



AS Sertifitseerimiskeskus – Certificate Policy for TLS Server Certificates

Version 2.0
 OID: 1.3.6.1.4.1.10015.7.2
 3 February 2017

Version and Changes		
Date	Version	Changes
03.02.2017	2.0	Approved version -Chapter 1.1 – Removed paragraph which stated that the current document is a redesign of the previous “AS Sertifitseerimiskeskus – Certification Practice Statement” and “Certification Policy for Organisation Certificates”; -Chapter 1.2 - Removed “This is the first version of this document”; -Chapter 1.5.4 – Replaced “client” with the term “Subscriber”; added procedure for CP amendment in case of changes in compliance requirements; -Chapter 2.2.1 – Added that the CP and related documents can be published 30 days prior to taking effect; Chapter 3.2.2.4 – Removed CA’s obligation to verify that the domain name is resolvable by the public DNS service.
01.11.2016	1.1	Draft of version 2.0
1.07.2016	1.0	Approved version Chapter 3.2.2.4 – Added option 5 from section 3.2.2.4 of Baseline Requirements; Chapter 3.2.2.5 – Added option 4 from section 3.2.2.4 of Baseline Requirements; Chapter 4.10.2 – Added OCSP.
1.04.2016	0.1	Draft of version 1.0.

1. INTRODUCTION	9
1.1 Overview	9
1.2 Certificate Policy Name and Identification	10
1.3 PKI Participants	10
1.3.1 Certification Authorities	10
1.3.2 Registration Authorities	11
1.3.3 Subscribers	11



1.3.4 Relying Parties	11
1.3.5 Other Participants	11
1.4 Certificate Usage	11
1.4.1. Appropriate Certificate Uses	11
1.4.2 Prohibited Certificate Uses.....	11
1.5 Policy Administration	12
1.5.1 Organisation Administering the Document.....	12
1.5.2 Contact Person	12
1.5.3 Person Determining CPS Suitability for the Policy.....	12
1.5.4 CP Approval Procedures.....	12
1.6 Definitions and Acronyms	13
1.6.1 Terminology	13
1.6.2 Acronyms	14
2. PUBLICATION AND REPOSITORY RESPONSIBILITIES	14
2.1 Repositories	15
2.2 Publication of Certification Information	15
2.2.1 Publication and Notification Policies	15
2.2.2 Items not Published in the Certification Practice Statement	15
2.3 Time or Frequency of Publication	15
2.4 Access Controls on Repositories	15
3. IDENTIFICATION AND AUTHENTICATION.....	15
3.1 Naming	15
3.1.1 Types of Names	15
3.1.2 Need for Names to be Meaningful	16
3.1.3 Anonymity or Pseudonymity of Subscribers.....	16
3.1.4 Rules for Interpreting Various Name Forms.....	16
3.1.5 Uniqueness of Names	16
3.1.6 Recognition, Authentication, and Role of Trademarks.....	16
3.2 Initial Identity Validation	16
3.2.1 Method to Prove Possession of Private Key.....	16
3.2.2 Authentication of Organisation Identity	16
3.2.3 Authentication of Individual Identity.....	17
3.2.4 Non-Verified Subscriber Information	17
3.2.5 Validation of Authority	18



3.2.6	Criteria for Interoperation	18
3.3	Identification and Authentication for Re-Key Requests	18
3.3.1	Identification and Authentication for Routine Re-Key.....	18
3.3.2	Identification and Authentication for Re-Key after Revocation.....	18
3.4	Identification and Authentication for Revocation Request	18
4.	CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS.....	18
4.1	Certificate Application	19
4.1.1	Who Can Submit a Certificate Application	19
4.1.2	Enrollment Process and Responsibilities	19
4.2	Certificate Application Processing	19
4.2.1	Performing Identification and Authentication Functions	19
4.2.2	Approval or Rejection of Certificate Applications	19
4.2.3	Time to Process Certificate Applications.....	19
4.3	Certificate Issuance	19
4.3.1	CA Actions During Certificate Issuance.....	20
4.3.2	Notification to Subscriber by the CA of Issuance of Certificate	20
4.4	Certificate Acceptance.....	20
4.4.1	Conduct Constituting Certificate Acceptance	20
4.4.2	Publication of the Certificate by the CA.....	20
4.4.3	Notification of Certificate Issuance by the CA to Other Entities	20
4.5	Key Pair and Certificate Usage.....	20
4.5.1	Subscriber Private Key and Certificate Usage	20
4.5.2	Relying Party Public Key and Certificate Usage	20
4.6	Certificate Renewal.....	20
4.7	Certificate Re-Key.....	20
4.7.1	Circumstances for Certificate Re-Key.....	20
4.7.2	Who May Request Certification of a New Public Key	21
4.7.3	Processing Certificate Re-Keying Requests	21
4.7.4	Notification of New Certificate Issuance to Subscriber	21
4.7.5	Conduct Constituting Acceptance of a Re-Keyed Certificate.....	21
4.7.6	Publication of the Re-Keyed Certificate by the CA.....	21
4.7.7	Notification of Certificate Issuance by the CA to Other Entities	21
4.8	Certificate Modification	21
4.8.1	Circumstances for Certificate Modification	21



