	Date 2007-10-18	**Page No.** 1 (46)
Creator	**Identifier**	**Version** 1.0 Approved
Approved by	**Relation**	

TeliaSonera Root CA v1
Certificate Practice Statement

Published by: TeliaSonera AB

1. Contents

2. Version history

Version number	Document name	Version Date	Description
V 1.0	TeliaSonera Root CA v1 – Certificate Practice Statement	2007-10-18	The first TeliaSonera Root CA v1 Certification Practice Statement

All published versions are available at:
http://repository.trust.teliasonera.com/.

3. Terminology

***Activation data**: Access code (e.g. PIN-code), used by the Subject to activate his private key. The PIN code must be entered separately every time the key is used.*

***Applicant for Certificate:** A person to whom a certificate is applied for. After issuing of the certificate the person is called Subject.*

***Certificate:** The public key of a user, together with some other information, rendered unforgeable by encipherment with the private key of the Certification Authority which issued it. [ISO/IEC 9594-8; ITU-T X.509]*

***Certificate Manufacturer (CM):** An entity that is responsible for expressly assigned tasks in the manufacturing and delivery of certificates, signed by a certification authority, or of Signature-Creation Devices. An example of a Certificate Manufacturer within Sonera PKI is the Card Manufacturer.*

***Certificate Policy (CP):** A named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements. [ISO/IEC 9594-8; ITU-T X.509]*

***Certificate Revocation List (CRL):** A list containing the serial numbers of revoked certificates from a given CA, together with other revocation information.*

***Certification Authority (CA)**: An authority trusted by one or more users to create and assign certificates. Optionally the Certification Authority may create the users' keys [ISO/IEC 9594-8; ITU-T X.509]. In this Policy the CA is TeliaSonera Finland Oyj.*

***Certification Practice Statement (CPS):** A statement of the practices that a Certification Authority employs in issuing certificates. [RFC 2527].*

***Cryptographic Device:** A device used by a Subject, implementing cryptographic algorithms and containing the private key of the Subject. The cryptographic device used as a Signature-Creation Device within Sonera PKI is a smart card or USB token.*

***Cryptographic Module:** A set of hardware, software, and firmware implementing cryptographic algorithms and used by the CA to ensure the secure creation, storage, and use of the CA cryptographic keys.*

***Customer Organization:** TeliaSonera Finland Oyj's (hereafter referred to as "Sonera") business customer who uses Sonera's certification services.*

***Electronic Signature:** Data in electronic form which are attached to, or logically associated with, other electronic data and which serve as a method of authentication [EU Directive].*

***Issuer:** The field in the certificate that defines the signatory of the certificate.*

***Key pair:** A key pair is composed of a private key created for the use by the Subject, and the associated public key.*

***Policy Authority:** An authority within the CA who sets, approves, and manages the Certificate Policy and maintains the applied practices.*

***Private key:** That key of a Subject's asymmetric key pair, which can only be used by the Subject by entering the activation data related with the key.*

***Public key:** That key of a Subject's asymmetric key pair, which is used by Relying Parties.*

***Public Key Infrastructure (PKI)**: The set of hardware, software, people, policies, and procedures needed to create, manage, store, distribute, and revoke certificates based on public-key cryptography [PKIX Roadmap].*

***Registration Authority (RA):** An entity that is responsible for identification and authentication of certificate Subjects, but that does not sign or issue certificates (i.e. an RA is delegated certain tasks on behalf of a CA) [RFC 2527].*

***Registration Officer:** An individual carrying out Registration Authority duties i.e. responsible for approval of certificate generation and dissemination procedures.*

***Relying Party**: A user or agent that relies on the data in a certificate in making decisions [ISO/IEC 9594-8; ITU-T X.509].*

***Repository:** A system where the public documents concerning certification operations have been stored by the CA, and from where they may be retrieved. The repository related to certificates may be accessed via the internet at http://repository.trust.teliasonera.com/.*

***Revocation Service:** The service that receives revocation requests and passes the authorized requests to the CA.*

***Revocation Status Service:** The service that the Relying Parties can use to check the status of the certificate, e.g. directory*

***SAP state:** A mobile subscription is in SAP state when it has been discontinued at the customer's request so that it can still be taken back into use. SAP state bars all outgoing and incoming traffic of the mobile subscription.*

***Signature-Creation Device (SCD):** A SIM card, USB-token, PKCS#12-file, or smart card, which contains the Subject's private key.*

TeliaSonera: *In this document the term refers to TeliaSonera AB.*

Subordinate Certificate Authority: *CA whose certificate signature key is certified by another CA, and whose activities are constrained by that other CA.*

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]*

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").*

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 TeliaSonera Root CA v1 uses when issuing certificates, and that all applicants, Subscribers, Subjects, and users shall follow in connection with these certificates. The structure of this CPS is based on the document RFC 2527 ”Certificate Policy and Certification Practices Framework”.

