TeliaSonera Customer CA Certificate Policy and Certification Practice Statement

OID: 1.3.6.1.4.1.271.2.3.1.1.18

Date: 4th January 2016

Version: 1.2

Published by: TeliaSonera

Table of Contents

Revision History

Version	Version date	Change	Author
1.0	27th May 2014	The first official version	TeliaSonera CA Policy Management team
1.1	17th February 2015	Minor corrections	TeliaSonera CA Policy Management Team
1.2	4th January 2016	Added description to chapter 4.1.2	TeliaSonera CA Policy Management Team

1 INTRODUCTION

1.1 Overview

A Certification Practice Statement (CPS) is a Certification Authority's (CA) description of the practices it follows when issuing certificates. The purpose of this CPS is to describe the procedures that the CA uses when issuing certificates, and that all Registration Authorities, Subscribers, Subjects, and Relying Parties shall follow in connection with these certificates. This document defines the Certification Practice Statement for customer CA's issued from TeliaSonera Root CA v1.

This CPS describes the procedures and routines which apply when completing a certificate for individuals, organizations, functions and devices and for revoking and revocation checking of such certificates. This CPS will refer to separate TeliaSonera Production CPS, which describes the premises, procedures and routines which apply for the Production of TeliaSonera CA Services.

This CPS generally conforms to the IETF PKIX Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practice Statement Framework (also known as RFC 3647). This document is divided into nine sections:

- Section 1 - provides an overview of the policy and set of provisions, as well as the types of entities and the appropriate applications for certificates.
- Section 2 - contains any applicable provisions regarding identification of the entity or entities that operate repositories; responsibility of a PKI participant to publish information regarding its practices, certificates, and the current status; frequency of publication; and access control on published information.
- Section 3 - covers the identification and authentication requirements for certificate related activity.
- Section 4 - deals with certificate life-cycle management and operational requirements including application for a certificate, revocation, suspension, audit, archival and compromise.
- Section 5 - covers facility, management and operational controls (physical and procedural security requirements).
- Section 6 - provides the technical controls with regard to cryptographic key requirements.
- Section 7 - defines requirements for certificate, Certificate Revocation List (CRL) and Online Certificate Status Protocol (OCSP) formats. This includes information on profiles, versions, and extensions used.
- Section 8 - addresses topics covered and methodology used for assessments/audits; frequency of compliance audits or assessments; identity and/or qualifications of the personnel performing the audit or assessment; actions taken as a result of deficiencies found during the assessment; and who is entitled to see results of an assessment.
- Section 9 - covers general business and legal matters: the business issues of fees, liabilities, obligations, legal requirements, governing laws, processes, and confidentiality.

1.2 Document name and identification

This CP/CPS is titled *TeliaSonera Customer CA Certificate Policy and Certification Practise Statement*. The name of this CP/CPS is {TELIASONERA-CUSTOMER-CA-CPS-18}.

The certificates issued according to this CPS contain Certificate policy object identifier corresponding to the applicable certificate type. The routines and roles resulting from this CPS apply only in connection with certificates referring to the following Certificate policy object identifiers:

Certificate type	**Issuing CA**	**Certificate policy object identifier**
User certificates for corporate Customers	Customer specific CA under TeliaSonera Root CA v1	1.3.6.1.4.1.271.2.3.1.1.18

This CP/CPS also refers to the TeliaSonera Production CPS with the name {TELIASONERA-PRODUCTION-CPS-2}.

1.3 PKI participants

TeliaSonera will issue certificates to Customers of TeliaSonera. The participating organizations shall undertake what is stated in this Certification Practice Statement and the related Certificate Policies.

1.3.1 Certification authorities

The Certification Authority operating in compliance with this Certification Practice Statement is a customer of TeliaSonera. The name of the Certification Authority in the “Issuer” field of the certificate is the name of the customer organization.

These CAs are subordinate CAs of TeliaSonera Root CA v1. TeliaSonera Root CA has its own CPS describing the management of the certificate life cycle of subordinate CA certificates signed by it. The title of that CPS is TeliaSonera Root CPS and its CPS name is {TELIASONERA-ROOT-CPS-2}.

The Certification Authorities are responsible for managing the certificate life cycle of end entity certificates signed by the CAs. This will include:

- creating and signing of certificates binding Subjects with their public key
- promulgating certificate status through CRLs and/or OCSP responders
- creating, storing and recovering end entity confidential key pairs for organizations using the TeliaSonera key backup/restore service

1.3.2 Registration authorities

The CA’s units authorized to perform registration functions, Customer Organizations acting as Customers of certification services and authorized by CA, or other organizations selected and authorized as RAs, with which the CA makes written agreements, can act as Registration Authorities. Through those agreements, RAs are obliged to comply with this CPS for their part.

Typically RA is responsible for the following activities on behalf of a CA:

- identification and authentication of certificate Subjects
- initiate or pass along revocation requests for certificates
- approve applications for new, renewal or re-keying certificates

The Registration Officer can be a physical person or a Virtual Registration Officer i.e. a TeliaSonera’s or Customer Organization’s system that is used to authenticate individual identity and submit the certificate request to the CA system. Virtual Registration Officer System has to be approved by the CA.

1.3.3 Subscribers

The Subscriber makes an agreement with the CA about issuance of a certificate either to itself or to a natural person represented by it or to a Device in its possession (Subject). The Subscriber shall ensure that the Subject fulfils the obligations defined in this CPS and the conditions of the certification services. A subscriber may be an organization that is a Customer of TeliaSonera. The Subject of a certificate can be a natural person for whose exclusive use the private key corresponding to the public key in the certificate is intended, or a Device with installed software capable of utilizing the private key stored in the Device.

1.3.4 Relying parties

The Relying Party is a Customer Organization, which utilizes certificates for securing the organization’s internal or external activities. The Relying Party can also be a company, organization or a private person having business with the Customer Organization.

1.3.5 Other participants

Certificate manufacturer is CA's subcontractor that is involved in production of certification services in another role than that of Registration Authority. Also, when using Certificate Manufacturers as subcontractors, TeliaSonera CA is, however, ultimately responsible for the certification services as a whole.

A Certificate Manufacturer within TeliaSonera PKI is the Card Manufacturer responsible for the Smart Card life cycle.

1.4 Certificate usage

1.4.1 Appropriate certificate uses

Certificates under this CPS are issued to end-entities to be used for the following applications:

- Subject authentication
- verification of digital data origin and integrity
- confidentiality of digital data
- verification of electronic signatures

1.4.2 Prohibited certificate uses

Certificates under this CPS are not intended for servers or gateways. Thus "Extended Key Usage" purposes for "Server authentication", "Code signing", "Time stamping" and "OCSP signing" are prohibited.

Applications using certificates issued under this CPS shall take into account the key usage purpose stated in the "Key Usage" and "Extended Key Usage" extension field of the certificate.

Additionally, the key usage purposes and limitations possibly stated in the contract between the Subscriber and the CA shall be taken into account when using certificates.

It is not recommended to use certificates for encryption if the private key of the certificate is not backed up.

1.5 Policy administration

1.5.1 Organization administering the document

TeliaSonera CA Policy Management Team is the responsible authority for reviewing and approving changes to this CPS. Written and signed comments on proposed changes shall be directed to the TeliaSonera contact as described in Section 1.5.2. Decisions with respect to the proposed changes are at the sole discretion of the TeliaSonera CA Policy Management Team.

Contact information:

TELIASONERA AB
SE-106 63 Stockholm
Phone: +46 (0)8 504 550 00
Internet: https://repository.trust.teliasonera.com/

1.5.2 Contact person

Contact person in matters related to this CPS:

TeliaSonera Customer Service
Email: kundtjanst-eid@teliasonera.com
Phone: +46 (0)20 32 32 62

Other contact information:

Customer and Revocation Service:	020 32 32 62, +46 771 32 32 62 kundtjanst-eid@teliasonera.com

1.5.3 Person determining CPS suitability for the policy

TeliaSonera CA Policy Management Team is the administrative entity for determining this Certification Practice Statement (CPS) suitability to the applicable policies.

1.5.4 CPS approval procedures

TeliaSonera CA Policy Management Team will review any modifications, additions or deletions from this CPS and determine if modifications, additions or deletions are acceptable and do not jeopardize operations or the security of the production environment.

1.6 Definitions and acronyms

A list of definitions and acronyms can be found at the end of this document.

2 PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 Repositories

2.1.1 CPS Repository

A full text version of this CPS is published at https://repository.trust.teliasonera.com

2.1.2 Revocation Information Repository

Certificate Revocation Lists (CRLs) are published according to CRL-distribution point certificate extension as stated in the issued certificate.

OCSP server location is specified in Authority Information Access certificate extension as stated in the issued certificate. OCSP requests may be signed or unsigned depending on the Customer agreement.

2.1.3 Certificate Repository

All issued certificates are stored in the local database of the CA system. Certificates may also be published to other repositories if it is a part of the TeliaSonera CA Service or agreed with a Customer.

2.2 Publication of certification information

It is TeliaSonera's duty to make the following information available:

a) This CPS.

b) Certificate revocation lists of revoked certificates or revocation information via OCSP.

c) Issued CA certificates and cross certificates for cross-certified CAs.

