuance, SK treats it as a new application and requests the Subscriber to submit a new application for the Certificate.

4.9 Certificate Revocation and Suspension

4.9.1 Circumstances for Revocation

Refer to clause 4.9.1 of the CP [2] and clause 4.9.1 of the CP for TLS Server Certificates [3].

4.9.2 Who Can Request Revocation

Any person can request revocation.

4.9.3 Procedure for Revocation Request

An electronically signed application for revocation can be submitted to the Customer Service Point's email address. A signed application for revocation of the Certificate can also be submitted to the Customer Service Point. In case of a signed application, the identity of the person is verified based on the copy of the identity document by an employee of the Customer Service Point.

After SK has received a request for revocation of the Certificate, the procedure for processing the request is the following:

- The revocation request is registered by an employee of the Customer Service Point;
- The person filing an application for revocation is verified;
- The legality to request revocation is established;
- The compliance of the application for revocation with the CP [2] and the CP for TLS Server Certificates [3] is verified in SK's information system;
- The Certificate is removed from LDAP directory;
- A new CRL is published according to clause 4.9.7 of this CPS;
- The documentation on which the application for revocation was based is archived;
- The Subscriber is notified of revocation of the Certificate.

Detailed workflow is described in Incident Management Process (internal document).

The Certificate is revoked immediately after the request's legality has been verified, but no later than 12 hours after an application for revocation has been submitted. The revocation of the Certificate is recorded in the certificate database of SK and in CRL no later than 24 hours after an application has been submitted.

The Subscriber has a possibility to verify from the LDAP directory or the CRL that the Certificate has been revoked.

Revoked Certificate can not be reinstated.

4.9.4 Revocation Request Grace Period

The Subscriber is required to request revocation immediately after the loss and compromise of the Private Key.

4.9.5 Time Within Which CA Must Process the Revocation Request

SK is immediately obliged to process an application for revocation but no later than 6 hours after an application for revocation has been submitted.

4.9.6 Revocation Checking Requirements for Relying Parties

The mechanisms available to a Relying Party for checking the status of the Certificate on which it wishes to rely have been in established in the Terms and Conditions [4].

4.9.7 CRL Issuance Frequency

The value of the nextUpdate field of CRL is set to 12 hours after issuance of CRL.

4.9.8 Maximum Latency for CRLs

SK monitors of the expiry time of the CRL that is published on SK's website. If a new CRL is not published 120 minutes before expiry of the previous one, an alarm is raised.

4.9.9 On-Line Revocation/Status Checking Availability

An OCSP service is free of charge and publicly accessible.

4.9.10 On-Line Revocation Checking Requirements

The mechanisms available to a Relying Party for checking the status of the Certificate on which it wishes to rely have been in established in the Terms and Conditions [4].

4.9.11 Other Forms of Revocation Advertisements Available

SK offers an OCSP service with better SLA under agreement and price list.

4.9.12 Special Requirements Related to Key Compromise

Not applicable.

4.9.13 Circumstances for Suspension

Suspension is allowed only for e-Seal Certificates, circumstances of suspension are listed in clause 4.9.13 of the CP [2].

4.9.14 Who Can Request Suspension

Any person can request suspension.

4.9.15 Procedure for Suspension Request

An application for suspension of an e-Seal Certificate can be submitted to Customer Service Point's e-mail address. A written application for suspension can also be submitted to the Customer Service Point. An application for suspension does not need to be signed.

After SK has received a request for suspension of the E-Seal Certificate, the procedure for processing the request is the following:

- The suspension request is registered by an employee of the Customer Service Point;
- The person filing an application for suspension is identified by using professional skills of the Customer Service Point employee;

- The legality to request suspension is verified by using professional skills of the Customer Service Point employee;
- The compliance of the application for suspension of the E-Seal Certificate with the CP [2] is verified in SK's information system;
- The E-Seal Certificate is marked as suspended in the certificate database;
- The E-Seal Certificate is deleted from LDAP directory;
- A new CRL is published according to clause 4.9.7 of this CPS;
- The documentation on which the application for suspension was based is archived;
- The Subscriber is notified of suspension of the Certificate.

Detailed workflow is described in Incident Management Process (internal document).

E-Seal Certificate is suspended immediately after the request's legality has been verified, but no later than 12 hours after an application for suspension has been submitted.