Certificates issued by this CA may only be subordinate CA. This CPS does not stipulate any restraints for issuing end-entity certificates under those subordinate CA's.

Certificates can be used for certificate signing, certificate revocation list signing and OCSP answer signing.

Policies which direct implementation and maintenance of TeliaSonera CA's (hereafter referred to as ”the CA”) services and define the rules for applying, issuing, and use of certificates have been described in the Certificate Policies ”TeliaSonera Finland CP-Class2”. The CA issues certificates according to the security requirements defined in the aforementioned Certificate Policies.

1.2. Identification of the document

The object identifier if this document is { 1.2.752.35.4.2.1}.

1.3. Community and applicability

1.3.1. Certification Authority (CA)

The Certification Authority operating in compliance with this Certification Practice Statement is TeliaSonera. The name of the Certification Authority in the “Issuer” field of the certificate is “TeliaSonera Root CA v1”.

In addition to issuing and publishing certificates the CA also provides the Revocation Service and the Revocation Status Service.

1.3.2. Registration Authority (RA)

This CA is only issuing subordinate CA's which may only be installed in the same CA-system as this CA. This means that only specially assigned CA personal may issue certificates under this CA.

1.3.3. Subject

The Subject of a certificate can only be a subordinate CA which have exclusive use of the private key corresponding to the public key in the certificate is intended.

1.3.4. Applicability

All certificates issued by TeliaSonera Root CA are stored in an HSM and are used for issuing certificates.

An organization that has agreed to and executed an Agreement with TeliaSonera, and meets the requirements of the TeliaSonera Public Root Certificate Policy can have a hosted CA at the TeliaSonera site.

1.4. Contact details

This CPS is administered by TeliaSonera CA Policy Authority.

TeliaSonera Sverige AB

Customer Service

Box 352

831 25 Östersund, Sweden

Telephone: +46 (0)20 32 32 62

E-mail: e-id@telia.se

Web: www.telia.se

2. General provisions

2.1. Obligations

General obligations of the parties have been defined in the Certificate Policies (paragraphs 2.1.1 – 2.1.4).

The Subscriber has been obliged by the Certificate Policies to ensure that the Subject commits to the obligations laid down to him. The Subscriber shall issue instructions to the Subject for fulfilling the following obligations:

- The Subject shall submit sufficient and correct information for applying for a certificate, particularly with regard to registration.
- The Subject shall use his private key only for purposes accepted by the Subscriber.
- The Subject shall keep his private key and the PIN code needed for its activation protected in such a way that they are not lost, disclosed, or do not fall into the possession of others.
- The Subject shall notify, without any reasonable delay according to the Subscriber's instructions, either the CA directly or the Registration Officer of his own organization if he suspects that his private key or PIN code may be in possession of another person or if he knows that the information in the certificate does not hold true any more.
- If the Subject suspects or knows that his private key or PIN code has been disclosed to others, the use of the private key shall be discontinued immediately and permanently.

The document "TeliaSonera CA Customer's Responsibilities" drawn up by the CA includes instructions to be given also to the Subjects.

2.2. Liability

2.2.1. Limitations on the CA's liability

The CA shall not be liable for legal acts or other commitments that come about when a certificate is used.

The CA shall not be liable for consequential damages.

The CA shall not be liable for damages that result from force majeure.

The CA shall not be liable for damages caused by the use of a certificate contrary to the agreement or to the terms of use.

The CA shall not be liable for damages resulting from disclosure of the private keys or the activation data required for their use.

The CA shall not be liable for prevention of the use of certification services due to unavailability of general telecommunications connections or networks.

If bugs or defects that have an injurious effect on the use of services are found in CA-owned tools needed for the use of certification services, the CA has the right to change the tools in question.

The CA shall not be liable for the functionality, security, or suitability for the use of certification services of the Subject's or Customer Organization's equipment or software needed for the use of certification services.

2.3. Financial responsibility

Financial responsibility has been described in the Certificate Policies.

2.4. Customer feedback

Reclamation procedures shall follow TeliaSonera's general delivery terms for business customers concerning services.