TeliaSonera may publish and supply certificate information in accordance with applicable legislation.

Each published certificate revocation list (CRL) provides all processed revocation information at the time of publication for all revoked certificates of which the revocation list is intended to give notification.

TeliaSonera supplies CA certificates for all public CA keys provided these can be used for verifying valid certificates.

Subscribers will be notified that a CA may publish information submitted by them to publicly accessible directories in association with certificate information. The publication of this information will be within the limits of sections 9.3 and 9.4.

2.3 Time or frequency of publication

Updates to this CPS are published in accordance with the provisions specified in section 9.12.

Revocation information publication provisions are specified in section 4.9.

All issued certificates are stored in the local database of the CA system promptly on issuing. Certificates may also be published to other repositories if it is a part of the TeliaSonera CA Service or agreed with a Customer.

2.4 Access controls on repositories

This CPS, CRLs and CA certificates are publicly available.

OCSP services and end entity certificates are only available through an agreement with TeliaSonera.

Only authorized CA personnel have access to subscriber certificates stored in the local database of the CA system.

3 IDENTIFICATION AND AUTHENTICATION

3.1 Naming

3.1.1 Types of names

An X.501 Distinguished Name (DN) is used as an unambiguous name of the Subject in the ”Subject” field of the certificate. The name always includes the following attributes:

Attribute	**Description of value**
commonName (CN, OID 2.5.4.3)	Name of the Subject.
OrganizationName (O, OID 2.5.4.10)	Customer Organization in relation to which the Subject is identified.

Additionally, the “Subject” field may include following attributes depending on the usage purpose of the certificate:

Attribute	**Description of value**
Surname (S, OID 2.5.4.4)	Family name of the Subject
givenName (G, OID 2.5.4.42)	Subject’s names, which are not family name
emailAddress (EA, OID 1.2.840.113549.1.9.1)	E-mail address of the Subject
serialNumber (SN, OID 2.5.4.5)	Character string that can be used to distinguish otherwise similar Subject names, e.g. personal ID number or username.
organizationalUnitName (OU, OID 2.5.4.11)	Determined by the application or the implementation of the service with which the certificate is used.
State or province (ST, OID 2.5.4.8)	Qualifier for describing the location of the Subscriber or the Subject.
Locality (L, OID 2.5.4.7)	Qualifier for describing the location of the Subscriber or the Subject.
Country (C, OID 2.5.4.6)	Qualifier for describing the location of the Subscriber or the Subject. Two letter country code e.g. “FI” or “SE”.
domainComponent (DC, OID 0.9.2342.19200300.100.1.25)	Multiple values specifying the domain name of the Subject.

Subject name information may also be contained in the Subject Alternative Name X.509 version 3 extensions. Subject Alternative Name extension may contain following information:

Attribute	**Description of value**

rfc822Name	E-mail address of the Subject
otherName	Other Name field can be used for Microsoft Windows user principal name (UPN) in the certificates issued to natural persons.

Additional Distinguished Name (DN) and Subject Alternative Name attributes may be used as necessary.

3.1.2 Need for names to be meaningful

Names will be meaningful as stated in the section 3.1.1.

3.1.3 Anonymity or pseudonymity of subscribers

The commonName attribute can include the name, or a pseudonym, of the Subject. OrganizationName attribute contains always a Customer organization's name that accurately identifies the customer.

3.1.4 Rules for interpreting various name forms

The commonName (CN) is composed of the given and family name of the Subject, and it can additionally contain other given names or initials.

If the certificate is issued to a group email account or similar, then the commonName should be the name of the related function or organizational unit.

The Organization (O) attribute states the Customer Organization in relation to which the Subject is identified. Normally Organization attribute contains the registered name of the Organization with or without the abbreviation for the form of company incorporation. In some cases, the CA may also accept an Organization name attribute that is other than the official registered name of the Organization, if the name is commonly used or there is otherwise no risk of confusion.

3.1.5 Uniqueness of names

The Subject name stated in a certificate will be unique for all certificates issued within the domain of the CA, and conform to X.500 standards for name uniqueness. Subject name uniqueness means that the CA will not issue certificates with identical names to different entities. However, the CA may issue several certificates to the same entity, and in that case the Subject names in those certificates may be the same.

Unambiguousness of the Subject names is secured in a two-phased procedure. A name contains both the name of the organization and the name of the Subject. The CA system allows only unambiguous organization names. The Customer Organization is not able to change the organization name that the CA has recorded for the organization in the CA system. The Customer Organizations are responsible for the unambiguousness of the names of their own users and devices.

3.1.6 Recognition, authentication, and role of trademarks

The priority to entity names are given to registered trademark holders.
The use of a Domain Name is restricted to the authenticated legal owner of that Domain Name.
The use of an email address is restricted to the authenticated legal owner of that email address.

TeliaSonera does not otherwise check the right of the Customer Organization to use the names it gives in its certificate applications except for the Organization Name as stated in section 3.2.2, nor does the CA participate in any name claim dispute resolution procedures concerning brand names, domain names, trademarks, or service names. TeliaSonera reserves the right not to issue such a certificate, or to revoke a certificate that has already been issued, when there is a name claim dispute involved concerning the certificate contents.

3.2 Initial identity validation

3.2.1 Method to prove possession of private key

If the CA does not generate the key pair of the Subject but it is generated in the Customer Organization, the CA can verify the possession of the private key by verifying the electronic signature included in the certificate request.

3.2.2 Authentication of organization identity

TeliaSonera verifies the organization name of a new Customer Organization by checking the existence of the company. Its legal name, business identity code and other relevant organization information are confirmed from an official business register maintained by an applicable government agency (e.g. ytj.fi in Finland) orby using another trustworthy method. Common variations, tradenames, abbreviations or suffixes for the name are allowed provided that the new name can be clearly associated with the Customer Organization.

3.2.3 Authentication of individual identity

The Customer Organization act as a Registration Officer within the Customer Organization and to register certificates for the persons or client devices related to the organization.

Customer is responsible for authenticating the Subject. The Registration Officers are obliged to follow the policies and instructions given by the CA.

The Registration Officer should use Organization's previously recorded directories, databases or other similar information on Organization's employees, partners or devices to verify the Subject information including the email address, or the Registration Officer should verify the information by checking the Subject's identity card.

3.2.4 Non-verified subscriber information

The Customer Registration Officer is required to verify the following Subject information as described in section 3.2.3:

- commonName (CN)

If email address (EA), Surname (S) and givenName (G) attributes or Subject Alternative Name extensions are used then the Registration Officer should verify them also.

Other information is not verified by TeliaSonera or Customer Organization.

3.2.5 Validation of authority

The Administrative Contact Person, who grants the necessary authorizations in the Customer Organization, has been identified in the service agreement or order. TeliaSonera verifies that the Organization has authorized the certificate service by contacting the contact person specified in the agreement by phone, mail or other similar methods.

Customer Registration Officers may also be identified in the service agreement or the Administrative Contact Person may authorize Registration Officers by delivering to TeliaSonera an authorization in writing and signed by him/her. The certificate application information of the Registration Officer is delivered at the same time.

In certain services, a Registration Officer in a Customer Organization has the right to define new Registration Officers in the organization and initiate the application for their Registration Officer certificates.

When registering Subjects, the identity and authority of the Registration Officer is verified by means of his certificate issued by TeliaSonera, or from his signature on the certificate order form, or using other comparable methods approved by the CA.

3.2.6 Criteria for interoperation

Not applicable.

3.3 Identification and authentication for re-key requests

3.3.1 Identification and authentication for routine re-key

Re-keying request can be automatically accepted without strong authentication if the subject information remains the same (e.g. one-time-password can be sent to the same mobile phone and/or email address again to re-new the subject's existing certificate).

If there are changes in the Subject or certificate delivery information the request will be validated in the same way as at initial registration.

3.3.2 Identification and authentication for re-key after revocation

In accordance with 3.3.1.

3.4 Identification and authentication for revocation request

Revocation by Customer Organization

Customer's self-service revocation can be activated by the Subject or the Subscriber. The revocation request can be submitted to TeliaSonera by the Subject directly or via the Revocation Officer of the Customer Organization. In the latter case The Revocation Officer is responsible for the verification of the authenticity of the request. TeliaSonera verifies the identity of the Subject or the Revocation Officer with a certificate, one-time-password scheme or other reliable method.

Revocation by the Revocation Service of the CA

The Subject, or Subscriber, or Registration Officer in a Customer Organization shall submit a request for certificate revocation to the Revocation Service by telephone or by e-mail. The source of the revocation request will be authenticated based on the digital signature or the Revocation Service will make a call back to the Customer Organization and asks certain detailed data. This data is compared with the information recorded about the Subject at registration, and if necessary, with information in the agreements made with the Subscriber or with the Customer Organization. If the data match the certificate will be revoked.

In certain situations where there is an identified risk of abuse of the private key or when it is obvious that the authorized use of the key is prevented, it may be necessary to revoke the certificate on request of someone else but the above mentioned entities. In that case the verification of the authenticity of the revocation request can require other authentication methods. In cases where reliable verification cannot be immediately performed, the CA may revoke the certificate to reduce risks.

