

SK ID Solutions AS – Certificate Policy for Organisation Certificates

Version 13.0

OID: 1.3.6.1.4.1.10015.7.3

17. April 2022

| Version information | | |
|---------------------|---------|--|
| Date | Version | Changes/amendments |
| 17.04.2022 | 13.0 | <ul style="list-style-type: none"> Clause 1.5.4 – enforcement time for changes is changed to minimum 30 days after publication. |
| 12.07.2021 | 12.0 | <ul style="list-style-type: none"> Approved version; specified that Certificate may be issued to any of the European Economic Area member state and to Switzerland and United Kingdom of Great Britain and Northern Ireland. Therefore, clauses 1.3.3 and 3.2.2 of this CP have been amended accordingly; clauses 1.5.2 and 1.5.4 – replaced business development manager with head of trust services; clause 1.6.2 – updated the name of the CPS. |
| 15.08.2019 | 11 | <ul style="list-style-type: none"> Approved version; current CP has been reviewed to ensure compliance with the latest ETSI EN 319 401 [10], ETSI EN 319 411-1 [1] and ETSI EN 319 411-2 [11] policies; clause 1.2 – specified that each Certificate issued under this CP shall include distinct OID that shall be specific to that particular Certificate; clause 1.5.4 – added that SK performs annual review of this CP; references – updated previous versions of ETSI EN 319 401 [10], ETSI EN 319 411-1 [1] and ETSI EN 319 411-2 [11] policies with the latest ones. |
| 30.11.2017 | 10 | <ul style="list-style-type: none"> Approved version; clause 6.4.2 – corrected that if Private Key is generated by the CA, activation codes shall be delivered to the Subscriber or handed over in a secure envelope separately from QSCD. |
| 01.09.2017 | 9.1 | <ul style="list-style-type: none"> Draft of version 10. |
| 03.07.2017 | 9.0 | <ul style="list-style-type: none"> Approved version; clause 1.3.3 – amended the clause so it would reflect that the Subscriber can be any legal person who is registered in one of the European Union member state registries; removed the restriction that Subscribers for e-Seal Certificates shall be limited to Estonian registries; clauses 1.4.1, 1.6.1, 4.1.2 - corrected terminology and replaced the term “digital” with “electronic”; clause 1.6.1 – added terms Advanced Electronic Signature and Qualified Electronic Signature; clause 3.2.2 - removed the restriction that Certificate for Encryption or Authentication can only be issued to the Subscriber registered in the Estonian, Latvian, Lithuanian, Finnish or Swedish Business Register and who is discoverable from the European Business Register; added that the register, where the Subscriber is registered shall have legal effect; clause 3.2.5 – amended the clause so it would reflect that CA verifies that the Certificate application is signed by a person authorised by the legal representative; |