The suspension of the E-Seal Certificate is recorded in the certificate database of SK and CRL no later than 24 hours after an application has been submitted.

The Subscriber has a possibility to verify from the LDAP directory or the CRL that the E-Seal Certificate has been suspended.

4.9.16 Limits on Suspension Period

There are no limits on the suspension period.

4.9.17 Circumstances for Termination of Suspension

Refer to clause 4.9.17 of the CP [2].

By requesting termination of suspension of an e-Seal Certificate, the Subscriber takes responsibility for all actions made with the Private Key throughout the whole suspension period. If the Subscriber cannot prove the possession of the Private Key during the suspension period, revocation of an e-Seal Certificate must be requested instead.

4.9.18 Who Can Request Termination of Suspension

Any person can request termination of suspension.

4.9.19 Procedure for Termination of Suspension

An electronically signed application for termination of suspension of an e-Seal Certificate can be submitted to SK's email address.

A signed application for termination of suspension of an e-Seal Certificate can also be submitted to the Customer Service Point. In case of signed application, the identity of the requester is verified by the physical presence at the Customer Service Point.

The procedure of termination of suspension is the following:

- The termination of suspension request is registered by an employee of the Customer Service Point;
- The identity of the person filing an application for termination of suspension is verified as for the initial issuance of an e-Seal Certificate;
- The authority to request termination of suspension is established as for the initial issuance of an e-Seal Certificate;
- The compliance of the termination of suspension with the CP [2] is verified in SK's information system;
- The fact of termination of suspension is registered in SK's information system;
- After suspension of the e-Seal Certificate is terminated, it is published again in the LDAP directory;
- A new CRL is published according to clause 4.9.7 of this CPS.

The suspension of e-Seal Certificate is terminated immediately after the request's legality has been verified and the details about the termination of suspension are recorded in SK's information system.

SK notifies the Subscriber immediately of the successful completion of the termination of suspension procedure by sending a notification to the Subscriber's email stated in the application for termination of suspension.

The Subscriber has a possibility to verify from the LDAP directory or the next CRL that the suspension of the e-Seal Certificate has been terminated.

If the Subscriber does not have the ability to submit an application for termination of suspension, the Subscriber has to file an application for revocation.

4.10 Certificate Status Services

4.10.1 Operational Characteristics

SK offers CRL and OCSP services for checking certificate status. Services are accessible over HTTP protocol. The URLs of the services are included in the certificates on the CRL Distribution Point (CDP) and Authority Information Access (AIA) fields respectively in accordance with the Certificate Profile [5]. The URLs of the CDP is included in the certificates issued until 1 July 2016.

4.10.2 Service Availability

SK ensures availability of Certificate Status Services 24 hours a day, 7 days a week with a minimum of 99.44% availability overall per year with a scheduled downtime that does not exceed 0.28% annually.

4.10.3 Operational Features

None.

4.11 End of Subscription

The maximum validity period for the Certificate is 1,125 days (3 years and 30 days).

The maximum validity period for the Certificate can be extended to 5 years if the Certificate is not used in publicly accessible systems.

The Subscriber may also end a subscription for the Certificate by revoking the Certificate without replacing it.

4.12 Key Escrow and Recovery

SK does not provide the Subscriber with key escrow and recovery services.

5. FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

Refer to clause 5 of SK PS [7].

5.1 Physical Controls

Refer to clause 5 of SK PS [7].

5.2 Procedural Controls

Refer to clause 5.2.1 of SK PS [7].

5.3 Personnel Controls

5.3.1 Qualifications, Experience, and Clearance Requirements

Refer to clause 5.3.1 of SK PS [7].

5.3.2 Background Check Procedures

Refer to clause 5.3.2 of SK PS [7].

5.3.3 Training Requirements

Refer to clause 5.3.3 of SK PS [7].

The employees of SK responsible for issuing the Certificate are required to pass an examination provided by SK on the issuance of the Certificate. The right to issue the Certificate is given on the basis of a decree issued by the CEO.

5.3.4 Retraining Frequency and Requirements

Refer to clause 5.3.4 of SK PS [7].

5.3.5 Job Rotation Frequency and Sequence

Refer to clause 5.3.5 of SK PS [7].

5.3.6 Sanctions for Unauthorized Actions

Refer to clause 5.3.6 of SK PS [7].

5.3.7 Independent Contractor Requirements

Refer to clause 5.3.7 of SK PS [7].