Reinstatement of suspended certificate

Customer Registration Officers may reinstate suspended certificates in their own organizations if there is such service agreement with CA.

Reinstatement of a suspended certificate can be requested by the Subject or by the Registration Officer operating in the Customer Organization. A request from the Subject will be executed only after confirmation from the Registration Officer. A request or confirmation received from the Registration Officer in an e-mail message or in an electronic form will be verified based on an electronic signature, or the Registration Officer shall be authenticated using certificates, some other strong authentication or by making a call back to the Customer Organization and asking and checking data recorded of the Subject or Registration Officer at registration, or checking information that can be found in the agreements made with the Subscriber or Customer Organization.

4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 Certificate Application

4.1.1 Who can submit a certificate application

When a certificate is applied to a person or Device, it is required that the ordering organization is TeliaSonera's Customer Organization with which the Subject has a contractual relation or which possesses the Device to which the certificate is applied.

Certificate request can be submitted by

a) A Registration Officer in a Customer Organization

b) An employee or other individual contracted by a Customer Organization (Subject)

c) An Administrative contact person of a Customer Organization

4.1.2 Enrollment process and responsibilities

Certificates can be applied for either through the RA office of the CA or directly from the CA system by using the tools delivered by the CA.

a) The Registration Officer in the Customer Organization pre-registers the Subject using self service software provided by TeliaSonera and applies for a certificate to the Subject or the Subject can, after pre-registration, initiate the application for a certificate by using the one-time password sent to him/her. The Subject uses the one-time-password to authenticate to the registration tool. The Registration Officer or the Subject generates the key pair and submits the certificate request to the CA system containing the certificate information defined by the Registration Officer during the pre-registration and the public key.

b) The Subject initiates the enrollment process by submitting a certificate application using self service software provided by TeliaSonera. The Subject generates the key pair using browser software and submits the certificate request containing the certificate information. The Registration Officer in the Customer Organization verifies the information in the request and sends the Subject a link to pick up the issued certificate.

c) The self service software provided by TeliaSonera is integrated with the existing authentication solution at the customer site. The subject uses the user credentials in the customer organizations authentication solution to enroll for a certificate.

d) Certificate is applied for through the RA office of the CA. The Registration Officer or Administrative contact person sends a manually or electronically signed order that contains the necessary information for the certificate there. At the RA office of the CA the signature is checked, the sufficiency of information given for the certificate is examined, and the Subject is pre-registered. The actual certificate request to the CA system can be initiated by the RA office of the CA, or alternatively the necessary instructions and one-time password for the certificate request can be delivered, according to the order, either directly to the Subject or to the Registration Officer of the Customer Organization.

The Customer Organization is bound to registration policies and Customer responsibilities through a certification service agreement with TeliaSonera. Customer Organization's Registration Officers also accept Customer Responsibilities when they logon to TeliaSonera's self service application first time.

Test certificates

The CA has granted special authorities to a few of its employees to apply for test certificates for tests that must be carried out in the production system. The applicant of a certificate is authenticated on the basis of his certificate. One of the following details in the contents of the "Subject" field of a certificate will serve as an indication of a test certificate:

- the word "Test" or comprises the contents of the "Organization Name" field (the primary method),
- the "Common Name" field contains the word "test", or
- another field contains the word "test".

A test certificate is valid at most seven (7) days or it shall always be revoked after seven (7) days of its coming into force, at the latest. If such a test case emerges where the contents of the certificate cannot indicate the test nature of the certificate, it must be revoked immediately after the test.

The CA has granted a few of its employees special authorities to apply for certificates in the pilot phase of information security services of Sonera, when the registration responsibilities have not yet been moved to the RA office of the CA. The applicant of a pilot certificate is authenticated on the basis of his certificate. The same certificate application requirements, which apply in the production phase of the service, shall be followed when applying for pilot certificates.

4.2 Certificate application processing

4.2.1 Performing identification and authentication functions

Identification and authentication of Subject and Subscriber information is performed in accordance with the section 3.2.

4.2.2 Approval or rejection of certificate applications

TeliaSonera will approve a certificate application if it meets the requirements of validation and identification. All other certificate applications will be rejected.

The subscriber will be informed on why the certificate application was rejected and on how to proceed to be approved.

4.2.3 Time to process certificate applications

When a certificate is applied for directly from the CA system by the tools provided by the CA, the certificate request is processed automatically by TeliaSonera's RA and CA systems immediately after the request is submitted.

When a certificate is applied for through the RA office of the CA, TeliaSonera process the applications within reasonable time frame. There are no specific requirements for the processing time unless otherwise agreed with the Customer.

4.3 Certificate issuance

4.3.1 CA actions during certificate issuance

If the certificate application is approved by the Registration Officer, the CA issues the certificate. The certificate is created by the CA according to the information contained in the certificate request. However, the CA may overwrite some certificate information using pre-defined certificate profile specific standard values.

4.3.2 Notification to subscriber by the CA of issuance of certificate

The certificate is available for the Customer Organization's Registration Officer or for the Subject in the registration tool after the issuance.

4.4 Certificate acceptance

4.4.1 Conduct constituting certificate acceptance

The Subject, or when certificates to Devices are concerned, the Subscriber, is considered to have accepted the certificate when the private key associated with it has been used for the first time, or when the certificate has been installed into a device.

4.4.2 Publication of the certificate by the CA

TeliaSonera will not publish subscriber certificates to a publicly available repository if not agreed upon with the Customer Organization.

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

The subscriber shall only use certificates and their associated key pairs for the purposes identified in this CPS and in applicable agreements with TeliaSonera. Issued certificates contain information which defines suitable areas of application for the certificate and its associated keys. Area of application labelling takes place in accordance with X.509 and chapter 7 of this CPS.

For more information regarding appropriate subscriber key usage see sections 1.4.1 and 6.1.7.

The subscriber shall protect the Subject private key from unauthorized use. If the private key is compromised the subscriber shall discontinue the use of the Subject private key immediately and permanently and request for the revocation of the certificate.

4.5.2 Relying party public key and certificate usage

Prior to accepting a TeliaSonera certificate, a relying party is responsible to:

a) Verify that the certificate is appropriate for the intended use;

b) Check the validity of the certificate, i.e. verify the validity dates and the validity of the certificate and issuance signatures; and

c) Verify from a valid Certificate Revocation List (CRL) or other certificate status service provided by the CA that the certificate has not been revoked or suspended. If certificate status cannot be verified due to system failure or similar, the certificates shall not be accepted.

4.6 Certificate renewal

Certificate renewal is the re-issuance of a certificate with a new validity date using the same public key corresponding to the same private key. Normally a new key pair is generated when a certificate is renewed and TeliaSonera prefers that the certificates are re-keyed instead of renewing them using the existing key pair. However, it is possible that Subscriber uses existing key pairs instead of generating new public and private keys.

Certificate renewal requests are processed as certificate re-keys as described in section 4.7

4.7 Certificate re-key

Certificate re-key is the re-issuance of a certificate using new public and private keys.

4.7.1 Circumstance for certificate re-key

When the validity time of a certificate is about to end, the certificate can be re-keyed. Also technical problems in certificate installation or in certificate storage may trigger re-keying.

4.7.2 Who may request certification of a new public key

Re-key may be requested by the same persons as the initial certificate application as described in section 4.1.1. If the Subject has technical problems with the certificate or he/she has lost the certificate, the Subject may also request a new certificate from TeliaSonera's Customer Service.

4.7.3 Processing certificate re-keying requests

If the certificate re-key is started by the Registration Officer in the Customer Organization, it is his/her responsibility to ensure that there are no obstacles to the re-key. If there are changes in the Subject information or in the certificate delivery information those shall be checked in the same way as at initial registration. Re-keyed certificate is issued and delivered in the same way as the initial certificate as described in section 4.1 – 4.4.

If the certificate re-key is processed by the Customer Service of the CA or other authorized CA personnel, they ensure that the original usage purpose for the certificate still exists. Then they use the information from the initial certificate request authorized by the Registration Officer and deliver the one-time password to the Subject using the existing contact information stored in the registration system. The Subject can then use the one-time password to initiate the application for a certificate.

4.7.4 Notification of new certificate issuance to subscriber

Subscriber is notified in the same ways when the certificate is issued first time as described in section 4.3.2.

4.7.5 Conduct constituting acceptance of a re-keyed certificate

Conduct constituting acceptance of a re-keyed certificate is described in section 4.4.1.

4.7.6 Publication of the re-keyed certificate by the CA

Re-keyed certificates are published like initial certificates as described in section 4.4.2.

4.7.7 Notification of certificate issuance by the CA to other entities

No stipulation.

4.8 Certificate modification

Certificate modification is the re-issuance of the certificate due to changes in the certificate information other than the validity time (certificate renewal) or Subscriber's public key (certificate re-key). Certificate modification requests are processed as initial certificate requests as described in sections 4.1 – 4.4.