| | | |
|------------|-----|---|
| | | <ul style="list-style-type: none"> clause 4.1.2 – added specifications that application for e-Seal Certificate shall be signed with Qualified Electronic Signature, and application for Certificate for Encryption or Authentication shall be signed with an Advanced or Qualified Electronic Signature; also added that SK may accept physically delivered notarized and apostilled documents; clause 4.2.1 – added that if an application is submitted for e-Seal Certificate, the CA shall verify that the CA that issued the Certificate used for Qualified Electronic Signature, has physically identified the Subscriber’s legal representative or authorised person before issuing the Certificate to him/her. |
| 04.04.2017 | 8.1 | <ul style="list-style-type: none"> Draft of version 9.0. |
| 01.06.2017 | 8.0 | <ul style="list-style-type: none"> Approved version; due to change of SK’s business name from AS Sertifitseerimiskeskus to SK ID Solutions AS, name of the CP has been changed accordingly. Also, former business name has been replaced with the new one in clauses 1.1, 1.2, 1.5.1 and 1.6.2 of this CP; chapter 1.6.2 – generalised the name of the CPS as it shall also cover operations of the new CA KLASS3-SK 2016 in addition to operations of the old CA KLASS3-SK 2010. |
| 01.03.2017 | 7.1 | <ul style="list-style-type: none"> Draft of version 8.0. |
| 03.02.2017 | 7.0 | <ul style="list-style-type: none"> 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 1.5.4 – 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. |
| 01.11.2016 | 6.1 | <ul style="list-style-type: none"> Draft of version 7.0. |
| 01.07.2016 | 6.0 | <ul style="list-style-type: none"> Approved version; Redesigned the Certificate Policy in accordance with the IETF RFC 3647; Moved TLS Server Certificates into separate certificate policy; Chapter 1.1 - Added ETSI EN 319 411-2 Policy: QCP-I; Chapter 1.2 – Added OID for e-Seal Certificates issued under policy QCP-I; Chapter 6.1.1 – Specified key pair generation for e-Seal Certificates; Chapter 6.2.1 – Added specification “e-Seal Certificates on QSCD issued under policy QCP-I-qscd”; Chapter 4.10.2 – Added OCSP. |
| 22.06.2016 | 5.0 | <ul style="list-style-type: none"> Approved version. |
| 1.04.2016 | 5.1 | <ul style="list-style-type: none"> Draft of version 6.0. |
| 24.03.2016 | 4.1 | <ul style="list-style-type: none"> Draft of version 5.0; Chapter 1.4 - changed identification of the Certification Policy |
| 01.12.2015 | 4.0 | <ul style="list-style-type: none"> Approved version |
| 30.10.2015 | 3.1 | <ul style="list-style-type: none"> Draft of version 4.0; updated chapter 1.5.2.2 – added information about operator of help line; updated chapter 1.6 – updated contact details; updated chapter 2.1.2.2 – added obligations of Help line; |

| | | |
|------------|-----|--|
| | | <ul style="list-style-type: none"> • updated chapter 2.2.2.2 – added liability of Help line; • updated chapter 4.3 – specified formal requirements for applications for suspension and revocation of certificates; • updated chapter 4.4 – updated means for suspension of certificates; added information about where and when details about suspension shall be recorded; • updated chapter 4.6.2 – updated the procedure for submission of application for revocation; • updated chapter 4.6.4 – described the timeframe for certificate revocation and the period during which details about revocation shall be recorded in registry and certification revocation list; • updated chapter 9 – updated the list of referred and related documents. |
| 13.02.2015 | 3.0 | <ul style="list-style-type: none"> • Approved version. |
| 14.11.2014 | 2.7 | <ul style="list-style-type: none"> • Draft of version 3.0; • updated chapter 1.3.2 - updated list of abbreviations; • updated chapter 1.6 - updated contact e-mail address; • updated chapter 4.2.1 - added information about not checking CAA record in the application processing; • updated chapter 4.2.2 - updated list of persons to sign certificate application for SSL server certificate. |
| 20.06.2014 | 2.6 | <ul style="list-style-type: none"> • Updated chapter 4.6.1 – updated terms for certificate revocation; • updated chapter 8 – updated certification policy management policy; web server certificate is now stated as SSL server certificate; • updated chapter 4.2.2 – adjusted certificate issuance requirements separately for each certificate type; • minor changes/adjustments in accordance to new RFC versions; restructuring. |
| 21.12.2012 | 2.5 | <ul style="list-style-type: none"> • Updated chapter 2.4.4 – updated rules for certificate publication in public catalogue. |
| 28.09.2012 | 2.4 | <ul style="list-style-type: none"> • Updated chapter 4.2.4 – retired discrepancy with the CPS. |
| 20.07.2012 | 2.3 | <ul style="list-style-type: none"> • Updated chapter 4.6.1 – added authority descriptions for revoking certificates. |
| 10.05.2010 | 2.2 | <ul style="list-style-type: none"> • Updated chapters: • 1.3.4 – single certificate may contain multiple usage areas (except digital stamp certificate); • 4.2.2 – the term “smart card” has been replaced with “secure signature creation device”. |
| 13.08.2009 | 2.1 | <ul style="list-style-type: none"> • Removed discrepancies with Digital Signatures Act. The term “device certificates” is no longer in use. |
| 13.10.2006 | 1.1 | <ul style="list-style-type: none"> • Corrected version. |
| 10.04.2002 | 1.0 | <ul style="list-style-type: none"> • Primary version. |