2.5. Interpretation and enforcement of Certification Practice Statement

2.5.1. Governing law

Certification services shall be governed by the laws of Finland.

2.5.2. Dispute resolution procedures

Any disputes between the Customer Organization and the CA, arising out of or in connection with certification services, shall be settled primarily by negotiations. If no agreement can be reached, the dispute shall be submitted to arbitration under one arbitrator.

2.6. Fees

Fees for certification services shall be charged according to the agreement between the Customer Organization and the CA.

The Revocation Status Service, however, is available to the Relying Party free of charge.

2.6.1. Refund policy

TeliaSonera's general delivery terms for business customers concerning services shall be applied to refunds. As a general rule, the CA does not return payments received already from the Customer Organization. Limitations related to liabilities for damages have been given in paragraph 2.2 ”Liability” of this document as far as certificates are concerned, and the general limitations have been given in paragraph 9.2 of Sonera's general delivery terms for business customers concerning services.

2.7. Publication and repository

The published information is available in the repository 24 hours per day, 7 days per week, except for the necessary maintenance breaks. The CA shall not be responsible for the availability of service experienced by the user if a fault or break occurs in systems or services that are not under the control of the CA.

2.7.1. CA information and repositories

The CA publishes Certificate Revocation Lists in accordance with paragraph 4.4.5 ”CRL issuance” in the LDAP directory. The addresses of the CRLs have been given in paragraph 4.4.6 ”CRL checking requirements”, and they can also be found in the “CRL Distribution Point” field in the certificate.

The following CA information and information concerning certification services are publicly available on the internet at: http://repository.trust.teliasonera.com.

- valid Certificate Policy (CP) and its former published versions,
- valid Certification Practice Statement (CPS) and its former published versions,
- document ”Sonera CA Customer’s Responsibilities”,
- Description of the register of customers of TeliaSonera’s information security services,
- CA certificates.

2.7.2. Frequency of publication

Publicly accessible information has been made permanently available. Information is updated on the above-mentioned CA’s www page immediately when there have been changes in the information.

CRLs are published at least once in a day. The CRL validity period is 168 hours.

2.7.3. Access control

The CA’s www pages are publicly available on the internet. The Certificate Revocation List is available in the CA’s LDAP-directory.

2.8. Compliance audit

2.8.1. Auditing carried out by the CA

The CA controls the information security of the different sub-areas of its own activities by reviewing log files and by occasional inspections. In internal auditing it is possible to use also resources of TeliaSonera’s Corporate Security Unit. The CA can also inspect the operations of Registration Authorities operating in Customer Organizations. If any defects come up in inspections carried out by the CA, it will take the necessary measures to correct them.

The CA’s subcontractors implement also their own auditing programs.

2.8.2. Auditing carried out by external auditor

The CA’s activities are audited at least annually by an external auditor. In the auditing it is evaluated whether the CA operates according to the published Certificate Policy and Certification Practice Statement, and whether the CA follows the Security Policy it has defined. In auditing, all processes of certification operations, systems used by the CA, and its organization, are reviewed. Auditing covers also the activities of CA’s subcontractors, like Card Manufacturers and Registration Authorities, except for RA’s operating in Customer Organizations. External auditing is conducted regularly and always when there are substantial changes in processes or systems. The subcontractors of the CA use auditing performed by a third party, according to standard BS7799, for example.

The CA’s subcontractors use, for example, auditing based on standard BS7799 carried out by a third party.

2.8.2.1. Auditor and the necessary qualifications

The auditor accepted by the CA shall be an independent, well-known company of good reputation in the industry. The auditor is expected to have sufficient expertise and familiarity with utilization of PKI technologies and auditing of certification operations.

2.8.2.2. Measures after discovering a defect

The auditor delivers a report of the results of the auditing to the CA. If defects have been found in the operations, the CA will take measures to correct them.

In order to correct defects in the CA's own activities, a plan is drawn up including timetables for corrective measures based on the criticality of the defect and the time required for correction.

If defects have been discovered in the activities of the CA's subcontractors, the parties concerned shall be informed, and each subcontractor is expected to correct the defect found within a reasonable time.

If the auditing results in a need to change the CP or the CPS, the changes will be notified according to the procedures described in chapter 8 of the document in question.

2.8.2.3. Communication of results

The report given by the auditor is for internal use of the CA. The CA can inform a subcontractor about the auditing results of the subcontractor's operation. Information about the report can be given to third parties or it can be published partly or in its entirety by the decision of the management of the CA's organization.