4.9 Certificate revocation and suspension

4.9.1 Circumstances for revocation

A certificate must be revoked or suspended (i.e. cancelled for the time being) under the following conditions:

1. Upon suspected or known compromise of the private key;
2. Upon suspected or known compromise of the media holding the private key;
3. Subject or subscriber information is known to be invalid or re-verification fails.
4. When there is an essential error in the certificate

A certificate may be revoked or suspended (i.e. cancelled for the time being) under the following conditions:

1. When any information in the certificate changes;
2. Upon termination of a Subject;
3. When a Subject no longer needs access to secured organizational resources;
4. When the certificate is redundant (for example, a duplicate certificate has been issued).
5. Customer's certificate contract with Teliasonera has ended.
6. Any other reason that makes the certificate obsolete or threats related keys

TeliaSonera in its discretion may revoke a certificate under any circumstances, for example when an entity fails to comply with obligations set out in this CPS, any applicable agreement or applicable law. TeliaSonera will revoke a certificate at any time if TeliaSonera suspects that conditions may lead to a compromise of a Subscriber's keys or certificates.

4.9.2 Who can request revocation

The revocation of a certificate can be requested by:

1. A Subject whose name the certificate is issued under;
2. A Subscriber or Registration Officer in the Customer Organization that has made an application for a certificate on behalf of an organization, device or application; or
3. Personnel of TeliaSonera.

4.9.3 Procedure for revocation request

A revocation request may be received by TeliaSonera in one of the following ways:

a) The Registration Officer in the Customer Organization makes the revocation request using the administration interface.

b) The Subject makes the revocation request using a self-administration or re-enrollment interface

If the revocation request cannot be carried out in accordance with a) or b), the Registration Officer in the Customer Organization or the Subject may contact TeliaSonera Revocation Service by telephone or email and make a revocation request. Authorized TeliaSonera revocation staff, then authenticates the identity of the originator of a revocation request according to section 3.4 and makes the revocation request using TeliaSonera's CA system.

When making a revocation request as above, TeliaSonera's system checks that the person making revocation request is authorized to do so and after that the certificate in question is revoked.

4.9.4 Revocation request grace period

The CA is available for revocation requests 24 hours per day, 7 days per week.

When a reason for the revocation of a certificate appears, the Subject or Subscriber shall immediately inform the Revocation Service directly or the Customer Organization through its Registration Officer. Also the Registration Officer shall revoke the certificate using the administration interface or inform TeliaSonera's Revocation Service immediately, when a reason for the revocation of a certificate comes to his/her notice.

The CA shall not be responsible for the damage caused by illicit use of the Subject's private key. The CA shall be responsible for the publication of the revocation information on the Certificate Revocation List according to the principles given in this CPS.

4.9.5 Time within which CA must process the revocation request

TeliaSonera process revocation requests within reasonable time frame. There are no specific requirements for the processing time unless otherwise agreed with the Customer.

4.9.6 Revocation checking requirement for relying parties

Prior to using a certificate, it is the Relying Party's responsibility to check the status of all certificates in the certificate validation chain against the current CRL's or on-line certificate status server (OCSP). A certificate cannot be reasonably relied on if the Relying Party does not diligently follow the certificate status checking procedures denoted below:

- A Relying Party shall ensure him-/herself of the authenticity and integrity of the CRLs or on-line certificate status responses by checking the digital signature and the certification path related to it.
- The Relying Party shall also check the validity period of the CRL and OCSP response in order to make sure that the information in the CRL or OCSP response is up-to-date.
- Certificates may be stored locally in the Relying Party's system, but the prevailing revocation status of each of those certificates shall be checked before use.
- If valid certificate status information cannot be obtained because of a system or service failure, not a single certificate must be trusted. The acceptance of a certificate in violation of this condition befalls at the Relying Party's own risk.

The Relying Party may acquire the checking of the CRLs as a service that shall follow the certificate status checking procedures denoted above.

4.9.7 CRL issuance frequency

The Revocation Status Service is implemented by publishing Certificate Revocation Lists (CRLs), digitally signed by the CA, in a public directory. The rules below are followed:

- A new CRL is published in the directory at intervals of not more than 2 hours.
- The validity time of every CRL is forty-eight (48) hours.
- The publishing intervals and validity time may also be agreed upon with Teliasoneras customer.

There may be several valid CRLs available at the same time. The one of those, which has been published as the latest, contains the most real time information.

4.9.8 Maximum latency for CRL's

Latency may be up to five minutes.

4.9.9 On-line revocation/status checking availability

TeliaSonera may provide on-line revocation status checking via the OCSP protocol.

The service is only accessible provided that the relying party has an agreement with TeliaSonera. Availability of the service will be provided in the agreement.

4.9.10 On-line revocation checking requirements

All responses will be signed by a private key corresponding to a public key certified by the CA on which the OCSP request is made. A separate key pair will be used for the responses of each CA.

The OCSP service is normally updated through the use of CRLs and/or deltaCRLs that are published on regular basis. The actual time intervals for the updates of the CRLs and/or deltaCRLs are described in the section 4.9.7. OCSP service may use online checking from CA database provided that the relying party has such agreement with TeliaSonera.

4.9.11 Other forms of revocation advertisements available

No stipulation.

4.9.12 Special requirements regarding key compromise

No stipulation.

4.9.13 Circumstances for suspension

For some services, certificates are suspended (i.e. cancelled for the time being) by default, instead of permanently revoking them.

A certificate shall be suspended under the same conditions that apply to revocation as described in section 4.9.1.

4.9.14 Who can request suspension

Suspension may be requested by the same persons as the revocation as described in section 4.9.2.

4.9.15 Procedure for suspension request

A certificate is suspended in the same way as when the certificate is revoked as described in section 4.9.3

4.9.16 Limits on suspension period

Certificates shall be permanently revoked after six (6) months from suspension, at the latest, unless they have been reinstated.

4.10 Certificate status services

4.10.1 Operational characteristics

The CRLs are published in the TeliaSonera's LDAP directory and website as disclosed in the section 2.1.2.

The OCSP service is only accessible provided that the relying party has an agreement with TeliaSonera. Operational characteristics of the service will be provided in the agreement.

4.10.2 Service availability

The certificate status services are available 24 hours per day, 7 days per week excluding scheduled maintenance or other planned breaks.

4.10.3 Optional features

The OCSP service is only accessible provided that the Customer organisation has an agreement with TeliaSonera.

4.11 End of subscription

The end of a subscription as a result of no longer requiring the service, compromise, or termination of employment (voluntary or imposed) will result in the immediate revocation of the certificate and the publishing of a CRL or other certificate status verification system.

4.12 Key escrow and recovery

4.12.1 Key escrow and recovery policy and practices

A Subscriber's digital signature private keys will not be escrowed.

A Subscriber's confidentiality private keys will be not be escrowed but TeliaSonera may keep a backup of the keys if so agreed between TeliaSonera and the Customer. The keys are protected in an encrypted form and are protected in a level no lower than stipulated for the primary versions of the keys. The decryption key used to decrypt the key backups is stored in a Hardware Security Module (HSM) and the key backups are saved for a period that is agreed with the Customer.
A private key may be recovered for two separate reasons:

a) The hard disc, the Smart Card or equivalent that holds the Subscriber's private key is corrupted and the Subscriber needs to make a recovery of his key. The process of authenticating the Subscriber is the same as at the initial certificate issuance.
b) The Subscriber is for some reason prevented from using his private key (the Subscriber may for instance be deceased, injured or has left the organization) and the Subscriber's organization needs to decrypt data encrypted by the Subscriber. The process of such a key recovery involves at least three persons from the Subscribers' organization where all are authenticated by certificates.

4.12.2 Session key encapsulation and recovery policy and practices

No stipulation.

5 FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

All stipulations regarding chapter 5 Facility Management, and Operational Control are specified in "TeliaSonera Production CPS". The TeliaSonera Production CPS can be found at https://repository.trust.teliasonera.com.

6 TECHNICAL SECURITY CONTROLS

All general stipulations regarding chapter 6 Technical Security Controls are specified in TeliaSonera Production CPS. The TeliaSonera Production CPS can be found at https://repository.trust.teliasonera.com.

The sections below are additions to the texts in the corresponding sections of the "TeliaSonera Production CPS" to complement and specify information concerning Subscriber key management.

6.1 Key pair generation and installation

6.1.1 Key pair generation

The Subscriber key pair may be generated by the Subscriber or the Subscriber may use the registration tool provided by the CA to generate the key pair (PKCS#12 files). The Subscriber normally generates the key pair using browser software. The Subscriber may also generate the key pair on a Smart Card or USB token. It is also possible to use Smart Cards that have the key pair generated by the Card Manufacturer.

If the key pair is generated by the Subscriber in a Customer Organization, the Customer Organization itself is responsible for the secure generation of the key pair and the confidentiality of the private key.

If the key pair is provided by the CA, the generation will be carried out according to the secure procedures defined by the CA.

6.1.2 Private key delivery to subscriber

The CA delivers the Subscriber's private key on a Smart Card, on a USB token, or in a file to the Registration Officer in Customer Organization or to the Subject.

When the Subject generates his key pair the private key will be recorded on the Subjects workstation, Smart Card or USB token, a separate delivery of the key is not needed.