| | | |
|-------|---|----|
| 1. | Introduction | 7 |
| 1.1. | Overview | 7 |
| 1.2. | Certificate Policy Name and Identification..... | 7 |
| 1.3. | PKI Participants | 8 |
| 1.4. | Certificate Usage | 8 |
| 1.5. | Policy Administration | 9 |
| 1.6. | Definitions and Acronyms | 10 |
| 2. | Publication and repository responsibilities..... | 12 |
| 2.1. | Repositories..... | 12 |
| 2.2. | Publication of Certification Information | 12 |
| 2.3. | Time or Frequency of Publication | 12 |
| 2.4. | Access Controls on Repositories | 12 |
| 3. | Identification and authentication | 13 |
| 3.1. | Naming | 13 |
| 3.2. | Initial Identity Validation..... | 13 |
| 3.3. | Identification and Authentication for Re-Key Requests..... | 14 |
| 3.4. | Identification and Authentication for Revocation Request..... | 14 |
| 4. | Certificate life-cycle operational requirements | 15 |
| 4.1. | Certificate Application..... | 15 |
| 4.2. | Certificate Application Processing..... | 15 |
| 4.3. | Certificate Issuance | 15 |
| 4.4. | Certificate Acceptance | 16 |
| 4.5. | Key Pair and Certificate Usage | 16 |
| 4.6. | Certificate Renewal | 16 |
| 4.7. | Certificate Re-Key..... | 16 |
| 4.8. | Certificate Modification | 16 |
| 4.9. | Certificate Revocation and Suspension..... | 17 |
| 4.10. | Certificate Status Services | 18 |
| 4.11. | End of Subscription | 19 |
| 4.12. | Key Escrow and Recovery..... | 19 |
| 5. | Facility, management, and operational controls | 20 |
| 5.1. | Physical Controls | 20 |
| 5.2. | Procedural Controls..... | 20 |
| 5.3. | Personnel Controls..... | 20 |
| 5.4. | Audit Logging Procedures | 21 |
| 5.5. | Records Archival..... | 21 |

| | | |
|-------|--|----|
| 5.6. | Key Changeover..... | 22 |
| 5.7. | Compromise and Disaster Recovery | 22 |
| 5.8. | CA Termination | 22 |
| 6. | Technical security controls..... | 23 |
| 6.1. | Key Pair Generation and Installation..... | 23 |
| 6.2. | Private Key Protection and Cryptographic Module Engineering Controls | 23 |
| 6.3. | Other Aspects of Key Pair Management | 24 |
| 6.4. | Activation Data..... | 24 |
| 6.5. | Computer Security Controls | 24 |
| 6.6. | Life Cycle Technical Controls..... | 24 |
| 6.7. | Network Security Controls | 25 |
| 6.8. | Time-Stamping | 25 |
| 7. | Certificate, CRL, and OCSP profiles | 26 |
| 7.1. | Certificate Profile | 26 |
| 7.2. | CRL Profile | 26 |
| 7.3. | OCSP Profile | 26 |
| 8. | Compliance audit and other assessments | 27 |
| 8.1. | Frequency or Circumstances of Assessment..... | 27 |
| 8.2. | Identity/Qualifications of Assessor | 27 |
| 8.3. | Assessor's Relationship to Assessed Entity | 27 |
| 8.4. | Topics Covered by Assessment | 27 |
| 8.5. | Actions Taken as a Result of Deficiency | 27 |
| 8.6. | Communication of Results | 27 |
| 9. | Other business and legal matters | 28 |
| 9.1. | Fees | 28 |
| 9.2. | Financial Responsibility | 28 |
| 9.3. | Confidentiality of Business Information..... | 28 |
| 9.4. | Privacy of Personal Information..... | 28 |
| 9.5. | Intellectual Property Rights..... | 29 |
| 9.6. | Representations and Warranties | 29 |
| 9.7. | Disclaimers of Warranties | 29 |
| 9.8. | Limitations of Liability | 29 |
| 9.9. | Indemnities | 29 |
| 9.10. | Term and Termination | 29 |
| 9.11. | Individual Notices and Communications with Participants..... | 29 |
| 9.12. | Amendments..... | 30 |
| 9.13. | Dispute Resolution Provisions..... | 30 |