4.8.2	Who May Request Certificate Modification	21
4.8.3	Processing Certificate Modification Requests	22
4.8.4	Notification of New Certificate Issuance to Subscriber	22
4.8.5	Conduct Constituting Acceptance of Modified Certificate	22
4.8.6	Publication of the Modified Certificate by the CA	22
4.8.7	Notification of Certificate Issuance by the CA to Other Entities	22
4.9	Certificate Revocation and Suspension	22
4.9.1	Circumstances for Revocation	22
4.9.2	Who Can Request Revocation	22
4.9.3	Procedure for Revocation Request	22
4.9.4	Revocation Request Grace Period	22
4.9.5	Time Within Which CA Must Process the Revocation Request	22
4.9.6	Revocation Checking Requirements for Relying Parties	23
4.9.7	CRL Issuance Frequency	23
4.9.8	Maximum Latency for CRLs	23
4.9.9	On-Line Revocation/Status Checking Availability	23
4.9.10	On-Line Revocation Checking Requirements	23
4.9.11	Other Forms of Revocation Advertisements Available	23
4.9.12	Special Requirements Related to Key Compromise	23
4.9.13	Circumstances for Suspension	23
4.9.14	Who Can Request Suspension	23
4.9.15	Procedure for Suspension Request	23
4.9.16	Limits on Suspension Period	23
4.9.17	Circumstances for Termination of Suspension	24
4.9.18	Who Can Request Termination of Suspension	24
4.9.19	Procedure for Termination of Suspension	24
4.10	Certificate Status Services	24
4.10.1	Operational Characteristics	24
4.10.2	Service Availability	24
4.10.3	Optional Features	24
4.11	End of Subscription	24
4.12	Key Escrow and Recovery	24
4.12.1	Key Escrow and Recovery Policy and Practices	24
4.12.2	Session Key Encapsulation and Recovery Policy and Practices	24



5. FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS.....	25
5.1 Physical Controls	25
5.1.1 Site Location and Construction	25
5.1.2 Physical Access	25
5.1.3 Power and Air Conditioning.....	25
5.1.4 Water Exposures.....	25
5.1.5 Fire Prevention and Protection.....	25
5.1.6 Media Storage	25
5.1.7 Waste Disposal	25
5.1.8 Off-Site Backup	25
5.2 Procedural Controls	26
5.2.1 Trusted Roles.....	26
5.2.2 Number of Persons Required per Task.....	26
5.2.3 Identification and Authentication for Each Role	26
5.2.4 Roles Requiring Separation of Duties	26
5.3 Personnel Controls	26
5.3.1 Qualifications, Experience, and Clearance Requirements.....	26
5.3.2 Background Check Procedures	26
5.3.3 Training Requirements.....	26
5.3.4 Retraining Frequency and Requirements	26
5.3.5 Job Rotation Frequency and Sequence	26
5.3.6 Sanctions for Unauthorized Actions	26
5.3.7 Independent Contractor Requirements	27
5.3.8 Documentation Supplied to Personnel.....	27
5.4 Audit Logging Procedures	27
5.4.1 Types of Events Recorded.....	27
5.4.2 Frequency of Processing Log	27
5.4.3 Retention Period for Audit Log	27
5.4.4 Protection of Audit Log.....	27
5.4.5 Audit Log Backup Procedures.....	27
5.4.6 Audit Collection System (Internal vs. External)	27
5.4.7 Notification to Event-Causing Subject.....	27
5.4.8 Vulnerability Assessments	27
5.5 Records Archival.....	28



5.5.1	Types of Records Archived	28
5.5.2	Retention Period for Archive	28
5.5.3	Protection of Archive	28
5.5.4	Archive Backup Procedures	28
5.5.5	Requirements for Time-Stamping of Records	28
5.5.6	Archive Collection System (Internal or External)	28
5.5.7	Procedures to Obtain and Verify Archive Information	28
5.6	Key Changeover	28
5.7	Compromise and Disaster Recovery	28
5.7.1	Incident and Compromise Handling Procedures	28
5.7.2	Computing Resources, Software, and/or Data are Corrupted	28
5.7.3	Entity Private Key Compromise Procedures	29
5.7.4	Business Continuity Capabilities After a Disaster	29
5.8	CA Termination	29
6.	TECHNICAL SECURITY CONTROLS	29
6.1	Key Pair Generation and Installation	29
6.1.1	Key Pair Generation	29
6.1.2	Private Key Delivery to Subscriber	29
6.1.3	Public Key Delivery to Certificate Issuer	29
6.1.4	CA Public Key Delivery to Relying Parties	29
6.1.5	Key Sizes	29
6.1.6	Public Key Parameters Generation and Quality Checking	29
6.1.7	Key Usage Purposes (as per X.509 v3 Key Usage Field)	30
6.2	Private Key Protection and Cryptographic Module Engineering Controls	30
6.2.1	Cryptographic Module Standards and Controls	30
6.2.2	Private Key (n out of m) Multi-Person Control	30
6.2.3	Private Key Escrow	30
6.2.4	Private Key Backup	30
6.2.5	Private Key Archival	30
6.2.6	Private Key Transfer Into or From a Cryptographic Module	30
6.2.7	Private Key Storage on Cryptographic Module	30
6.2.8	Method of Activating Private Key	30
6.2.9	Method of Deactivating Private Key	30
6.2.10	Method of Destroying Private Key	31