Software certificates
If the key pair is generated using the self service software provided by the CA, the private key is delivered to the Subscriber in a password protected PKCS#12 file. The Registration Officer can download the PKCS#12 file directly from the application or send the Subject a one-time password, The Subject can access the self-service software with the one-time password and generate a key pair and download the PKCS#12 file.

Smart Cards and USB tokens
If the key pair is generated by the Card Manufacturer, the Card Manufacturer delivers the Smart Card that contains the private keys to the address specified in the card order, which is normally the address of the Registration Officer of the Customer Organization. The Registration Officer will deliver the card to the Subject.

If the key pair is generated by the CA, the certificate and the private key associated with it are delivered through a secure channel to the Subscribers Smart Card or USB token..

6.1.3 Public key delivery to certificate issuer

The public key is digitally signed and delivered through an encrypted connection, from the site where the key has been generated, to the CA system.

6.1.4 CA public key delivery to relying parties

Not applicable to subscriber keys. Methods to delivered CA certificates to Subscribers and Relying Parties are described in in TeliaSonera Production CPS.

6.1.5 Key sizes

The length of the Subscriber keys generated by the CA in connection with the RSA algorithm is at least 2048 bits.

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)

Issued certificates contain information which defines suitable areas of application for the certificate and its associated keys. The CA is not responsible for use other than the given key usage purposes. Area of application labeling takes place in accordance with X.509 and chapter 7.

End entity certificates issued according to this CPS include the following areas of application:

Certificate stored on a Smart Card, signing key:
NonRepudiation

Certificate stored in a Smart Card, authentication/encryption key:
DigitalSignature, KeyEncipherment, DataEncipherment *

* not in use for all certificates

Other certificates:
All the purposes mentioned on the list are not contained in all certificates, and in certain certificates there is no key usage purpose given.

DigitalSignature, NonRepudiation, KeyEncipherment, DataEncipherment, KeyAgreement.

6.2 Private key protection and cryptographic module engineering controls

6.2.1 Cryptographic module standards and controls

The Subscriber private keys may be stored in the software of a workstation/device or the private keys may be stored in a Smart Card or in a USB token.

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

Not applicable to subscriber keys.

6.2.3 Private key escrow

TeliaSonera does not escrow subscriber private keys.

6.2.4 Private key backup

Backups may be made of the subscribers' private confidentially keys, if so agreed between TeliaSonera and the Customer. The keys are then copied and stored in encrypted form and protected at a level no lower than stipulated for the primary version of the keys.

No backups are made of the subscribers private non repudiation keys.

See section 4.12 for more detailed description.

6.2.5 Private key archival

TeliaSonera does not archive subscriber private keys.

6.2.6 Private key transfer into or from a cryptographic module

All stipulations regarding the section 6.2.6 Private key transfer into or from a cryptographic module are specified in TeliaSonera Production CPS.

6.2.7 Private key storage on cryptographic module

All stipulations regarding the section 6.2.7 Private key storage on cryptographic module are specified in TeliaSonera Production CPS.

6.2.8 Method of activating private key

Software keys

The CA recommends that the Customer Organizations use passwords for private key activation in accordance with the section 6.4 and take appropriate measures for the physical protection of the workstations or other devices used to store private keys.

Smart Cards and USB tokens

Activation of the private key of the Subject requires the use of activation data as described in section 6.4.

6.2.9 Method of deactivating private key

Software keys

Locking of the private key of the Subject depends on the software in use.

Smart Cards and USB tokens

The private key on a Smart Card or USB token will be locked if the activation data related to it is inserted falsely too many times in succession. The lock-out threshold depends on the Smart Card or USB token type used and can be, for example, 3 or 5 failed attempts. A locked key can be returned into use with the help of a PUK code (PUK = PIN Unblocking Key) or equivalent technology (e.g. challenge/response).

6.2.10 Method of destroying private key

When the certificate of a Subject has expired and has not been renewed, the private key related to it cannot be used any more in connection with certification services. The key is not returned to the CA to be destroyed but it remains in the possession of the Subscriber.

The subscriber private confidentiality keys that are stored by the CA for backup purposes are securely destroyed at the end of service.

6.2.11 Cryptographic module rating

See section 6.2.1.

6.3 Other aspects of key pair management

6.3.1 Public key archival

The CA stores the Subject public keys according to section 5.5 of the TeliaSonera Production CPS.

6.3.2 Certificate operational periods and key pair usage periods

The usage period of the Subject certificate shall not be longer than five (5) years.

The same keys may be certified again on expiration of a certificate, although it is not recommended by TeliaSonera. The usage period of the Subject public and private keys shall not exceed the period during which the applied cryptographic algorithms and their pertinent parameters remain cryptographically strong enough or otherwise suitable.

6.4 Activation data

The Subscriber uses his private keys with the help of activation data, which are given on the keyboard of a card reader, workstation, mobile phone or other device.

6.4.1 Activation data generation and installation

Software keys

When the Subject or Registration Officer in the Customer Organization generates the key pair, a password can be choosen as activation data according to Customer Organization policy.

If the Registration Officer of the CA generates the key pair, the activation data will be generated using sufficient number of characters to be secure.

Smart Cards and USB tokens

The Card Manufacturer, Customer Organisation or RA system generates the activation data in pursuance of key pair generation.

When it is possible for the Subscriber to change the activation data, the Subscriber is recommended to make sure that the new activation data consists of sufficiently many characters to be secure.

6.4.2 Activation data protection

When the Card Manufacturer generates the key pairs, the activation data is generated at the same time and delivered securely to the Subject. Secure delivery is obtained by using:

- Concealed under a protective surface layer or enclosed in a sealed envelope.
- Encrypted activation data file.
- Or other similar secure method.

When the RA office of the CA generates the key pair, the activation data and the private key are sent as separate deliveries through different channels to the Subscriber. The activation data can be delivered for example to a mobile phone as an SMS or it can be given over the phone.

When the Registration Officer in a Customer Organization generates the key pairs, the organization is responsible for the secure delivery of the activation data to the Subject.

The Subscriber shall instruct the Subject to keep his activation data safe enough. He/She should memorize the activation data. The activation data must not be disclosed to others.

6.4.3 Other aspects of activation data

No stipulation.

7 CERTIFICATE, CRL, AND OCSP PROFILES

7.1 Certificate profile

The contents definition of a certificate, in other words the certificate profile, defines the fields in a certificate. The certificate profile of the certificates follows the version 3 profile defined in the ITU X.509 standard. The profile of the certificates also follows the document RFC 5280 “Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile”.

The basic fields used in certificates are listed in the table below:

Field name	Field description and contents
Version	This field states which of the certificate versions defined in the X.509 standard the certificate conforms to. The issued certificates conform to the version 3.
Serial number	The CA generates an individual random serial number for every certificate. The number that has been given in this field is unique for every certificate created by the CA system. The software manages the uniqueness of the serial number automatically.
Signature algorithm	The signature algorithm is the set of mathematical rules according to which the CA software executes the signing of the certificate. Identifiers have been allocated for the algorithms that are generally used. The identifier of the algorithm used for the signing of the certificate is given in this field. The signature cannot be verified if the algorithm used is not known. The algorithm that is used for the signing of the certificates is sha1RSA or sha256RSA.
Issuer	This field states the name of the Issuer of the certificate. The Issuer name in the certificates of each CA has been described in section 1.3.1.
Validity	The validity of the certificate is that period of time during which the CA guarantees that it maintains status information of the certificate, in other words about the possible revocation of the certificate. This field states the date and time when the certificate comes into force, and the date and time after which the certificate is no more valid. The certificate can be trusted during its validity period if the certificate has not been published on the CRL.
Subject	This field identifies the person or device under whose possession the private key is, that corresponds to the public key contained in the certificate. The field includes the unambiguous name of the Subject. The contents of the field have been described in section 3.1.
Subject public key info	This field gives the algorithm under which the public key of the Subject shall be used. The Subject’s public key itself is also given in this field. The algorithms and key lengths of the Subject keys are described in section 6.1.5.

7.1.1 Version number(s)

All issued certificates are X.509 Version 3 certificates, in accordance with the PKIX Certificate and CRL Profile.

7.1.2 Certificate extensions

Certificate extensions will be supported in accordance with RFC 5280 “Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile”. In general, following

extensions may be used in a certificate. In the table “Authority” means who verifies the content of extension:

Extension	Authority	Extension description and contents
Authority key identifier	CA	The identifier of the issuing CA public key is given in this extension. The identifier can be used to identify the public key that corresponds to the private key used for the signing of the certificate. SHA-1 hash algorithm is used to calculate the identifier.
Subject key Identifier	CA	The identifier of the Subject public key that is contained in the certificate is given in this extension. The identifier can be used to pick up those certificates that contain a given public key. SHA-1 hash algorithm is used to calculate the identifier.
Certificate policies	CA	This extension states the policies according to which the certificate has been issued. The relevant policy is identified based on an individual identifier (object identifier, OID) assigned to the policy document or certain certificate type. The identifiers covered by this CPS have been given in section 1.2..
CRL distribution points	CA	This extension gives the location where the CRL is available. The exact addresses of the CRLs corresponding to the different certificate classes are given in section 4.10.1.
Key usage	CA	The key usage purposes of the public key contained in the certificate are given in this extension. The key usage purposes of the public keys contained in the certificates are listed in section 6.1.7.
Extended key usage	CA	This extension contains other key usage purposes of the public key except those contained in the “Key usage” extension. A key usage purpose given in this extension may be generally known or privately defined for a certain application. E.g. the following key usage purposes may be given in a Certificate: ClientAuthentication, WindowsLogon, SMIME,
Basic constraints	CA	This extension may be used to express explicitly, if the certificate is a CA certificate (i.e. the Subject of the certificate is a CA) or not. Certain end entity certificates state that the certificate in question is not a CA certificate.
Subject alternative name	Subscriber	This extension can be used to relate alternative identification information to the Subject. Subject alternative name information used in the Certificates is described in section 3.1.1.
Authority Info Access	CA	The url to the OCSP service or CA-certificate may be given in this field.
Smartcard serial number	Subscriber	Certificate stored on a Smart Card: The serial number of the Smart Card of the Subject is given in this field. The serial number is used to relate the Subject to the cryptographic device used by the Subject. An individual number together with a checksum is used as a serial number. The number belongs to the number space reserved for the Smart Cards of the CA and it is stored on the Smart Card.