| | | |
|-------|-------------------------------------|----|
| 9.14. | Governing Law..... | 30 |
| 9.15. | Compliance with Applicable Law..... | 30 |
| 9.16. | Miscellaneous Provisions | 30 |
| 9.17. | Other Provisions..... | 30 |
| 10. | References..... | 31 |

1. Introduction

1.1. Overview

This document "SK ID Solutions AS – Certificate Policy for Organisation Certificates" (CP) defines the procedural and operational requirements that SK ID Solutions AS (SK) adheres to and requires entities to adhere to when issuing and managing Organisation Certificates such as e-Seal Certificates, Certificates for Encryption and Certificates for Authentication.

Issuing and managing of the Organisation Certificates by SK is based on The Regulation (EU) No 910/2014 [7] which establishes a legal framework for electronic signature and electronic seal.

This document only describes the restrictions to Certificate Policy for EU Qualified Certificates Issued to Legal Persons with Private Key Related to the Certified Public Key in a QSCD (QCP-I-qscd) and for EU Qualified Certificates Issued to Legal Persons (QCP-I) from ETSI EN 319 411-2 [11] ("QCP-I-qscd" and "QCP-I") and Normalized Certificate Policy from ETSI EN 319 411-1 [1] (NCP).

The semantics of "no stipulation" in this document means that no additional restrictions are set and relevant provisions from QCP-I-qscd, QCP-I and NCP are applied directly.

Issuing and managing of E-Seal Certificates by SK is based on the requirements of the Policy QCP-I-qscd: certificate policy for EU qualified certificates issued to legal persons with private key related to the certified Public Key in a QSCD and Policy QCP-I: certificate policy for EU qualified certificates issued to legal persons from ETSI EN 319 411-2 [11].

The certification service for e-Seals described in this CP SHALL be granted qualified status in the Trusted List of Estonia.

Issuing and managing of Certificates for Encryption and Certificates for Authentication by SK is based on the requirements for the policy NCP: Normalized Certificate Policy from ETSI EN 319 411-1 [1].

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

- QCP-I-qscd;
- QCP-I;
- NCP;
- This CP;
- CPS .

Pursuant to the IETF RFC 3647 [3] this CP is divided into nine parts. To preserve the outline specified by RFC 3647 [3], section headings that do not apply have the statement "**Not applicable**". Each first-level chapter includes reference to the relevant section of ETSI EN 319 411-1 [1] and ETSI EN 319 411-2 [11].

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) [2].

1.2. Certificate Policy Name and Identification

Refer to clause 5.3 of ETSI EN 319 411-1 [1] and ETSI EN 319 411-2 [11].

This document is called "SK ID Solutions AS – Certificate Policy for Organisation Certificates".

This CP is identified by OID: 1.3.6.1.4.1.10015.7.3

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 | 7.3 |
|---------------------------------|-----|

OID that is specific to each Certificate issued under this CP is composed according to the contents of the following table 2.

| Parameter | OID reference |
|--|-------------------|
| Internet Assigned Numbers Authority (IANA) | 1.3.6.1.4.1.10015 |
| Organisation Certificates | 9 |
| Certificate type | 1 to <i>n</i> |

e-Seal Certificate on QSCD SHALL include OID:

- of the policy ETSI EN 319 411-2 [11] clause 5.3 d) for QCP-I-qscd;
- of this CP;
- specific to this particular Certificate according to clause 3.2.3 of the Certificate Profile [5].

e-Seal Certificate on Secure Cryptographic Device SHALL include OID:

- of the policy ETSI EN 319 411-2 [11] clause 5.3 b) for QCP-I;
- of this CP;
- specific to this particular Certificate according to clause 3.2.3 of the Certificate Profile [5].