6.2.11 Cryptographic Module Rating.....	31
6.3 Other Aspects of Key Pair Management	31
6.3.1 Public Key Archival	31
6.3.2 Certificate Operational Periods and Key Pair Usage Periods.....	31
6.4 Activation Data.....	31
6.4.1 Activation Data Generation and Installation	31
6.4.2 Activation Data Protection	31
6.4.3 Other Aspects of Activation Data	31
6.5 Computer Security Controls.....	31
6.5.1 Specific Computer Security Technical Requirements	31
6.5.2 Computer Security Rating	31
6.6 Life Cycle Technical Controls	32
6.6.1 System Development Controls.....	32
6.6.2 Security Management Controls	32
6.6.3 Life Cycle Security Controls	32
6.7 Network Security Controls	32
6.8 Time-Stamping	32
7. CERTIFICATE, CRL, AND OCSP PROFILES	32
7.1 Certificate Profile	32
7.2 CRL Profile	32
7.3 OCSP Profile	32
7.3.1 Version Number(s)	33
7.3.2 OCSP Extensions	33
8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS.....	33
8.1 Frequency or Circumstances of Assessment	33
8.2 Identity/Qualifications of Assessor	33
8.3 Assessor's Relationship to Assessed Entity	33
8.4 Topics Covered by Assessment	33
8.5 Actions Taken as a Result of Deficiency	33
8.6 Communication of Results.....	33
9. OTHER BUSINESS AND LEGAL MATTERS	33
9.1 Fees.....	34
9.1.1 Certificate Issuance or Renewal Fees	34
9.1.2 Certificate Access Fees	34



9.1.3 Revocation or Status Information Access Fees	34
9.1.4 Fees for Other Services	34
9.1.5 Refund Policy	34
9.2 Financial Responsibility	34
9.2.1 Insurance Coverage	34
9.2.2 Other Assets	34
9.2.3 Insurance or Warranty Coverage for End-Entities	34
9.3 Confidentiality of Business Information.....	34
9.4 Privacy of Personal Information.....	35
9.4.1 Personal Data Protection Principles.....	35
9.4.2 Personal Information Processed by SK	35
9.4.3 Responsibility to Protect Private Information	35
9.4.4 Notice and Consent to Use Private Information	35
9.4.5 Disclosure Pursuant to Judicial or Administrative Process	35
9.4.6 Other Information Disclosure Circumstances.....	35
9.5 Intellectual Property Rights.....	35
9.6 Representations and Warranties	35
9.6.1 CA Representations and Warranties.....	35
9.6.2 RA Representations and Warranties.....	35
9.6.3 Subscriber Representations and Warranties	35
9.6.4 Relying Party Representations and Warranties	36
9.6.5 Representations and Warranties of Other Participants.....	36
9.7 Disclaimers of Warranties.....	36
9.8 Limitations of Liability.....	36
9.9 Indemnities	36
9.10 Term and Termination	36
9.10.1 Term.....	36
9.10.2 Termination	36
9.10.3 Effect of Termination and Survival	36
9.11 Individual Notices and Communications with Participants.....	37
9.12 Amendments.....	37
9.12.1 Procedure for Amendment.....	37
9.12.2 Notification Mechanism and Period.....	37
9.12.3 Circumstances Under Which OID Must be Changed.....	37



9.13 Dispute Resolution Provisions	37
9.14 Governing Law.....	37
9.15 Compliance with Applicable Law.....	37
9.16 Miscellaneous Provisions	38
9.16.1 Entire Agreement	38
9.16.2 Assignment	38
9.16.3 Severability.....	38
9.16.4 Enforcement (Attorneys' Fees and Waiver of Rights)	38
9.16.5 Force Majeure	38
9.17 Other Provisions	38

1. INTRODUCTION

1.1 Overview

This document "AS Sertifitseerimiskeskus – Certificate Policy for TLS Server Certificates" (CP) defines the procedural and operational requirements that Sertifitseerimiskeskus (SK) adheres to and requires entities to adhere to when issuing and managing TLS Server Certificates.

This document only describes the restrictions to Organizational Validation Certificate Policy (OVCP) from ETSI EN 319 411-1 [1] ("OVCP"), which also includes CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates ("Baseline Requirements"). The requirements of Browser root program from Microsoft [3], Mozilla [4] and Apple [5] ("Browser root program requirements") apply.

The semantics of "no stipulation" in this document means that no additional restrictions are set and relevant provisions from OVCP, Baseline Requirements and Browser root program requirements are applied directly.

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

- Browser root program requirements;
- Baseline Requirements;
- OVCP;
- This CP;
- CPS.

Pursuant to the IETF RFC 3647 [7] this CP is divided into nine parts. To preserve the outline specified by RFC 3647 [7], 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 [1]. References to Baseline Requirements [2] are not included since both documents follow the structure of IETF RFC 3647 [7] and each reference would be to the section with the same number.

In this CP "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "MAY" and so on are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions) [6].

1.2 Certificate Policy Name and Identification

Refer to clause 5.3 of ETSI EN 319 411-1 [1].