2.9. Confidentiality

2.9.1. Types of information to be kept confidential

Information regarding Subscribers and Subjects that is submitted at registration will be kept confidential by the RA and the CA. Finnish law is applied to concealment of confidential information and to the non-disclosure agreements possibly made between the parties. The CA releases information collected and generated in connection with certification operations within the limits permitted and obliged by the Finnish law.

2.9.2. Types of information not considered confidential

Information contained in certificates is not considered confidential.

Also information contained in the Certificate Revocation Lists is public. Identification data of the Subject is not published on the CRL but the revoked certificate is identified based on its serial number.

2.9.3. Release of information to law enforcement officials

The CA releases information collected or generated in connection with certification operations only within the limits permitted and obliged by the Finnish law.

2.9.4. Release of information to the Subject

The Subject has the right to obtain information concerning himself based e.g. on the Personal Data Act.

2.10. Intellectual property rights

Intellectual property rights have been described in the Certificate Policies in paragraph 2.10.

3. Identification and authentication

3.1. Naming practices for CA certificates

In a CA certificate, the CA's name shall be a unique X.501 Distinguished Name (DN), which is used both in the ”Issuer” field and ”Subject” field of the certificate and includes the following attributes:

- commonName, (CN),
- organizationName, (O),

For this policy, the CA has the following values:

- CN=TeliaSonera Root CA v1
- O=TeliaSonera

3.2. Initial registration

3.2.1. Naming of Subjects

In a Certificate, the name of the Subject can be composed of the following attributes:

- commonName, (CN),
- givenName, (GN),
- Surname, (S),
- serialNumber, (SN),
- organizationName, (O),
- organizationalUnitName, (OU),
- countryName, (C),
- Location,
- State.

Of the above-mentioned attributes CN and O are obligatory in all certificates. The CA is always responsible for defining attribute O. The other attributes of the certificate can be defined by the customer.

When necessary, also other attributes can be included in the Subject's name.

3.2.2. Meanings and interpretation of names

Meanings and interpretation of names have been described in the Certificate Policy.

3.2.3. Uniqueness of names

Requirements related to uniqueness of names have been defined in the Certificate Policies.

3.2.4. Name claim dispute resolution procedure

Settlement procedure of name claim disputes has been defined in the Certificate Policies.

3.2.5. Authentication of organization identity

The identity of a new Customer Organization is verified on the basis of information in the order or agreement by verifying the existence of the company and the Business Identity Code or other similar identifier from a database maintained by a third party. The Subscriber's administrative contact person who grants the necessary authorizations in the Customer Organization has been identified in the order or agreement. The authenticity of the contact person is checked by calling him via the Customer Organization's PBX number or when there is no switchboard, by making a call to some other number in the organization, which is looked up from a directory maintained by a third party.

3.2.6. Verifying of Subject identity and name

For organizationName in subject, it is taken from the authentication of the organization identity. Other parts of the subject is verified against the order or agreement with the Customer Organization.

3.2.7. Method to prove possession of private key

All CA private keys are generated within the system and stored in a HSM.

3.3. Revocation request

3.3.1. 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 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.

The information that has been used for verification of the identity of the person requesting revocation, and the revocation request reception time, will be recorded.

If other authentication methods are used, the authentication information and reason to use it will be recorded.

4. Operational requirements

4.1. *Certificate application*

Applying for a certificate is done within the CA system with the keys generated within the CA system.

When applying for a certificate, all the required information must be given. The information is given in a form or by using tools delivered by the CA.

4.2. *Certificate issuance*

The CA system accepts only such certificate requests the origin of which can be authenticated based on an electric signature.

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.

4.3. *Certificate revocation and suspension*

4.3.1. Circumstances for revocation

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

- The customer organization of a certificate asks for revocation of the certificate (for any given reason).
- The private key of the subordinate CA is lost, or it has been stolen or disclosed to others.
- The certificate has not been issued according to the applicable Certificate Policy or this Certification Practice Statement.
- Essential breach by the Subject or Subscriber of the agreement made with the CA.

A certificate can be revoked or suspended also under the following conditions:

- There are reasons to suspect that the private key of the Subject is lost, or that it has been stolen or disclosed to others.
- Breach by the Subject or Subscriber of the agreement made with the CA.
- There is another specific reason for the revocation of a certificate.