Certificate for Encryption or Authentication SHALL include OID:

- of the policy ETSI EN 319 411-1 [1] clause 5.3 a) for NCP;
- of this CP;
- specific to this particular Certificate according to clause 3.2.3 of the Certificate Profile [5].

1.3. PKI Participants

Refer to clause 5.4 of ETSI EN 319 411-1 [1] and ETSI EN 319 411-2 [11].

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 only be a legal person 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; or
- one of the European Economic Area member state business registries;
- the Swiss business register;
- United Kingdom of Great Britain and Northern Ireland business register.

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] and ETSI EN 319 411-2 [11].

1.4.1. Appropriate Certificate Uses

Subscriber certificates are intended for the following purposes:

- e-Seal Certificate – used for proof of integrity of an electronic document and the relation with the owner of such document;
- Certificate for Encryption – certificate used for data encryption;
- Certificate for Authentication – certificate used for authentication of the Subscriber in WWW, S/MIME or other data processing systems.

Various areas of application MAY be combined into a single certificate. The e-Seal Certificate SHALL not be combined with other areas of application.

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

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

1.4.2. Prohibited Certificate Uses

The use of the Organisation Certificates issued under this CP is prohibited for any of the following purposes:

- unlawful activity (including cyber attacks and attempts to damage the certificate);
- issuance of new certificates and information on certificate validity;
- use of the e-Seal Certificate for signing documents which can bring about unwanted consequences (including signing such documents during testing of the systems).

1.5. Policy Administration

1.5.1. Organisation Administering the Document

This CP is administered by SK.

SK ID Solutions AS

Registry code 10747013

Pärnu mnt 141, 11314 Tallinn

Tel +372 610 1880

Fax +372 610 1881

Email: info@skidsolutions.eu

<https://www.skidsolutions.eu/>

1.5.2. Contact Person

Head of trust services

Email: info@skidsolutions.eu

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 30 days after publication, SHALL be published electronically on SK website.

SK performs annual review of this CP to ensure compliance of the present document and services provided based on this CP with the applicable requirements.

All amendments are to be approved by the head of trust services 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 |
|----------------------------------|--|
| Advanced Electronic Signature | Electronic Signature which meets the requirements provided in Article 26 of eIDAS [7]. |
| Authentication | Unique identification of a person by checking his/her alleged identity. |
| Certificate | e-Seal Certificate, Certificate for Encryption and Certificate for Authentication. Within the meaning of this CP, the term "Certificate" encompasses all the previously listed certificates. |
| 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). |
| Organisation Certificate | e-Seal Certificate, Certificate for Encryption and Certificate for Authentication. Within the meaning of this CP, the term "Organisation 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 electronic 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 electronic 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 | Qualified Electronic Signature according to eIDAS [7] . |
| Qualified Electronic Signature/Seal Creation Device | A secure signature creation device that meets the requirements laid down in eIDAS Regulation [7] . |
| Relying Party | Entity that relies upon 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 which 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. |
| Terms and Conditions | Document that describes the obligations and responsibilities of the Subscriber while using the Organisation 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 Organisation Certificates |
| CPS | Certification Practice Statement of Organisation Certificates |
| 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 [7] |
| HSM | Hardware Security Module |
| OID | Object Identifier, a unique object identification code |
| PKI | Public Key Infrastructure |
| QSCD | Qualified electronic Signature/Seal Creation Device |
| RA | Registration Authority |
| SK | SK ID Solutions AS, provider of the certification service |
| SK PS | SK ID Solutions AS Trust Services Practice Statement [12] |

2. Publication and repository responsibilities

Refer to clause 6.1 of ETSI EN 319 411-1 [1] and ETSI EN 319 411-2 [11].

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://www.skidsolutions.eu/en/repository/CP/>.