		Certificate stored in a USB token: The field can be utilized also in connection with other cryptographic devices to indicate the type of the Device in question. The field is used also in certificates stored in USB tokens and its contents are a character string defined by the CA.

Also other extensions may be used.

7.1.3 Algorithm object identifiers

At least the following algorithms are supported for signing and verification:

sha1withRSAEncryption OBJECT IDENTIFIER ::== iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 5; {1.2.840.113549.1.1.5}.

sha256withRSAEncryption OBJECT IDENTIFIER ::== iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11; {1.2.840.113549.1.1.11}

7.1.4 Name forms

Every DN will be in the form of an X.501 DirectoryString in accordance with section 3.1.1.

7.1.5 Name constraints

Subject and Issuer DNs comply with PKIX standards and are present in all certificates.

7.1.6 Certificate policy object identifier

The certificate policy object identifier will be present in issued certificates and will contain the OID of the policy according to which the certificate has been issued. The identifiers covered by this CPS have been given in section 1.2.

7.1.7 Usage of Policy Constraints extension

No stipulation.

7.1.8 Policy qualifiers syntax and semantics

The policy qualifier CPSuri may be used in the subscriber certificates. The value of the CPSuri points to TeliaSonera CA Services repository website where this CPS is published.

7.1.9 Processing semantics for the critical Certificate Policies extension

No stipulation.

7.2 CRL profile

The information contained in a Certificate Revocation List has been described below. The CRL is used to state which of the certificates, whose validity period has not yet expired, have been revoked.

CRL basic fields are listed in the table below:

Field name	Field description and contents
Version	This field states which of the CRL versions defined in the X.509 standard the CRL conforms to. The CRLs conform to the version 2.
Signature algorithm	The CRLs are signed by using the same algorithm used for signing the certificates.
Issuer	This field states the name of the Issuer of the CRL. The CRL issuer name is always the same as the Issuer name (the CA's name) in the certificates listed on the CRL.

This update	Date and time of the CRL issuance.
Next update	Date and time by which the next CRL shall be issued. The next CRL may be issued at any time after the issuing of the previous CRL, however, it shall be issued before the time stated in the “Next update” field. The time difference between “This update” and “Next update” is defined in section 4.9.7.
Revoked certificates	This field states the serial numbers of revoked certificates, and for each revoked certificate the date and time of revocation and the reason for revocation.

In general, following CRL extension may be used:

Extension	**Extension description and contents**
Authority key identifier	The identifier of the public key of the CRL Issuer is given in this field. The identifier can be used to identify the public key that corresponds to the private key used for the signing of the CRL. Within TeliaSonera PKI the SHA-1 hash algorithm is used to calculate the identifier.
CRL number	The CRL number is a number that indicates the position of the CRL in the sequence of issued CRLs. The numbering starts with 1, and it increases monotonically by one for each issued CRL. Based on the CRL number the user is able to determine if a certain CRL replaces another CRL.

7.2.1 Version number(s)

All issued CRL’s are X.509 version 2 CRL’s in accordance with the RFC 5280 “Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.

7.2.2 CRL and CRL entry extensions

CRL extensions will be supported in accordance with RFC 5280 “Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.

In general, the following entry extensions may be included in a CRL:

Extension	**Extension description and contents**
Reason Code of the CRL Entry	The reason for revocation can be one of the following: KeyCompromise, CACompromise, AffiliationChanged, Superseded, CessationOfOperation, CertificateHold
Invalidity date	The invalidity date provides the date, on which it is known or suspected that the private key was compromised or that the certificate otherwise became invalid. This date may be earlier than the revocation date in the CRL entry, which is the date at which the CA processed the revocation.

7.3 OCSP profile

7.3.1 Version number(s)

Version 1 of the OCSP specification as defined by RFC2560 (X.509 Internet Public Key Infrastructure Online Certificate Status Protocol) is implemented for the OCSP responders.

7.3.2 OCSP extensions

OCSP Nonce extension should be used in requests.

8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS

8.1 Frequency or circumstances of assessment

An annual Compliance Audit will be performed by an independent, qualified third party.

8.2 Identity/qualifications of assessor

The Compliance Auditor must demonstrate competence in the field of compliance audits, and must be thoroughly familiar with the requirements which a CA service imposes on the issuance and management of certificates.

8.3 Assessor's relationship to assessed entity

The Compliance Auditor should not have any financial, legal or organizational relationship with the audited party.

8.4 Topics covered by assessment

The purpose of the Compliance Audit is to verify that TeliaSonera and all engaged subcontractors are complying with the requirements of this CPS and TeliaSonera Production CPS. The Compliance Audit will cover all requirements that define the operation of a CA under these CPSes including:

a. The CA production integrity (key and certificate life cycle management); and
b. CA environmental controls.

The scope of the compliance audit includes CAs in scope of this CPS.

8.5 Actions taken as a result of deficiency

Depending on the severity of the deficiency, the following actions may be taken:

a) The Compliance Auditor may note the deficiency as part of the report;
b) The Compliance Auditor may meet with TeliaSonera and determine if the deficiency can be remedied and an action plan should be developed and steps taken to remedy the deficiency. Such steps could be to change applied procedures and/or updating the CPS;
c) The Compliance Auditor may report the deficiency and if the TeliaSonera CA Service deems the deficiency to have risk to the operation of the TeliaSonera or Customers CAs, the TeliaSonera CA Service operator may revoke the CA's certificate.

Should the CPS be updated in such a way that the new CPS is deemed to involve an amended degree of security; a new CPS with a new identity shall be drawn up (see section 1.2).

8.6 Communication of results

The Compliance Auditor shall provide the TeliaSonera CA Service management with a copy of the results of the Compliance Audit. The results will not be made public unless required by law.

9 OTHER BUSINESS AND LEGAL MATTERS

9.1 Fees

Fees are defined in applicable Customer agreement.

9.2 Financial responsibility

All stipulations regarding the section 9.2 Financial responsibility are specified in TeliaSonera Production CPS.

9.3 Confidentiality of business information

All stipulations regarding the section 9.3 Confidentiality of business information are specified in TeliaSonera Production CPS.

9.4 Privacy of personal information

All stipulations regarding the section 9.4 Privacy of personal information are specified in TeliaSonera Production CPS.

9.5 Intellectual property rights

The private signing key is the sole property of the legitimate holder of the corresponding public key identified in a certificate.

No part of this CPS (other than in accordance with the exceptions detailed below) may be reproduced, published in a database system or transmitted in any form (electronic, mechanical, photocopied, recorded or similar) without written permission from TeliaSonera AB.

However, permission generally applies for reproducing and disseminating this CPS in its entirety provided that this is at no charge and that no information in the document is added to, removed or changed.

Applications to reproduce and disseminate parts of this document in any other way may be made to TeliaSonera in accordance with section 1.5.2.

9.6 Representations and warranties

All stipulations regarding the section 9.6 Representations and warranties are specified in TeliaSonera Production CPS.

9.7 Disclaimers of warranties

All stipulations regarding the section 9.7 Disclaimers of warranties are specified in TeliaSonera Production CPS.

9.8 Limitations of liability

All stipulations regarding the section 9.8 Limitations of liability are specified in TeliaSonera Production CPS.

9.9 Indemnities

All stipulations regarding the section 9.9 Indemnities are specified in TeliaSonera Production CPS.

9.10 Term and termination

9.10.1 Term

This CPS remains in force until notice of the opposite is communicated by TeliaSonera on its web site in the TeliaSonera CA Service Repository (https://repository.trust.teliasonera.com).

9.10.2 Termination

Termination of this document will be upon publication of a newer version or replacement document, or upon termination of CA operations.

9.10.3 Effect of termination and survival

The conditions and effect resulting from termination of this document will be communicated, on TeliaSonera's web site in the TeliaSonera CA Service Repository (https://repository.trust.teliasonera.com), upon termination outlining the provisions that may survive termination of the document and remain in force.

9.11 Individual notices and communications with participants

TeliaSonera will define in any applicable agreement the appropriate provisions governing notices.