4.3.2. Who can request revocation

As a rule, only the customer organization or another contact person of the agreement, can ask for the revocation of a certificate. However, the CA can also initiate the revocation based on any reliable and tenable information brought by any given party, which refers to revocation conditions described in paragraph 4.4.1 “Circumstances for revocation”.

4.3.3. Procedure for revocation request

4.3.3.1. 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 inform the Revocation Service immediately, when a reason for the revocation of a certificate comes to his 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.

4.3.3.2. Revocation request processing

The identity of the originator of a revocation request is verified according to paragraph 3.5 “Revocation request”.

Certificates are suspended, i.e. cancelled for the time being, always after reception of an authorized and validated revocation request. Certificates shall be permanently revoked after six (6) months from suspension, at the latest, unless they have been reinstated.

4.3.4. Certificate suspension

See paragraph 4.4.3.2 ”Revocation request processing”.

4.3.5. CRL issuance

The Revocation Status Service is implemented by publishing Certificate Revocation Lists (CRLs), electronically 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 24 hours**.
- The validity time of every CRL is **hundred-sixty-eight (168) hours**.

The CRL is available in the directory 24 hours per day, 7 days per week, except for the necessary maintenance breaks. The CA shall not be responsible for availability of the service experienced by a user, if the fault or break appears in a system or service that is not under the control of the CA.

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

4.3.6. CRL checking requirements

Before trusting in a certificate the Relying Party must make sure that the certificate has not been listed in the CRL. A certificate cannot be reasonably relied on if the Relying Party does not diligently follow the CRL checking procedures denoted below:

- A Relying Party that retrieves a CRL from the directory shall ensure himself of the authenticity of the CRL by checking its digital signature and the certification path related to it.

- The Relying Party shall also check the validity period of the CRL in order to make sure that the information in the CRL 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 CRL 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 CRLs can be found in the addresses given below.

ldap://crl-1.trust.telia.com/cn=TeliaSonera%20Class2%20CA%20v1,o=TeliaSonera?certificaterevocationlist;binary

http://crl-2.trust.telia.com/TeliaSoneraClass2CAv1.crl

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

4.4. Certificate reinstatement

The Customer Organization may request reinstatement of a revoked certificate.

The certificate reinstatement request is processed and accepted by an employee of the CA, separately authorized to do this task. Before execution of the required reinstatement the Revocation Service shall make sure that the request comes from a person authorized by the CA.

The Customer Organization shall deliver the certificate reinstatement request or the confirmation of the request in writing (in an e-mail message, electric form, or fax) to the CA. The written request or confirmation is recorded together with its reception time and with the information that has been used for verifying the identity of the Registration Officer. Accordingly, the reinstatement request that has been delivered to the Revocation Service for execution shall be recorded with the following information: contents of the request, reception time of the request, name of the authorized employee of the CA, and the reinstatement execution time.

4.5. Security audit procedures

4.5.1. Types of events recorded

The CA records automatically or manually the following information which is essentially related to the certification operations:

Audit logs related to the life cycle of the CA private key

- generation, back-up, recovery, and destruction of the private key
- life cycle maintenance events of the cryptographic module

Certificate life cycle maintenance events of the CA certificates.

- certificate applications, certificate requests, and certificate renewal requests for new keys and for keys that have been in use already
- certificate revocations and suspensions

- reinstatements of suspended certificates
- issuances of certificates
- issuances of CRLs

Events related to the maintenance of the information security:

- events that have been created when using the tools delivered by the CA for certificate requests
- measures taken by the CA personnel and directed at the CA system or security systems, e.g. installation of software, hardware and software updates, recovery from back-up media, system shutdown and restart, and changes in the system settings
- system downfalls, hardware failures, and other anomalies in the systems
- events encountered by routers, firewalls, and intrusion detection systems
- events of access control of the CA system premises

The information to be recorded includes the type, date, and time of the event, and for log files that are automatically recorded, a serial number and the identifier of the system producing the log.

The following information is recorded at the RA office of the CA:

- authorization forms of Registration Officers in Customer Organizations
- certificate orders from Customer Organizations including the name of the ordering Registration Officer
- events of look-up from the databases of third parties.

The following information concerning revocation requests is recorded at the Revocation Service:

- information concerning the person requesting revocation
- method of verifying the identity of the person requesting revocation
- revocation request reception time
- information concerning the certificate to be revoked.

4.5.2. Processing of audit logs

The CA personnel examine regularly audit logs that are essential for the security and operations.