This document is called "AS Sertifitseerimiskeskus – Certificate Policy for TLS Server Certificates".

This CP is identified by OID: 1.3.6.1.4.1.10015.7.2

OID is composed according to the contents of the following table 1.

Parameter	OID reference
Internet attribute	1.3.6.1
Private entity attribute	4
Registered business attribute given by private business manager IANA	1
SK attribute in IANA register	10015
Certification service attribute	7.2

The certificates issued to Subscribers SHALL include OIDs of the following policies:

- ETSI EN 319 411-1 [1] clause 5.3 f) for OVCP: Organizational Validation Certificate Policy
- Baseline Requirements [2] clause 1.2 for organization-validated Certificates
- This CP.

1.3 PKI Participants

Refer to clause 5.4 of ETSI EN 319 411-1 [1].

1.3.1 Certification Authorities

No stipulation.

1.3.2 Registration Authorities

No stipulation.

1.3.3 Subscribers

Subscriber is the subject of the Certificate issued under this CP.

Subscriber can be only a legal person registered in:

- a) the Estonian, Latvian, Lithuanian, Finnish or Swedish Business Register and is discoverable from the European Business Register; or
- b) the Estonian Non-Profit Associations and Foundations Register; or
- c) the Estonian Register of State and Local Government Organisations.

Subscriber SHALL be owner of the domain or IP address for which the Certificate is requested.

1.3.4 Relying Parties

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

1.3.5 Other Participants

Not allowed.

1.4 Certificate Usage

Refer to clause 5.5 of ETSI EN 319 411-1 [1].

1.4.1. Appropriate Certificate Uses

The Subscriber Certificates are intended for proving the identity of web servers or other types of TLS servers in the public Internet.

CA Private Keys SHALL NOT be used to sign Certificates except the following:

- Subscriber Certificates;
- Certificates for Time-Stamping;
- OCSP Response verification Certificates;
- Internal Certificates for its own technical needs.

1.4.2 Prohibited Certificate Uses

Subscriber Certificates SHALL NOT be used for:



- Unlawful activity (including cyber attacks and attempts to damage the certificate);
- Issuance of new certificates and information on certificate validity.

1.5 Policy Administration

1.5.1 Organisation Administering the Document

This CP 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

No stipulation.

1.5.4 CP Approval Procedures

Amendments which do not change the meaning of the CP, 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 shall be enlarged.

In the case of substantial changes, the new CP version is clearly distinguishable from the previous ones. The new version bears a serial number enlarged by one. The amended CP 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 CP shall be published electronically on SK's website, otherwise the amendment is withdrawn.

In the case of changes in compliance requirements, the new CP version is clearly distinguishable from the previous ones. The new version bears a serial number enlarged by

one. The amended CP along with the enforcement date, which cannot be earlier than 30 days after publication, is published electronically on SK’s website.

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

1.6 Definitions and Acronyms

1.6.1 Terminology

In this CP the following terms have the following meaning.

Term	Definition
Authentication	Unique identification of a person by checking his/her alleged identity.
Browser root program requirements	Requirements for Browser root program from Microsoft [3], Mozilla [4] and Apple [5].
Certificate	Within the meaning of this CP, the term “Certificate” stands for TLS Server Certificate.
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 Certificates.
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.
Object Identifier	An identifier used to name an object (OID).
TLS Server Certificate	Certificate issued to TLS server (HTTPS, IMAPS, FTPS, etc.) for proof of authenticity of TLS server owner.
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.
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.
Subscriber	Legal person bound by agreement with CA to any subscriber obligations.
Terms and Conditions	Document that describes the obligations and responsibilities of the Subscriber while using the TLS Server Certificates. The Subscriber has to be familiar with the document and accept the terms and conditions described within when receiving the certificates.

1.6.2 Acronyms

Acronym	Definition
CA	Certification Authority
CP	Certificate Policy for TLS Server Certificates
CPS	Certification Practice Statement of KLASS3-SK 2010
CRL	Certificate Revocation List
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 [11]
gTLD	Generic top-level domain
IANA	The Internet Assigned Numbers Authority
ICANN	Internet Corporation for Assigned Names and Numbers
OID	Object Identifier, a unique object identification code
PKI	Public Key Infrastructure
RA	Registration Authority
SK	AS Sertifitseerimiskeskus, provider of the certification service
SK PS	AS Sertifitseerimiskeskus Trust Services Practice Statement [14]

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES

Refer to clause 6.1 of ETSI EN 319 411-1 [1].



2.1 Repositories

SK SHALL ensure that its repository is available 24 hours a day, 7 days a week with a minimum of 99% availability overall per year with a scheduled down-time that does not exceed 0.5% annually.

2.2 Publication of Certification Information

2.2.1 Publication and Notification Policies

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

This CP and referred documents – the CPS [8] and Certificate, CRL and OCSP Profile for Organisation Certificates Issued by SK (hereinafter Certificate Profile) [9] as well as the Terms and Conditions [10] with the enforcement dates SHALL be published no less than 30 days before taking effect.

2.2.2 Items not Published in the Certification Practice Statement

No stipulation.

2.3 Time or Frequency of Publication

No stipulation.