5.3.8 Documentation Supplied to Personnel

Refer to clause 5.3.8 of SK PS [7].

5.4 Audit Logging Procedures

5.4.1 Types of Events Recorded

Refer to clause 5.4.1 of SK PS [7].

If the private key of the Subscriber is generated by SK, an audit trail of events relating to the preparation of QSCD is kept.

5.4.2 Frequency of Processing Log

Refer to clause 5.4.2 of SK PS [7]

5.4.3 Retention Period for Audit Log

Refer to clause 5.4.3 of SK PS [7].

5.4.4 Protection of Audit Log

Refer to clause 5.4.4 of SK PS [7].

5.4.5 Audit Log Backup Procedures

Refer to clause 5.4.5 of SK PS [7].

5.4.6 Audit Collection System (Internal vs. External)

Refer to clause 5.4.6 of SK PS [7].

5.4.7 Notification to Event-Causing Subject

Refer to clause 5.4.7 of SK PS [7].

5.4.8 Vulnerability Assessments

Refer to clause 5.4.8 of SK PS [7].

5.5 Records Archival

5.5.1 Types of Records Archived

SK archives all recorded events as described in clause 5.4.1 of this CPS.

All physical records that are collected about issuance of the Certificate and other procedures are archived in accordance with relevant regulations.

5.5.2 Retention Period for Archive

Refer to clause 5.5.2 of SK PS [7].

5.5.3 Protection of Archive

Refer to clause 5.5.3 of SK PS [7].

5.5.4 Archive Backup Procedures

Refer to clause 5.5.4 of SK PS [7].

5.5.5 Requirements for Time-Stamping of Records

Refer to clause 5.5.5 of SK PS [7].

5.5.6 Archive Collection System (Internal or External)

Refer to clause 5.5.6 of SK PS [7].

5.5.7 Procedures to Obtain and Verify Archive Information

Refer to clause 5.5.7 of SK PS [7].

5.6 Key Changeover

The Public Key of KLASS3-SK 2010 does not change. The Public Key for the OCSP responder is sent inside the OCSP response, through which a change of key is known.

If necessary, details of a key changeover are considered each time. New CA certificate always contains a new distinguished name.

5.7 Compromise and Disaster Recovery

Refer to clause 5.7 of SK PS [7].

5.8 CA Termination

Refer to clause 5.8 of SK PS [7].

6. TECHNICAL SECURITY CONTROLS

6.1 Key Pair Generation and Installation

Refer to clause 6.1 of SK PS [7].

6.1.1 Key Pair Generation

Refer to clause 6.1.1 of SK PS [7], clause 6.1.1. the CP [2] and clause 6.1.1 the CP for TLS Server Certificates [3].

The Subscriber keys of TLS Server Certificates are generated by the Subscriber or on behalf of the Subscriber by the content delivery service provider.

If the Subscriber keys of an e-Seal Certificate are generated by the Subscriber in a QCSD, the Subscriber has responsibility for ensuring that the device is compliant throughout the validity period of the e-Seal Certificate and that the Private Key cannot be copied or extracted unencrypted from the device.

In case keys of e-Seal Certificates are generated by SK in a Secure Cryptographic Device or QSCD, SK warrants that no copies are made of the keys and keys are generated in the device. Key pair generation by SK is not performed without a Secure Cryptographic Device or QSCD.

6.1.2 Private Key Delivery to Subscriber

If the keys are generated by SK, the Private Keys are handed over to the Subscriber's legal representative or authorised person at the Customer Service Point or using a courier.

Prior a QSCD on which an e-Seal Certificate has been loaded is handed over to the Subscriber's legal representative or authorised person, the identity of the named persons is verified by the physical presence at the Customer Service Point. The Subscriber's legal representative or authorised person presents his/her identity document to an employee of the Customer Service Point who verifies the identity.

SK warrants the confidentiality and non-usage of the generated Private Keys and activation codes until the issuance of an e-Seal Certificate.

6.1.3 Public Key Delivery to Certificate Issuer

If the keys are generated by the Subscriber, the Public Key is delivered to SK over the public data network in the form of PKCS#10 [6] Certificate Signing Request.

6.1.4 CA Public Key Delivery to Relying Parties

Refer to clause 6.1.4 of SK PS [7].

6.1.5 Key Sizes

Refer to the Certificate Profile [5].