This CP and referred documents – the CPS [4] and Certificate and OCSP Profile for Organisation Certificates Issued by SK (hereinafter Certificate Profile) [5] as well as the Terms and Conditions [6] 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] and ETSI EN 319 411-2 [11].

3.1. Naming

The Distinguished Name of the Organisation Certificate SHALL be compiled in accordance with the Certificate Profile [5].

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).

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:

- the Estonian Business Register; or
- the Estonian Non-Profit Associations and Foundations Register; or
- the Estonian Register of State and Local Government Organisations; or
- one of the European Economic Area member state business registries; or
- the Swiss business register; or
- United Kingdom of Great Britain and Northern Ireland business register.

Registries SHALL have legal effect.

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.

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 [\[1\]](#) and ETSI EN 319 411-2 [\[11\]](#).

4.1. Certificate Application

4.1.1. Who Can Submit a Certificate Application

No stipulation.

4.1.2. Enrollment Process and Responsibilities

Only electronically signed applications SHALL be accepted.

Application for e-Seal Certificate SHALL be signed with Qualified Electronic Signature.

Application for Certificate for Encryption and Certificate for Authentication SHALL be signed with an Advanced or Qualified Electronic Signature.

If the legal person's representative does not have the ability to electronically sign the certificate application in the meaning of eIDAS [\[7\]](#), SK MAY accept physically delivered notarized and apostilled documents or 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 according to the legislation of its country of origin.

If the Subscriber's legal representative or a person authorised by the legal representative submits an application for e-Seal Certificate, SK SHALL additionally verify that the CA that issued the certificate used for Qualified Electronic Signature, has physically identified the legal representative or authorised person before issuing that certificate to him/her.

4.2.2. Approval or Rejection of Certificate Applications

No stipulation.

4.2.3. Time to Process Certificate Applications

SK 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 the 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 SHALL be allowed only for e-Seal Certificates.

SK SHALL suspend e-Seal Certificates under any of the following circumstances:

- SK has reasonable doubt that the certificate contains incorrect data or the Private Key corresponding to the Public Key contained in the certificate can be used without the Subscriber's consent;
- suspension of the certificate is requested by the Subscriber's legal representative or by an authorised person indicated on the certificate application;
- suspension of the certificate is requested by the supervisory body or data protection supervision authority in the case of reasonable doubt that the certificate contains incorrect data or the Private Key corresponding to the Public Key contained in the certificate can be used without the Subscriber's consent;
- suspension of the certificate is requested by a court, prosecutor's office or institutions carrying out pre-trial criminal investigation to prevent further crimes.

4.9.14. Who Can Request Suspension

Suspension of an e-Seal Certificate MAY be requested by:

- the Subscriber's legal representative or an authorised person indicated on the certificate application;
- CA;
- an authorised representative of the supervisory body or data protection supervision authority;
- an authorised public servant in order to carry out pre-trial criminal investigation and prevent further crimes.

4.9.15. Procedure for Suspension Request

No stipulation.

4.9.16. Limits on Suspension Period

No limits.

4.9.17. Circumstances for Termination of Suspension

Termination of Suspension SHALL be allowed only for e-Seal Certificates.

The CA SHALL terminate the suspension of e-Seal Certificate only upon electronically signed application by the Subscriber.

4.9.18. Who Can Request Termination of Suspension

The termination of suspension of a certificate MAY be requested by:

- the Subscriber's representative;
- any relevant authority acted upon suspension in accordance with clause 4.9.14.

4.9.19. Procedure for Termination of Suspension

No stipulation.

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 [\[1\]](#) and ETSI EN 319 411-2 [\[11\]](#).

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.

5.3.5. Sanctions for Unauthorized Actions

No stipulation.

5.3.6. Independent Contractor Requirements

No stipulation.

5.3.7. 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 [\[1\]](#) and ETSI EN 319 411-2 [\[11\]](#).