9.12 Amendments

TeliaSonera CA Policy Management Team is the responsible authority for reviewing and approving changes to this CPS. Written and signed comments on proposed changes shall be directed to the TeliaSonera CA Service contact as described in Section 1.5. Decisions with respect to the proposed changes are at the sole discretion of the TeliaSonera CA Policy Management Team.

9.12.1 Procedure for amendment

The only changes which can be carried out to this CPS without notification are linguistic amendments and rearrangements which do not affect the security level of the described procedures and regulations.

Changes which shall take place with notification can be made to this CPS 15 days after notification.

The TeliaSonera CA Policy Management Team will post the notification at the CPS publishing point at https://repository.trust.teliasonera.com. Changes affecting the terms of an agreement shall be notified in writing to the address given in the contact information of the signatory of the agreement.

TeliaSonera CA Policy Management Team decides which measures are taken in relation to the comments received. If comments received necessitate changes to the original change proposal which were not covered by the original notification, these changes may come into force no earlier than 15 days after publication of a new modified notification.

9.12.2 Notification mechanism and period

See 9.12.1

9.12.3 Circumstances under which OID must be changed

If TeliaSonera CA Policy Management Team determines that a new Object Identifier (OID) is required, TeliaSonera CA Policy Management Team will assign a new OID and required amendments will be made.

9.13 Dispute resolution provisions

All stipulations regarding the section 9.13 "Dispute resolution provisions" are specified in TeliaSonera Production CPS.

9.14 Governing law

All stipulations regarding the section 9.14 "Governing law" are specified in TeliaSonera Production CPS.

9.15 Compliance with applicable law

All stipulations regarding the section 9.15 "Compliance with applicable law" are specified in TeliaSonera Production CPS.

9.16 Miscellaneous provisions

All stipulations regarding the section 9.16 "Miscellaneous provisions" are specified in TeliaSonera Production CPS.

9.17 Other provisions

All stipulations regarding the section 9.17 “Other provisions” are specified in TeliaSonera Production CPS.

ACRONYMS

CA	Certification Authority
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
DER	Distinguished Encoding Rules
DN	Distinguished Name
DSA	Digital Signature Algorithm
EAL	Evaluation Assurance Level
EID	Electronic Identification
FIPS	Federal Information Processing Standard
HSM	Hardware Security Module
IETF	Internet Engineering Task Force
ISO	International Organization for Standardization
LDAP	Lightweight Directory Access Protocol
MD5	Message Digest 5
OCSP	On-line Certificate Status Protocol
OID	Object Identifier
PIN	Personal Identification Number
PKCS	Public Key Cryptography Standards
PKI	Public Key Infrastructure
PKIX	Public Key Infrastructure X.509 (IETF Working Group)
RA	Registration Authority
RFC	Request For Comments
RSA	Rivest-Shamir-Adleman asymmetric encryption algorithm
SEIS	Secure Electronic Information in Society
SHA –1	Secure Hash Algorithm
S/MIME	Secure Multipurpose Internet Mail Extension
SSL	Secure Sockets Layer
TTP	Trusted Third Party
UPS	Uninterruptible Power Supply
URI	Uniform Resource Identifier
URL	Uniform Resource Locator

DEFINITIONS

Access control:

The granting or denial of use or entry.

Activation Data:

Activation data, in the context of certificate enrollment, consists of a one-time secret communicated to the enrolling user (Subscriber) out of band. This shared secret permits the user to complete of the enrollment process.

Administrator:

A Trusted Person within the organization of a Processing Center, Service Center, Managed PKI Customer, or Gateway Customer that performs validation and other CA or RA functions.

Administrator Certificate:

A Certificate issued to an Administrator that may only be used to perform CA or RA functions.

Agent:

A person, contractor, service provider, etc. that is providing a service to an organization under contract and are subject to the same corporate policies as if they were an employee of the organization.

Application Server:

An application service that is provided to an organizational or one of its partners and may own a certificate issued under the organizational PKI. Examples are Web SSL servers, VPN servers (IPSec), object signer services, Domain Controllers, etc.

Authentication:

Checking the identity provided, e.g. when logging in, in the event of communication between two systems or when exchanging messages between users. General: strengthening of authenticity.

Authorization:

The granting of permissions of use.

Authorised representative:

An employee of the commissioner who has the authority to order and revoke certificates at the CA.

Asymmetric encryption algorithm:

An encryption technique which uses two related transformation algorithms: a public transformation, with the use of a public key, and a private transformation with the use of a private key. The two transformations are such that if the public transformation is known, it is mathematically impossible to derive the private transformation from this.

Base certificate:

See primary certificate.

Business process:

A set of one or more linked procedures or activities which collectively realize a business objective or policy goal, normally within the context of an organizational structure defining functional roles and relationships.

CA certificate:

Certificate which certifies that a particular public key is the public key for a specific CA.

CA key:

Key pair where the private key is used by the CA in order to sign certificates and where the public key is used to verify the same certificate.

Certificate:

The public key of a user, together with related information, digitally signed with the private key of the Certification Authority that issued it. The certificate format is in accordance with ITU-T Recommendation X.509.

Certificate extensions:

Sections of certificate content defined by standard X.509 version 3.

Certificate level:

Certificates exist at two levels: primary certificates and secondary certificates.

Certification Authority (CA):

An authority trusted by one or more users to manage X.509 certificates and CRLs.

Certification Chain:

An ordered list of Certificates containing an end-user Subscriber Certificate and CA Certificates, which terminates in a root Certificate.

Certificate Policy:

Named set of rules that indicates the applicability of a certificate to a particular community and/or class of applications with common security requirements. It is the principal statement of certificate policy governing the organizational PKI. The CP is a high-level document that describes the requirements, terms and conditions, and policy for issuing, utilizing and managing certificates issued by a CA.

Certification Practice Statement (CPS):

A statement of the practices, which a Certification Authority employs in issuing certificates. It is a comprehensive description of such details as the precise implementation of service offerings and detailed procedures of certificate life-cycle management and will be more detailed than the certificate policies supported by the CA.

Certificate Revocation List (CRL):

A periodically issued list, digitally signed by a CA, of identified Certificates that have been revoked prior to their expiration dates. The list generally indicates the CRL issuer's name, the date of issue, the date of the next scheduled CRL issue, the revoked Certificates' serial numbers, and the specific times and reasons for revocation. CRL can be used to check the status of certificates.

Confidential:

A security classification used to describe information which if disclosed could result in personal loss or minor financial loss. Personal information and tactical information would be deemed confidential.

Confidentiality:

Information that has an identifiable value associated with it such that if disclosed might cause damage to an entity.

Cross Certification:

The process describing the establishing of trust between two or more CAs. Usually involves the exchange and signing of CA certificates and involves the verification of assurance levels.

Cryptographic Module:

A unit in which encryption keys are stored together with a processor which can carry out critical cryptographic algorithms. Examples of cryptographic modules include EID cards.

Decryption:

The process of changing encrypted (coded) information into decrypted (legible) information. See also encryption.

Distinguished Encoding Rules (DER):

The Distinguished Encoding Rules for ASN.1, abbreviated DER, gives exactly one way to represent any ASN.1 value as an octet string. DER is intended for applications in which a unique octet string encoding is needed, as is the case when a digital signature is computed on an ASN.1 value.

Digital Signature:

The result of the transformation of a message by means of a cryptographic system using keys such that a person who has the initial message can determine that the key that corresponds to the signer's key created the transformation and the message was not altered.

Directory Service:

Database service which in this document relates to a database structure in accordance with standard X.500 or LDAP.

Distinguished Name (DN):

Every entry in a X.500 or LDAP directory has a Distinguished Name, or DN. It is a unique entry identifier through out the complete directory. No two Entries can have the same DN within the same directory. A DN is used in certificates to uniquely identify a certificate-owner.

Dual Control:

A process utilizing two or more separate entities (usually persons), operating in concert, to protect sensitive functions or information, whereby no single entity is able to access or utilize the materials, e.g., cryptographic key.

EID card:

Electronic ID card in the form of an active card containing certificates and keys while the front of the card can be used as a visual ID document.

Electronic identity check:

Identity check which can be carried out without the persons whose identity is being checked being present in person.

Electronic signature:

General signature designation created using IT. Digital equivalent to traditional signature. See also digital signature.

Encryption:

The process of changing information which can be interpreted (clear text) into encrypted information. The aim of the encrypted information is that it shall not be interpretable by anyone who does not hold exactly the right key (in symmetrical encryption) or exactly the right private key (in asymmetrical encryption) required to correctly decrypting the information.

E-mail Certificates:

Certificates utilized for encrypting and verifying digital signatures. Normally two separate certificate: one for encryption, the other for signature verification.

Entity:

Any autonomous element or component within the Public Key Infrastructure that participate is one form or another, such managing certificates or utilizing certificates. An Entity can be a CA, RA, Subscriber, Relying Party, etc.

FIPS 140-2:

Federal Information Processing Standard 140-2(FIPS 140-2) is a standard that describes US Federal government requirements that IT products shall meet for Sensitive, but Unclassified (SBU) use. The standard was published by the National Institute of Standards and Technology (NIST), has been adopted by the Canadian government's Communication Security Establishment (CSE), and is likely to be adopted by the financial community through the American National Standards Institute (ANSI). The different levels (1 to 4) within the standard provide different levels of security and in the higher levels, have different documentation requirements.