6.1.6 Public Key Parameters Generation and Quality Checking

Refer to clause 6.1.1 of this CPS.

In case the Public Key is provided by the Subscriber, it is checked against the list of Debian Weak Keys (CVE-2008-0166).

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

Key usage purposes are described in the Certificate Profile [5].

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic Module Standards and Controls

Refer to clause 6.2.1 of SK PS [7].

In case of TLS Certificate it is the Subscriber's responsibility to take adequate measures for protecting his/her Private Key.

In case of e-Seal Certificate on QSCD issued under policy QCP-l-qscd, the chip or the device that carries the Subscriber's Private Keys must be QSCD.

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

Refer to clause 6.2.2 of SK PS [7].

Multi-person control is not required for Subscriber keys.

6.2.3 Private Key Escrow

Refer to clause 6.2.3 of SK PS [7].

SK does not provide the Subscriber with key escrow and recovery services.

6.2.4 Private Key Backup

Refer to clause 6.2.4 of SK PS [7].

The Subscriber is responsible for backing up its Private Key.

If the Private Key is stored on a QSCD, the methods used for backup must not weaken the security of the Private Key.

6.2.5 Private Key Archival

Refer to clause 6.2.5 of SK PS [7].

The Subscriber is responsible for archiving its Private Key.

If the Private Key is stored on a QSCD, the methods used for archival must not weaken the security of the Private Key.

6.2.6 Private Key Transfer Into or From a Cryptographic Module

Refer to clause 6.2.6 of SK PS [7].

In case of TLS Server Certificate usage of Cryptographic Module is not required.

In case of e-Seal Certificate it is not allowed to store the Subscriber's keys outside of the QSCD or Secure Cryptographic Device except for backup, archiving or copying to another device in a way that does not weaken the security of the Private Keys and does not break the compliance required by CP [2].

6.2.7 Private Key Storage on Cryptographic Module

Refer to clause 6.2.7 of SK PS [7].

6.2.8 Method of Activating Private Key

Refer to clause 6.2.8 of SK PS [7].

It is responsibility of the Subscriber to take adequate means for protecting its Private Key.

6.2.9 Method of Deactivating Private Key

Refer to clause 6.2.9 of SK PS [7].

It is responsibility of the Subscriber to take adequate means for protecting its Private Key.

6.2.10 Method of Destroying Private Key

Refer to clause 6.2.9 of SK PS [7].

It is responsibility of the Subscriber to take adequate means for protecting its Private Key.

6.2.11 Cryptographic Module Rating

Refer to clause 6.2.1 of this CPS and clause 6.2.11 of SK PS [7].

6.3 Other Aspects of Key Pair Management

6.3.1 Public Key Archival

Refer to clause 6.3.1 of SK PS [7].

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

Refer to clause 6.3.2 of SK PS [7].

For the Certificate, the validity period is defined in clause 4.11 of this CPS.

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

Refer to clause 6.4.1 of SK PS [7].

If the Private Key of the Subscriber is generated by SK, this procedure also involves generating the necessary activation codes.

Activation codes generated by SK meet the following criteria:

- Contain numbers only;
- The length of the activation codes is at least 5 symbols;
- The length of the Admin password is at least 6 symbols;
- Do not contain more than 3 consecutive symbols (e.g. activation codes can contain “123”, but not “1234”);
- Do not contain more than 2 repetitive symbols (e.g. activation codes can contain “44”, but not “444”).

Otherwise it is the responsibility of the Subscriber to generate its activation codes.

6.4.2 Activation Data Protection

Refer to clause 6.4.2 of SK PS [7].

If the activation codes are generated by SK, they are delivered to the Subscriber via encrypted channel or handed over to the Subscriber in a closed envelope.

6.4.3 Other Aspects of Activation Data

Not applicable.

6.5 Computer Security Controls

Refer to clause 6.5.1 of SK PS [7].

6.6 Life Cycle Technical Controls

Refer to clause 6.6.1 of SK PS [7].

6.7 Network Security Controls

Refer to clause 6.7 of SK PS [7].

6.8 Time-Stamping

Refer to clause 6.8 of SK PS [7].

7. CERTIFICATE, CRL, AND OCSP PROFILES

7.1 Certificate Profile

The Certificate profile is described in the Certificate Profile [5], published in SK's public information repository https://www.sk.ee/en/repository/profiles/.