On the basis of alarms generated by the systems, the audit logs are examined to clarify suspicious or abnormal events.

4.5.3. Retention period for audit logs

The audit logs of the CA system will be stored at least for a year after they have been generated, and they will be kept in archive for a time period given in paragraph 4.7.2 ”Retention period for archive”.

The audit logs produced by the other systems of the CA will be retained at least for ten (10) days in the systems themselves. Furthermore, logs may be moved also to a separate log file server for retention. Depending on the system the log information may be transferred as such or after processing to another storage media for storing in archive.

4.5.4. Protection of audit logs

The logs, which are manually filed, and the logs automatically produced by the systems of the CA, have been protected from changing, destroying, and from illicit reading by user rights management and physical access control.

The audit logs of the CA system have been protected with a digital signature.

4.5.5. Audit log backup procedures

Back-up copies of the audit logs of the CA system are made regularly according to separately defined schedules.

The back-up practices for audit logs of other systems of the CA depend on the system in question and on the criticality of the log information. Back-ups are made regularly of the most essential log information.

4.5.6. Audit log collection system

The systems of the CA support collection of audit logs. Certain production system maintenance measures, e.g. changes and updates to the system as well as maintenance measures concerning the CA keys, are entered manually into a separate log.

The audit logs automatically generated in the CA system are stored at the application, network, and operating system level. The CA personnel generate manual logs in the form of minutes, either electronic or physical.

4.5.7. System vulnerability assessment

The CA assesses the vulnerability of its critical systems regularly to provide against penetration attacks by outsiders. On the basis of the assessment results the configurations of firewalls and other systems are updated and operation policies and practices are revised, if necessary.

4.6. Records archival

4.6.1. Types of events recorded

The CA stores in the archive records of the most critical events described in paragraph 4.6.1 “Types of events recorded”, e.g. of all audit logs generated by the CA system and of the manually generated logs of maintenance measures concerning the CA system.

In addition to the above mentioned audit logs, records of at least the following information are stored in the archive:

- agreements made with Customer Organizations,
- certificate applications and orders received from Customer Organizations,
- issued certificates,
- certificate revocation requests received by the Revocation Service,
- certificate reinstatement requests received by the CA (for cancellation of suspension of certificates),
- revocations of certificates,

- all CP versions published by the CA,
- all CPS versions published by the CA,
- reports on security audits performed by external auditors.

The archive can include both electronic format and physical format files.

4.6.2. Retention period for archive

Records of all information that is denoted in paragraph 4.7.1 “Types of events recorded” are stored in the archive for at least three (3) years after their generation.

The issued certificates with the associated registration information as well as possible revocation information are stored in the archive for at least three (3) years from the expiration date of the certificate.

However, the CA does not guarantee the storage of archive after the operation of the CA has terminated.

4.6.3. Protection of archive

The archive, which contain the information produced by the CA system and that is related to the generation and revocation of certificates, as well as the certificates themselves, are filed in fireproof premises protected with access control, and the information is protected with electronic signatures. The archive containing information on system changes and service events are filed in the same premises.

The information, which is produced by other systems of the CA and which is to be filed, is kept in premises protected with access control, either in a lockable cabinet or in a safe, depending on the criticality of the information.

4.6.3.1. Requirements for time-stamping of records

The filed information does not contain actual time-stamps. All the logs produced by the CA system contain date and time information. The time is synchronized with an external UTC time source.

Also the logs produced by other systems of the CA contain date and time information. In some of those systems the time is synchronised with an external UTC time source.

4.6.4. Archive backup procedures

Backup copies are taken of the archive information produced by the CA system to provide against loss or destruction of information, so that if the actual archive is destroyed the information can be recovered from back-up copies.

4.6.5. Procedures to obtain and verify archive information

The archive information is retained so that only the authorized CA personnel can have access to it. Those persons carrying out auditing according to paragraph 2.8 “Compliance audit” are entitled to study the archive information. Otherwise archive information is delivered only based on a written request and within the limits permitted and obliged by the Finnish law, under the supervision of Sonera’s Corporate Security Unit.

A Subject may obtain archive information that concerns him. The information is delivered free of charge within the limits of the inspection right defined in the of personal data protection act. Otherwise a reasonable fee is charged, based on the amount of work for the searching and delivery of information.

The CA makes its best endeavours to ensure that the archive information required at a given time can be searched and checked during the whole archive retention period.