6.1.1. Key Pair Generation

The Subscriber keys of e-Seal Certificates on QSCD issued under policy QCP-I-qscd SHALL be generated in one of the following ways:

- by the Subscriber in QSCD;
- by the CA in a hardware module that is compliant with requirements of QSCD and will be handed over to the Subscriber.

The Subscriber Private Keys for e-Seal Certificates on Secure Cryptographic Device issued under policy QCP-I, Certificates for Encryption and Certificates for Authentication MAY be generated by the Subscriber or by the CA.

6.1.2. Private Key Delivery to Subscriber

If the Private Keys are generated by the CA, the Private Keys SHALL be handed over to the legal representative of the Subscriber in person or using a courier.

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 [\[5\]](#).

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)

Allowed key usage flags SHALL be set as described in the Certificate Profile [\[5\]](#).

6.2. Private Key Protection and Cryptographic Module Engineering Controls

6.2.1. Cryptographic Module Standards and Controls

In case of e-Seal Certificates on QSCD issued under policy QCP-I-qscd the Private Key SHALL be generated on a device certified in accordance with eIDAS [\[7\]](#) and EN 419 211: Protection profiles for secure signature creation device [\[8\]](#).

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 [5].

6.4. Activation Data

6.4.1. Activation Data Generation and Installation

If the private key of the Subscriber is generated by the CA, copies of activation codes SHALL NOT be stored by the CA.

6.4.2. Activation Data Protection

If the Private Key of the Subscriber is generated by the CA, activation codes SHALL be delivered to the Subscriber or handed over in person to the legal representative of the Subscriber in a secure envelope separately from QSCD.

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 [\[1\]](#) and ETSI EN 319 411-2 [\[11\]](#).

7.1. Certificate Profile

Certificate SHALL be compliant with the profile described in the Certificate Profile [\[5\]](#).

7.2. CRL Profile

CRL SHALL be compliant to with the profile described in the Certificate Profile [\[5\]](#).

7.3. OCSP Profile

The OCSP responses SHALL be compliant with the profile described in the Certificate Profile [\[5\]](#).

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 [\[1\]](#) and ETSI EN 319 411-2 [\[11\]](#).

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 [\[1\]](#) and ETSI EN 319 411-2 [\[11\]](#).

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 Estonia.

9.15. Compliance with Applicable Law

SK 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 [\[7\]](#);
- Personal Data Protection Act [\[9\]](#);
- related European Standards:
 - ETSI EN 319 401 Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers [\[10\]](#);
 - ETSI EN 319 411-1 Electronic Signatures and Infrastructures (ESI); Policy and Security requirements for Trust Service Providers issuing certificates; Part 1: General requirements [\[1\]](#);
 - 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 [\[11\]](#);
 - EN 419 211 Protection profiles for secure signature creation device [\[8\]](#).

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.

10. References

- [1] ETSI EN 319 411-1 V1.3.1 (2021-05) Electronic Signatures and Infrastructures (ESI); Policy and Security requirements for Trust Service Providers issuing certificates; Part 1: General requirements;
- [2] ETSI Drafting Rules (Verbal forms for the expression of provisions);
- [3] 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>;
- [4] SK ID Solutions AS – Certification Practice Statement of Organisation Certificates, published: <https://www.skidsolutions.eu/en/repository/CPS/>;
- [5] Certificate, CRL and OCSP Profile for Organisation Certificates Issued by SK, published: <https://www.skidsolutions.eu/en/repository/profiles/>;
- [6] Terms and Conditions for use of organisation certificates, published: <https://www.skidsolutions.eu/en/repository/conditions-for-use-of-certificates/>;
- [7] 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;
- [8] EN 419 211 Protection profiles for secure signature creation device;
- [9] Personal Data Protection Act, RT I 06.01.2016, 10;
- [10] ETSI EN 319 401 V2.3.1 (2021-05) Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers;
- [11] ETSI EN 319 411-2 V2.3.3 (2021-08) 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;
- [12] SK ID Solutions AS Trust Services Practice Statement, published: <https://www.skidsolutions.eu/en/repository/sk-ps/>.