2.4 Access Controls on Repositories

No stipulation.

3. IDENTIFICATION AND AUTHENTICATION

Refer to clause 6.2 of ETSI EN 319 411-1 [1].

3.1 Naming

The Distinguished Name of the TLS Server Certificate SHALL be compiled in accordance with the Certificate Profile [9].

3.1.1 Types of Names

No stipulation.

3.1.2 Need for Names to be Meaningful

The following values in Subscriber information of the certificate SHALL be meaningful:

- Organization (O);
- Common Name (CN)
- Subject Alternative Name (SAN).

3.1.3 Anonymity or Pseudonymity of Subscribers

Not allowed.

3.1.4 Rules for Interpreting Various Name Forms

No stipulation.

3.1.5 Uniqueness of Names

SK SHALL NOT issue the Certificate with an identical Subscriber's Distinguished Name to different Subscribers.

3.1.6 Recognition, Authentication, and Role of Trademarks

No stipulation.

3.2 Initial Identity Validation

CA can use any legal means of communication or investigation to ascertain the identity of a natural or legal persons. CA MAY refuse to issue a Certificate in its sole discretion.

3.2.1 Method to Prove Possession of Private Key

No stipulation.

3.2.2 Authentication of Organisation Identity

CA SHALL verify that the Subscriber is registered in:

- a) the Estonian, Latvian, Lithuanian, Finnish or Swedish Business Register and is discoverable from the European Business Register; or
- b) the Estonian Non-Profit Associations and Foundations Register; or
- c) the Estonian Register of State and Local Government Organisations.



3.2.2.1. Identity

The identity and legal authority of the representative of the Subscriber SHALL be verified from the registries listed in 3.2.2.

3.2.2.2. DBA/Tradename

No stipulation.

3.2.2.3. Verification of Country

No stipulation.

3.2.2.4. Authorization by Domain Name Registrant

Only options 1, 3 and 5 from section 3.2.2.4 of Baseline Requirements [2] are allowed.

The CA SHALL only accept requests for domains or IP addresses for which data is discoverable from the IANA's registry.

3.2.2.5. Authentication for an IP Address

Only options 2 and 4 from section 3.2.2.5 of Baseline Requirements [2] are allowed.

3.2.2.6. Wildcard Domain Validation

Not allowed.

3.2.2.7. Data Source Accuracy

Only data sources mentioned in previous subsections of section 3.2 are allowed.

3.2.3 Authentication of Individual Identity

Not allowed.

3.2.4 Non-Verified Subscriber Information

The following values in the Subscriber information of the Certificate MAY be non-verified:

- Organizational Unit (OU);
- Locality (L);

- State (ST).

3.2.5 Validation of Authority

The CA SHALL verify that the application is signed by:

- a) a legal representative with the power to sign documents on behalf of the Subscriber;
or
- b) a person authorised by the legal representative by digital signature; or
- c) the contact person listed in the domain registrant's records.

If the representative is authorised with a letter of attorney, the CA SHALL verify that the letter is signed by:

- a) the person with the power to sign on behalf of the Subscriber or
- b) the person who signed the certificate application.

3.2.6 Criteria for Interoperation

Not allowed.

3.3 Identification and Authentication for Re-Key Requests

3.3.1 Identification and Authentication for Routine Re-Key

Refer to clause 3.2 of this CP.

3.3.2 Identification and Authentication for Re-Key after Revocation

No stipulation.

3.4 Identification and Authentication for Revocation Request

No stipulation.

4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

Refer to clause 6.3 of ETSI EN 319 411-1 [1].



4.1 Certificate Application

4.1.1 Who Can Submit a Certificate Application

No stipulation.

4.1.2 Enrollment Process and Responsibilities

Only digitally signed applications SHALL be accepted.

If the legal person's representative does not have the ability to digitally sign the certificate application in the meaning of eIDAS [11], SK MAY adopt additional checks prior to the certificate issuance.

4.2 Certificate Application Processing

At least two employees of the CA SHALL review each Certificate application before the Certificate is issued. Automated processes for issuance SHALL NOT be used.

4.2.1 Performing Identification and Authentication Functions

The CA SHALL verify that:

- a) the Subscriber is not bankrupt or in the process of liquidation; and
- b) its activities SHALL NOT be suspended or in other similar state in according to the legislation of its country of origin.

4.2.2 Approval or Rejection of Certificate Applications

The CA SHALL NOT issue Certificates containing a new gTLD under consideration by ICANN.

The CA SHALL NOT issue Certificates for IP addresses that are marked as "reserved" by IANA.

4.2.3 Time to Process Certificate Applications

The CA SHALL process certificate applications within 5 working days after receiving all the necessary documentation from the Subscriber.

4.3 Certificate Issuance

At least two employees of the CA SHALL review each issued Certificate to ascertain whether the Certificate complies with the application prior to notifying the Subscriber of issuance.

4.3.1 CA Actions During Certificate Issuance

No stipulation.

4.3.2 Notification to Subscriber by the CA of Issuance of Certificate

No stipulation.

4.4 Certificate Acceptance

4.4.1 Conduct Constituting Certificate Acceptance

No stipulation.

4.4.2 Publication of the Certificate by the CA

No stipulation.