FIPS 180-1:

Standard specifying a Secure Hash Algorithm, SHA-1, for computing a condensed representation of a message or a data files.

Integrity:

Ensuring consistency of an object or information. Within security systems, integrity is the principle of ensuring that a piece of data has not been modified maliciously or accidentally.

ISO 11568-5:

Basic principles and requirements for Key lifecycle for public key cryptosystems, provides instructions to financial institutions in the development, implementation and/or the operation of systems and procedures throughout Key's lifecycle

Key:

When used in the context of cryptography, it is a secret value, a sequence of characters that is used to encrypt and decrypt data. A key is a unique, generated electronic string of bits used for encrypting, decrypting, e-signing or validating digital signatures.

Key holder:

In this context, a person, an organisation, an organisational unit or a function which has exclusive control of the private key, the public equivalent of which is certified in a certificate. See also subscriber.

Key Pair:

Often referred to as public/private key pair. One key is used for encrypting and the other key used for decrypting. Although related, the keys are sufficiently different that knowing one does not allow derivation or computation of the other. This means that one key can be made publicly available without reducing security, provided the other key remains private.

Log:

A sequential and unbroken list of events in a system or a process. A typical log contains log entries for individual events, each containing information on the event, who initiated it, when it occurred, what it resulted in, etc.

MD5:

A Message Digest Algorithm.

Non-repudiation:

Protection against the denial of the transaction or service or activity occurrence.

Non-repudiation services:

Service which aim to hold a key holder responsible for signed messages in such a way that they can be verified by a third party at a later point in time.

Object Identifier:

The unique alpha-numeric identifier registered under the ISO registration standard to reference a standard object or class.

Operator:

Employee of a CA.

Out of band process:

Communications which occur outside of a previously established communication method or channel.

PKCS #1:

Standard that provides recommendations for the implementation of public-key cryptography based on the RSA algorithm, covering the following aspects: cryptographic primitives; encryption schemes; signature schemes, etc.

PKCS #7:

A cryptographic message format or syntax managed and edited by RSA Laboratories. A standard describing general syntax for data that may have cryptography applied to it, such as digital signatures and digital envelopes.

PKCS #10:

A certificate request format or syntax managed and edited by RSA Laboratories. It is a standard describing syntax for a request for certification of a public key, a name, and possibly a set of attributes.

PKIX:

The Public Key Infrastructure (X.509) or PKIX is an IETF Working Group established with the intent of developing Internet standards needed to support an X.509-based PKI. The scope of PKIX extends to also develop new standards for use of X.509-based PKIs in the Internet.

PKI personnel:

Persons, generally employees, associated with the operation, administration and management of a CA or RA.

Policy:

The set of laws, rules and practices that regulates how an organization manages its business. Specifically, security policy would be the set of laws, rules and practices that regulates how an organization manages, protects and distributes sensitive information.

Primary certificate:

A certificate which is issued on the basis of identifying key holders other than by the key holder producing another certificate. Identification then normally takes place through the key holder instead producing an identity document.

PrintableString:

String format for representing names, such as Common Name (CN), in X.509 certificates. The encoding of a value in this syntax is the string value itself.

Private Key:

The private key is one of the keys in a public/private key pair. This is the key that is kept secret as opposed to the other key that is publicly available. Private keys a utilized for digitally signing documents, uniquely authenticating an individual, or decrypting data that was encrypted with the corresponding public key.

Public Key Infrastructure:

A set of policies, procedures, technology, audit and control mechanisms used for the purpose of managing certificates and keys.

Public:

A security classification for information that if disclosed would not result in any personal damage or financial loss.

Public Key:

The community verification key for digital signature and the community encryption key for encrypting information to a specific Subscriber.

RA policy:

A named set of rules for the RA's role in producing, issuing and revoking certificates and which regulates the applicability of certificates within a specific area of application.

Registration Authority (RA):

An entity that performs registration services on behalf of a CA. RAs work with a particular CA to vet requests for certificates that will then be issued by the CA.

Re-key:

The process of replacing or updating the key(s). The expiration of the crypto period involves the replacement of the public key in the certificate and therefore the generation of a new certificate.

Relative Distinguished Name (RDN):

A Distinguished Name is made up of a sequence of Relative Distinguished Names, or RDNs. The sequences of RDNs are separated by commas (,) or semi-colons (;). There can be more than one identical RDN in a directory, but they must be in different bases, or branches, of the directory.

Relying Party:

A person or entity that uses a certificate signed by the CA to authenticate a digital signature or encrypt communications to a certificate Subject. The relying party relies on the certificate as a result of the certificate being sign by a CA, which is trusted. A relying party normally is but does not have to be a Subscriber of the PKI.

Repository:

A place or container where objects are stored. A data repository is technology where data is stored logically. In PKI terms, a repository accepts certificates and CRLs form one or more CAs and makes them available to entities that need them for implementing security services.

Revocation:

In PKI, revocation is the action associated with revoking a certificate. Revoking a certificate is to make the certificate invalid before its normal expiration. The Certification Authority that issued the certificate is the entity that revokes a certificate. The revoked status is normally published on a certificate revocation list (CRL).

RSA:

A public key cryptographic algorithm invented by Rivest, Shamir, and Adelman.

Secondary certificate:

A certificate issued on the basis of another certificate, the primary certificate. This means that the issuing CA relies on the CA which issued the primary certificate, i.e. accepts the public key's certification of the key holder, which is turn requires reliance on the identification of the key holder when issuing the primary certificate being correct.

Sensitive:

Used to describe the security classification of information where the information if disclosed would result in serious financial loss, serious loss in confidence or could result in personal harm or death.

Signature Verification Certificate:

Often referred to as simply a Signature Certificate. It is the certificate containing the public key used to verify a digital signature that was signed by the corresponding private key.

Split Knowledge

A condition under which two or more parties separately and confidentially have custody of components of a single key that, individually, convey no knowledge of the resultant cryptographic key. The resultant key exists only within secure cryptographic devices.

SSL Client Certificate:

Certificate utilized to verify the authentication of an end user to a server when a connection is being established via a SSL session (secure channel).

SSL Server Certificate:

Certificate utilized to verify the authentication of a web or application server to the end user (client) when a connection is being established via a SSL session (secure channel).

Storage module:

In this document relates to cryptographic module.

Subject:

Entity identified in a certificate as the holder of the private key associated with the public key given in the certificate. [ETSI TS 101 456 v1.2.1] Subject can also be a device (a data network component or software, hereafter referred to as “Device”).

Subscriber:

Entity subscribing with a Certification Authority on behalf of one or more Subjects. The Subject may be a Subscriber acting on its own behalf. [ETSI TS 101 456 v1.2.1]

Surveillance Camera:

A surveillance camera is a video recording device used for detection and identification of unauthorized physical entry to a secured area. A camera used for recording a signing ceremony for auditing purposes is not considered a surveillance camera.

Symmetric encryption:

Encryption system characterised by both the sender and the recipient of encrypted information using the same secret key for both encryption and decryption.

Threat:

A danger to an asset in terms of that asset's confidentiality, integrity, availability or legitimate use.

Token:

Hardware devices, normally associated with a reader, used to store and/or generate encryption keys, such as smartcards and USB tokens.

Trusted Third Party (TTP):

A party on which two or more collaborative parties rely. A TTP carries out services for the collaborative parties, such as time-stamping, certificate issuing, etc.

Trusting party:

A recipient of a certificate which trusts this certificate on authentication,

verification of digital signatures and/or encryption of information. See also Relying Party.

Unambiguous identity:

An identity comprising a set of attributes which relate unambiguously to a specific person. The unambiguous connection between the identity and the person may be dependant on the context within which the identity term is used. Certain contexts may require assistance from the current registrar of various attributes.

URI

Universal Resource Indicator - an address on the Internet.

UTF8String

UTF-8 is a type of Unicode, which is a character set supported across many commonly used software applications and operating systems. UTF-8 is a multibyte encoding in which each character can be encoded in as little as one byte and as many as four bytes. Most Western European languages require less than two bytes per character. Greek, Arabic, Hebrew, and Russian require an average of 1.7 bytes. Japanese, Korean, and Chinese typically require three bytes per character. Such Unicode is important to ensure that universal /foreign characters are supported.

Verification:

The process of ensuring that an assumption is correct. This term relates primarily to the process of ensuring that a digital signature represents the party which the signed information details as its issuer.

Vettor:

A person who verifies information provided by a person applying for a certificate.

Vulnerability:

Weaknesses in a safeguard or the absence of a safeguard.

Written:

Where this CPS specifies that information shall be written, this requirement is generally also met by digital data provided that the information it contains is accessible in such a way that it is useable by the parties involved.

X.500

Specification of the directory service required to support X.400 e-mail initially but common used by other applications as well.

X501 PrintableString:

String format for representing names, such as Common Name (CN), in X.509 certificates. The encoding of a value in this syntax is the string value itself; an arbitrary string of printable characters.

X.509:

ITU standard that describes the basic format for digital certificates.