7.2 CRL Profile

The CRL profile is described in the Certificate Profile [5], published in SK's public information repository https://www.sk.ee/en/repository/profiles/.

7.3 OCSP Profile

The OCSP profile is described in the Certificate Profile [5], published in SK's public information repository https://www.sk.ee/en/repository/profiles/.

8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS

Refer to chapter 8 of SK PS [7].

9. OTHER BUSINESS AND LEGAL MATTERS

9.1 Fees

9.1.1 Certificate Issuance or Renewal Fees

The fees for the issuance of the Certificate are described in the corresponding price list, published on SK's website .

Certificate renewal is not performed.

9.1.2 Certificate Access Fees

Valid and activated certificates are available in LDAP directory. LDAP directory is free of charge and is accessible on ldap://ldap.sk.ee.

9.1.3 Revocation or Status Information Access Fees

Revocation of the Certificate is free of charge.

A valid CRL is free of charge and is accessible on SK's website .

An OCSP service for online verification is free of charge and publicly accessible.

In case of other manners of publication information on status of the Certificate, SK may set a fee in the price list or require a corresponding agreement.

9.1.4 Fees for Other Services

Fees for other services are specified in SK's price list or in the Subscriber's or Relying Party's agreement.

9.1.5 Refund Policy

Refer to clause 9.1.5 of SK PS [7].

The Subscriber may request refund in the form of modification of the Certificate within 14 days after initial issuance of the Certificate.

9.2 Financial Responsibility

9.2.1 Insurance Coverage

Refer to clause 9.2.1 of SK PS [7].

9.2.2 Other Assets

Not applicable.

9.2.3 Insurance or Warranty Coverage for End-Entities

Refer to clause 9.2.1 of SK PS [7].

9.3 Confidentiality of Business Information

Refer to clause 9.3 of SK PS [7].

9.4 Privacy of Personal Information

Refer to clause 9.4.3 of SK PS [7].

9.5 Intellectual Property Rights

SK obtains intellectual property rights to this CPS.

9.6 Representations and Warranties

9.6.1 CA Representations and Warranties

Refer to clause 9.6.1 of SK PS [7].

SK ensures that:

- the supply of the certification service is in accordance with the relevant legislation;
- the supply of the certification service is in accordance with this CPS, the CP [2] and the CP for TLS Server Certificates [3];
- it accepts and processes requests for the Certificate from the Subscriber over a secured communications channel;
- it accepts applications for suspension of certificates 24 hours a day;
- the certification keys are protected by HSM and are under sole control of SK;
- the certification keys used in the supply of the certification service are activated on the basis of shared control.

9.6.2 RA Representations and Warranties

9.6.2.1. Customer Service Point

Refer to clause 9.6.2 of SK PS [7].

The Customer Service Point hereby undertakes to:

- accept applications for the Certificate issuance and termination of suspension;
- accept applications for the Certificate suspension and revocation 24 hours a day, 7 days a week;
- verify the authenticity and integrity of the abovementioned requests;
- verify identity and authority of legal person and its representative.

9.6.3 Subscriber Representations and Warranties

The Subscriber observes the requirements provided by SK in this CPS.

Refer to clause 9.6.3 of SK PS [7].

The Subscriber has to accept the Terms and Conditions [4].

9.6.4 Relying Party Representations and Warranties

Refer to clause 9.6.4 of SK PS [7].

A Relying Party studies the risks and liabilities related to acceptance of the Certificate. The risks and liabilities have been set out in this CPS, the CP [2] and the CP for TLS Server Certificates [3].

9.6.5 Representations and Warranties of Other Participants

Not applicable.

9.7 Disclaimers of Warranties

Refer to clause 9.7 of SK PS [7].

9.8 Limitations of Liability

Refer to clause 9.8 of SK PS [7].

9.9 Indemnities

Indemnities between the Subscriber and SK are regulated in Terms and Conditions [4].

9.10 Term and Termination

9.10.1 Term

Refer to clause 2.2.1 of this CPS.

9.10.2 Termination

Refer to clause 9.10.2 of SK PS [7].

9.10.3 Effect of Termination and Survival

SK communicates the conditions and effect of the termination of this CPS via its public repository. The communication specifies which provisions survive termination.

At a minimum, all responsibilities related to protecting personal and confidential information, also maintenance of SK archives for determined period and logs survive termination. All Subscriber agreements remain effective until the Certificate is revoked or expired, even if this CPS terminates.