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

No stipulation.

4.5 Key Pair and Certificate Usage

4.5.1 Subscriber Private Key and Certificate Usage

No stipulation.

4.5.2 Relying Party Public Key and Certificate Usage

No stipulation.

4.6 Certificate Renewal

Not allowed.

4.7. Certificate Re-Key

No stipulation.

4.7.1 Circumstances for Certificate Re-Key

No stipulation.



4.7.2 Who May Request Certification of a New Public Key

No stipulation.

4.7.3 Processing Certificate Re-Keying Requests

No stipulation.

4.7.4 Notification of New Certificate Issuance to Subscriber

No stipulation.

4.7.5 Conduct Constituting Acceptance of a Re-Keyed Certificate

No stipulation.

4.7.6 Publication of the Re-Keyed Certificate by the CA

No stipulation.

4.7.7 Notification of Certificate Issuance by the CA to Other Entities

Not allowed.

4.8 Certificate Modification

Certificate modification is allowed only for fixing errors in the Certificate within 14 days after initial issuance of the Certificate.

Before Certificate modification the erroneous Certificate SHALL be revoked.

Certificate modification MAY be performed based on the initial application.

Modification requests that are made more than 14 days after initial issuance SHALL be considered as new applications and procedures for initial issuance SHALL be followed..

4.8.1 Circumstances for Certificate Modification

Certificate modification is only allowed for fixing errors in the certificate.

4.8.2 Who May Request Certificate Modification

Only the Subscriber or the CA MAY request Certificate modification.



4.8.3 Processing Certificate Modification Requests

No stipulation.

4.8.4 Notification of New Certificate Issuance to Subscriber

No stipulation.

4.8.5 Conduct Constituting Acceptance of Modified Certificate

No stipulation.

4.8.6 Publication of the Modified Certificate by the CA

No stipulation.

4.8.7 Notification of Certificate Issuance by the CA to Other Entities

No stipulation.

4.9 Certificate Revocation and Suspension

4.9.1 Circumstances for Revocation

No stipulation.

4.9.2 Who Can Request Revocation

No stipulation.

4.9.3 Procedure for Revocation Request

No stipulation.

4.9.4 Revocation Request Grace Period

No stipulation.

4.9.5 Time Within Which CA Must Process the Revocation Request

No stipulation.

4.9.6 Revocation Checking Requirements for Relying Parties

No stipulation.

4.9.7 CRL Issuance Frequency

No stipulation.

4.9.8 Maximum Latency for CRLs

No stipulation.

4.9.9 On-Line Revocation/Status Checking Availability

No stipulation.

4.9.10 On-Line Revocation Checking Requirements

No stipulation.

4.9.11 Other Forms of Revocation Advertisements Available

No stipulation.

4.9.12 Special Requirements Related to Key Compromise

No stipulation.

4.9.13 Circumstances for Suspension

Suspension is not allowed.

4.9.14 Who Can Request Suspension

Not applicable.

4.9.15 Procedure for Suspension Request

Not applicable.

4.9.16 Limits on Suspension Period

Not applicable.



4.9.17 Circumstances for Termination of Suspension

Not applicable.

4.9.18 Who Can Request Termination of Suspension

Not applicable.

4.9.19 Procedure for Termination of Suspension

Not applicable.

4.10 Certificate Status Services

4.10.1 Operational Characteristics

No stipulation.

4.10.2 Service Availability

SK SHALL ensure that its CRL and OCSP is available 24 hours a day, 7 days a week with a minimum of 99% availability overall per year with a scheduled down-time that does not exceed 0.5% annually.

4.10.3 Optional Features

No stipulation.

4.11 End of Subscription

No stipulation.

4.12 Key Escrow and Recovery

4.12.1 Key Escrow and Recovery Policy and Practices

Not allowed.

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

Not applicable.



5. FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

Refer to clause 6.4 of ETSI EN 319 411-1 [1].

5.1 Physical Controls

5.1.1 Site Location and Construction

No stipulation.

5.1.2 Physical Access

No stipulation.

5.1.3 Power and Air Conditioning

No stipulation.

5.1.4 Water Exposures

No stipulation.

5.1.5 Fire Prevention and Protection

No stipulation.

5.1.6 Media Storage

No stipulation.

5.1.7 Waste Disposal

No stipulation.

5.1.8 Off-Site Backup

No stipulation.



5.2 Procedural Controls

5.2.1 Trusted Roles

No stipulation.

5.2.2 Number of Persons Required per Task

No stipulation.

5.2.3 Identification and Authentication for Each Role

No stipulation.

5.2.4 Roles Requiring Separation of Duties

No stipulation.

5.3 Personnel Controls

5.3.1 Qualifications, Experience, and Clearance Requirements

No stipulation.

5.3.2 Background Check Procedures

No stipulation.

5.3.3 Training Requirements

No stipulation.

5.3.4 Retraining Frequency and Requirements

No stipulation.

5.3.5 Job Rotation Frequency and Sequence

No stipulation.

5.3.6 Sanctions for Unauthorized Actions

No stipulation.

5.3.7 Independent Contractor Requirements

No stipulation.

5.3.8 Documentation Supplied to Personnel

No stipulation.