4.7. CA key changeover

A new signing key is generated to the CA before the usage period of the current (old) signing key for signing certificates expires. A new name is created to the CA for the new signing key, and the name can be found in the “Issuer” field of the certificates issued by the CA.

The key is used for the signing of certificates only for as long as to ensure that the validity period of even the last certificate signed with it expires before the usage period of the key expires. This ensures that the CRL can always be signed by using the same key that was used for signing the certificates that might be published in the CRL.

The following certificates are published in connection with key changeover:

- old CA public key certificate signed by new CA private key,
- new CA public key certificate signed by old CA private key,
- new CA public key certificate signed by new CA private key.

4.8. Compromise and disaster recovery

4.8.1. Disaster recovery

In the event of an emergency or a disaster the CA follows the process defined in the Business Continuity Plan as well as other directions established to provide against such events. In the event of a disaster the issuance of certificates is interrupted and the data communications links to the CA production systems are disconnected until the conditions have returned to normal.

4.8.2. Computing resources, software, and/or data are corrupted

The production system has been duplicated. In the case of hardware failure the production is transferred to a back-up device. In the case of software failure the software will be re-installed. If the data are corrupted they are recovered from a back-up copy that is always made before and after every change in the system and regularly otherwise. A back-up copy is made of the most critical information at least four times per week. A more wide-ranging destruction of a part of the production system causes interruption of the service, the length of which depends on the extent of the problem.

4.8.3. CA private key compromise

In the event of the CA private key compromise the procedure defined by the CA shall be followed. The use of the private key is ceased immediately. The CRLs signed with this key shall be removed from the Revocation Status Service immediately, which implies that certificates signed with the compromised key cannot be reasonably relied on. The CA notifies the Customer Organizations and other CAs, with which it has an agreement, of the key compromise and of the measures required, either by e-mail or by mail. Continuation of the operation concerning the certificate class in question requires the generation of new CA signing keys and creation of new certificates to the Subjects.

4.8.4. Secure facility after a natural or other type of disaster

The premises for the certification services production have been constructed to be secure taking into account the probable risks implied by the geographical location of the premises.

4.9. CA termination

The termination of the CA operations is an occasion where the issuance of certificates ceases permanently. The CA key changeover or the transfer of certification operations with the associated responsibilities to another organization is not considered as CA termination.

The essential measures related to the termination of the operation have been described in the Certificate Policies. The Policy Authority of the CA is responsible for executing the policies for the applicable part.

The CA informs of the CA termination as follows:

- to Subscribers and/or to Customer Organizations and to other CAs with which it has an agreement, in writing to the customer's contact address,
- to Registration Authorities, to Certificate Manufacturers, and to other subcontractors, with a letter that at the same time serves as a notice of termination of the agreement for carrying out certain CA assigned operations on behalf of the CA.

Furthermore, the CA takes the following measures in connection with the termination of its operation:

- The CA cancels all subcontractor authorizations related to certification operations as well as the subcontractors’ access rights to the systems of the CA.
- The CA terminates the Revocation Status Service, an thereafter the certificates issued by it cannot be reasonably relied on any more.
- The CA destroys or takes out of use its private signing keys so that they cannot be brought into use any more.

5. Physical, procedural and personnel security controls

5.1. Physical and environmental controls

Physical security controls are used for controlling access to software and hardware of the CA. These include the workstations of the CA system and the separate cryptographic modules and devices. A physical access control system records the arrivals to the CA premises and the departures from them.

The keys that are used for signing certificates and CRLs are physically protected so that they can never be disclosed as a result of a physical attack.

Back-up copies and data media have been stored in the CA premises in such a way that the loss, tampering, and unauthorised use of the recorded data has been prevented with a sufficient protection level. The back-up copies are maintained both for the recovery of data as well as for retention of important data files.

For the execution of the principles of physical security that have been described in the Security Policy the CA maintains descriptions of physical security management of the production system.

5.1.1. Site location and construction

The trustworthy system of the CA is located in Finland in premises, the physical protection of which corresponds at least with the requirements for “highly important premises” defined in the regulation on the physical protection of telecommunication network (Viestintävirasto 48 B/2004 M) issued by Ficora (Finnish Communications Regulatory Authority).

5.1.2. Physical access

The certificate production premises are secured with round-the-clock guarding and supervision. Access to the premises where the CA system is located has been restricted to the persons in certain trusted roles of the CA. Access to the equipment where the CA signing keys are located and where they may be used requires the presence of two persons that have separately been authorized to enter the premises.