Termination of this CPS cannot occur before termination actions described in clause 5.8 of this CPS.

9.11 Individual Notices and Communications with Participants

The Subscriber's individual notices are communicated via the contact details (telephone number and/or email address) provided by the Subscriber during submitting an application for the Certificate.

9.12 Amendments

9.12.1 Procedure for Amendment

Refer to clause 1.5.4 of this CPS.

9.12.2 Notification Mechanism and Period

Refer to clause 2.2.1 of this CPS.

9.12.3 Circumstances Under Which OID Must be Changed

Not applicable.

9.13 Dispute Resolution Provisions

Refer to clause 9.13 of SK PS [7].

The Subscriber or other party can submit their claim or complaint at the email address info@sk.ee.

9.14 Governing Law

This CPS is governed by the jurisdictions of the European Union and Estonia.

9.15 Compliance with Applicable Law

Refer to clause 9.15 of SK PS [7].

Additionally, SK ensures compliance with the following requirements:

- CA/Browser Forum, Baseline Requirements Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates [8];
- Browser root certificate programs:
  - Microsoft Trusted Root Certificate: Program Requirements [9];
  - Mozilla CA Certificate Policy [10];
  - Apple Root Certificate Program [11].

9.16 Miscellaneous Provisions

9.16.1 Entire Agreement

SK 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 contains provisions that differ from this CPS, then the agreement with that party controls but solely with respect to that party. Third parties may not rely on or bring action to enforce any such agreement.

9.16.2 Assignment

Any entities operating under this CPS may not assign their rights or obligations without the prior written consent of SK. Unless specified otherwise in a contract with a party, SK does not provide notice of assignment.

9.16.3 Severability

If any provision of this CPS is held invalid or unenforceable by a competent court or tribunal, the remainder of the CPS remains valid and enforceable. Each provision of this CPS that provides for a limitation of liability, disclaimer of a warranty, or an exclusion of damages is severable and independent of any other provision.

9.16.4 Enforcement (Attorneys' Fees and Waiver of Rights)

SK may claim indemnification and attorneys' fees from a party for damages, losses, and expenses related to that party's conduct. SK's failure to enforce a provision of this CPS does

not waive SK's right to enforce the same provision later or right to enforce any other provision of this CPS. To be effective, waivers must be in writing and signed by SK.

9.16.5 Force Majeure

Refer to clause 9.16.5 of SK PS [7].

9.17 Other Provisions

Not applicable.

REFERENCES

[1] RFC 3647 – Request For Comments 3647, Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework;

[2] AS Sertifitseerimiskeskus - Certification Policy for Organisation Certificates, published: https://sk.ee/en/repository/CP/;

[3] AS Sertifitseerimiskeskus – Certification Policy for TLS Server Certificates, published: https://sk.ee/en/repository/CP/;

[4] Terms and Conditions of Use of Organisation Certificates, published: https://sk.ee/en/repository/conditions-for-use-of-certificates/;

[5] Certificate, CRL and OCSP Profile for Organisation Certificates Issued by SK, published: https://sk.ee/en/repository/profiles/;

[6] PKCS#10 – Certification Request Syntax Standard, published: http://www.emc.com/emc-plus/rsa-labs/standards-initiatives/pkcs10-certification-request-syntax-standard.htm;

[7] AS Sertifitseerimiskeskus Trust Services Practice Statement, published: https://sk.ee/en/repository/sk-ps/;

[8] CA/Browser Forum, Baseline Requirements Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates, published: https://cabforum.org/baseline-requirements-documents/;

[9] Microsoft Trusted Root Certificate: Program Requirements, published: https://technet.microsoft.com/en-us/library/cc751157.aspx;

[10] Mozilla CA Certificate Policy, published: https://www.mozilla.org/en-US/about/governance/policies/security-group/certs/policy/;

[11] Apple Root Certificate Program, published: https://www.apple.com/certificateauthority/ca_program.html;

[12] ETSI EN 319 411-2 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Policy requirements for certification authorities issuing qualified certificates;

[13] ETSI EN 319 411-1 Electronic Signatures and Infrastructures (ESI); Policy and Security requirements for Trust Service Providers issuing certificates; Part 1: General requirements;

[14] eIDAS - Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC;

[15] EN 419 211 Protection profiles for secure signature creation device – Part 1: Overview; Part 3: Device with key generation.