5.4 Audit Logging Procedures

5.4.1 Types of Events Recorded

No stipulation.

5.4.2 Frequency of Processing Log

No stipulation.

5.4.3 Retention Period for Audit Log

No stipulation.

5.4.4 Protection of Audit Log

No stipulation.

5.4.5 Audit Log Backup Procedures

No stipulation.

5.4.6 Audit Collection System (Internal vs. External)

No stipulation.

5.4.7 Notification to Event-Causing Subject

No stipulation.

5.4.8 Vulnerability Assessments

No stipulation.

5.5 Records Archival

5.5.1 Types of Records Archived

No stipulation.

5.5.2 Retention Period for Archive

No stipulation.

5.5.3 Protection of Archive

No stipulation.

5.5.4 Archive Backup Procedures

No stipulation.

5.5.5 Requirements for Time-Stamping of Records

No stipulation.

5.5.6 Archive Collection System (Internal or External)

No stipulation.

5.5.7 Procedures to Obtain and Verify Archive Information

No stipulation.

5.6 Key Changeover

No stipulation.

5.7 Compromise and Disaster Recovery

5.7.1 Incident and Compromise Handling Procedures

No stipulation.

5.7.2 Computing Resources, Software, and/or Data are Corrupted

No stipulation.



5.7.3 Entity Private Key Compromise Procedures

No stipulation.

5.7.4 Business Continuity Capabilities After a Disaster

No stipulation.

5.8 CA Termination

No stipulation.

6. TECHNICAL SECURITY CONTROLS

6.1 Key Pair Generation and Installation

Refer to clause 6.5 of ETSI EN 319 411-1 [1].

6.1.1 Key Pair Generation

The Subscriber keys SHALL be generated by the Subscriber or on behalf of the Subscriber by the content delivery service provider.

6.1.2 Private Key Delivery to Subscriber

No stipulation.

6.1.3 Public Key Delivery to Certificate Issuer

No stipulation.

6.1.4 CA Public Key Delivery to Relying Parties

No stipulation.

6.1.5 Key Sizes

Allowed key sizes SHALL be as described in the Certificate Profile [9].

6.1.6 Public Key Parameters Generation and Quality Checking



No stipulation.

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

No stipulation.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic Module Standards and Controls

No stipulation.

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

No stipulation.

6.2.3 Private Key Escrow

No stipulation.

6.2.4 Private Key Backup

No stipulation.

6.2.5 Private Key Archival

No stipulation.

6.2.6 Private Key Transfer Into or From a Cryptographic Module

No stipulation.

6.2.7 Private Key Storage on Cryptographic Module

No stipulation.

6.2.8 Method of Activating Private Key

No stipulation.

6.2.9 Method of Deactivating Private Key

No stipulation.

6.2.10 Method of Destroying Private Key

No stipulation.

6.2.11 Cryptographic Module Rating

No stipulation.

6.3 Other Aspects of Key Pair Management

6.3.1 Public Key Archival

No stipulation.

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

The validity period of Subscriber certificates SHALL be as defined in the Certificate Profile [9].

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

No stipulation.

6.4.2 Activation Data Protection

No stipulation.

6.4.3 Other Aspects of Activation Data

Not allowed.

6.5 Computer Security Controls

6.5.1 Specific Computer Security Technical Requirements

No stipulation.

6.5.2 Computer Security Rating

No stipulation.

6.6 Life Cycle Technical Controls

6.6.1 System Development Controls

No stipulation.

6.6.2 Security Management Controls

No stipulation.

6.6.3 Life Cycle Security Controls

No stipulation.

6.7 Network Security Controls

No stipulation.

6.8 Time-Stamping

No stipulation.

7. CERTIFICATE, CRL, AND OCSP PROFILES

Refer to clause 6.6 of ETSI EN 319 411-1 [1].

7.1 Certificate Profile

Certificate SHALL be compliant with the profile described in the Certificate Profile [9] .

7.2 CRL Profile

CRL SHALL be compliant to with the profile described in the Certificate Profile [9].

7.3 OCSP Profile

The OCSP responses SHALL be compliant with the profile described in the Certificate Profile [9].

7.3.1 Version Number(s)

No stipulation.

7.3.2 OCSP Extensions

No stipulation.

8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS

Refer to clause 6.7 of ETSI EN 319 411-1 [1].

8.1 Frequency or Circumstances of Assessment

No stipulation.

8.2 Identity/Qualifications of Assessor

No stipulation.

8.3 Assessor's Relationship to Assessed Entity

No stipulation.

8.4 Topics Covered by Assessment

No stipulation.

8.5 Actions Taken as a Result of Deficiency

No stipulation.

8.6 Communication of Results

No stipulation.

9. OTHER BUSINESS AND LEGAL MATTERS

Refer to clause 6.8 of ETSI EN 319 411-1 [1].



9.1 Fees

9.1.1 Certificate Issuance or Renewal Fees

The CA MAY charge a fee for the issuance of the certificate according to its price list.

9.1.2 Certificate Access Fees

No stipulation.

9.1.3 Revocation or Status Information Access Fees

No stipulation.

9.1.4 Fees for Other Services

No stipulation.

9.1.5 Refund Policy

No stipulation.

9.2 Financial Responsibility

9.2.1 Insurance Coverage

No stipulation.

9.2.2 Other Assets

No stipulation.

9.2.3 Insurance or Warranty Coverage for End-Entities

No stipulation.

9.3 Confidentiality of Business Information

No stipulation.



9.4 Privacy of Personal Information

9.4.1 Personal Data Protection Principles

No stipulation.

9.4.2 Personal Information Processed by SK

No stipulation.

9.4.3 Responsibility to Protect Private Information

No stipulation.

9.4.4 Notice and Consent to Use Private Information

No stipulation.

9.4.5 Disclosure Pursuant to Judicial or Administrative Process

No stipulation.

9.4.6 Other Information Disclosure Circumstances

No stipulation.

9.5 Intellectual Property Rights

SK obtains intellectual property rights to this CP.

9.6 Representations and Warranties

9.6.1 CA Representations and Warranties

An employee of CA SHALL NOT have been punished for an intentional crime.

9.6.2 RA Representations and Warranties

An employee of RA SHALL NOT have been punished for an intentional crime.

9.6.3 Subscriber Representations and Warranties

No stipulation.



9.6.4 Relying Party Representations and Warranties

A Relying Party SHALL verify the validity of the certificate using validation services offered by SK before using the certificate.

A Relying Party SHALL follow the limitations stated in the certificate and SHALL make sure that the transaction to be accepted corresponds to this CP.

9.6.5 Representations and Warranties of Other Participants

No stipulation.

9.7 Disclaimers of Warranties

No stipulation.

9.8 Limitations of Liability

No stipulation.

9.9 Indemnities

No stipulation.

9.10 Term and Termination

9.10.1 Term

Refer to clause 2.2.1 of this CP.

9.10.2 Termination

This CP SHALL remain in force until it is replaced by the new version or when it is terminated due to CA termination or when the service is terminated and all the Certificates therefore become invalid.

9.10.3 Effect of Termination and Survival

SK SHALL communicate the conditions and effect of this CP's termination.

9.11 Individual Notices and Communications with Participants

No stipulation.

9.12 Amendments

9.12.1 Procedure for Amendment

Refer to clause 1.5.4 of this CP.

9.12.2 Notification Mechanism and Period

Refer to clause 1.5.4 of this CP.

9.12.3 Circumstances Under Which OID Must be Changed

OID SHALL change when the scope of this Policy will change or when a new type of Certificate will occur.

9.13 Dispute Resolution Provisions

No stipulation.

9.14 Governing Law

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

9.15 Compliance with Applicable Law

The CA SHALL ensure compliance with following requirements:

- 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 [11];
- Personal Data Protection Act [12];
- Related European Standards:
 - ETSI EN 319 401 Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers [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 [1];

- CA/Browser Forum, Baseline Requirements Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates [2];
- Browser root certificate programs:
 - Microsoft Trusted Root Certificate: Program Requirements [3];
 - Mozilla CA Certificate Inclusion Policy [4];
 - Apple Root Certificate Program [5].

9.16 Miscellaneous Provisions

9.16.1 Entire Agreement

No stipulation.

9.16.2 Assignment

No stipulation.

9.16.3 Severability

No stipulation.

9.16.4 Enforcement (Attorneys' Fees and Waiver of Rights)

No stipulation.

9.16.5 Force Majeure

No stipulation.

9.17 Other Provisions

Not allowed.

REFERENCES

- [1] ETSI EN 319 411-1 V1.1.0 Electronic Signatures and Infrastructures (ESI); Policy and Security requirements for Trust Service Providers issuing certificates; Part 1: General requirements;
- [2] CA/Browser Forum Baseline Requirements Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates (V 1.4.1), published: <https://cabforum.org/baseline-requirements-documents/>;
- [3] Microsoft Trusted Root Certificate: Program Requirements, published: <https://technet.microsoft.com/en-us/library/cc751157.aspx>;



- [4] Mozilla CA Certificate Inclusion Policy, published: <https://www.mozilla.org/en-US/about/governance/policies/security-group/certs/policy/>;
- [5] Apple Root Certificate Program, published: https://www.apple.com/certificateauthority/ca_program.html;
- [6] ETSI Drafting Rules (Verbal forms for the expression of provisions);
- [7] RFC 3647 – Request For Comments 3647, Internet X.509 Public Key Infrastructure, Certificate Policy and Certification Practices Framework, <https://www.ietf.org/rfc/rfc3647.txt>;
- [8] AS Sertifitseerimiskeskus – Certification Practice Statement of KLASS3-SK 2010 (CPS), published: <https://www.sk.ee/repositoorium/CPS/>;
- [9] Certificate and OCSP Profile for Organisation Certificates Issued by SK, published: <https://sk.ee/en/repository/profiles/>;
- [10] Terms and Conditions for use of organisation certificates, published: <https://sk.ee/en/repository/conditions-for-use-of-certificates/>;
- [11] 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;
- [12] Personal Data Protection Act, RT I 06.01.2016, 10;
- [13] ETSI EN 319 401 V2.0.0 Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers;
- [14] AS Sertifitseerimiskeskus Trust Services Practice Statement, published: <https://sk.ee/en/repository/sk-ps/>.