Access to other sites where parts of the CA system are located has been restricted to those persons who act in the roles mentioned in paragraph 5.2.1 “Trusted roles”. Access to the premises is supervised by using a physical access control system. If a person has not been granted permanent personal access rights to the premises, he may enter the premises and move around there only in the company of a person that has been granted those rights.

The RA offices shall be located in premises provided with access control. In RA offices of the CA and in offices of other RAs authorized by the CA, which are accessible to the public, the given directions on supervision of those offices shall be followed.

5.1.3. Power and air conditioning

The continuous operation of the CA system is secured by using an uninterruptible power supply and a reserve power generator. In the computer room there is an air conditioning system. The temperature and humidity of the air produced is continuously monitored.

5.1.4. Water exposures

Exposure to water damages is prevented with structural solutions. The computer room is controlled with humidity detectors. The computer room is located in premises situated above the lake surface level. The system of water and drain pipes in the premises has been limited to levels below the computer room.

5.1.5. Fire prevention and protection

The computer room is secured with an automatic fire alarm system. The premises have been equipped with smoke detectors and fire extinguishers.

5.1.6. Media storage

The media containing data generated by or related to the CA production system is stored in the same secure premises where the system itself is located. See also paragraph 5.1.8 “Off-site backup”.

5.1.7. Waste disposal

The disks of the CA system, magnetic tapes, and installation media with their back-up copies, which are not permanently stored in the CA production premises, will be securely destroyed when no more needed.

5.1.8. Off-site backup

Back-up copies are made of log information, and they are stored in a site located apart from the CA production site. Access to these premises has been restricted to the same separately authorized people who have access to the certificate production premises.

5.2. Procedural controls

5.2.1. Trusted roles

The personnel which participates in the certification operations has been divided into the following trusted roles, the responsibilities of which have been described in the Certificate Policies:

Security Manager
PKI Administrator
System Administrator
Registration Officer
Revocation Officer

The persons in trusted roles agree to be bound by this Certification Practice Statement.

5.2.2. Number of persons required per task

The CA shall ensure that it has employed a sufficient number of personnel per every task and that individual persons cannot serve simultaneously in all the roles.

The simultaneous participation of several persons is required for certain tasks. Critical measures directed towards the production of certificates and taken in the certificate production premises shall be carried out under at least dual control. The presence of at least three persons is required for generation and recovery of the CA private key and for making a back-up copy of the CA private key, according to the procedures defined by the CA.

5.2.3. Identification and authentication for each role

A certificate is required for verifying the identity of those serving in the following roles:

PKI Administrator
Registration Officer *
Revocation Officer

* At the registration of SoneraClass 2 certificates other strong authentication methods (eg. one-time SMS password) may also be used to verify the identity of the Registration Officer.

In the roles listed below a username and password are used for identity verification, as a rule. When the duties associated with the role require the use of the most critical systems of the CA, login to those systems requires identity verification based on a certificate or a one-time password also for the roles listed below.

Security Manager
System Administrator.

5.2.4. Internal documentation

In addition to the publicly available documents listed in paragraph 2.7.1 ”CA information and repositories”, the CA maintains and develops continuously internal documentation for the use of persons working in its organization. This documentation includes at least:

- Security Policy,
- technical descriptions of the system,
- description of the organization participating in certification operations,
- job descriptions related to the roles which belong to the CA’s organization,
- work instructions,
- process descriptions,
- Business Continuity Plan.

5.3. Personnel controls

5.3.1. Background information, qualifications, experience, and other requirements

In CA personnel employment Sonera’s normal employment procedures with the appropriate employee inspections are followed. The CA shall make sure that every person employed by the CA for tasks related to certification operations has the necessary qualifications and experience to perform his tasks. The subcontractors whose employees serve in important roles of the CA are obliged, based on agreements, to take care of this for their own employees.

Sonera has established and maintains comprehensive directions related to corporate security (policies, standards, procedures, instructions, and regulations), which every employee must familiarize himself with.

Every employee in the CA's own organization, that has been assigned tasks associated with certification operations, shall sign a personal non-disclosure agreement. Also every Certificate Manufacturer or other subcontractor of the CA, whose employees serve in the trusted roles of the CA, shall sign a non-disclosure agreement that obliges its employees.

5.3.2. Background check procedures

The background check procedures for all persons to be employed for duties of the CA shall follow the employment procedures defined by Sonera, with the appropriate employee inspections.

A background check is performed by a third party to the persons in the following roles:

Security Manager
PKI Operator
Registration Officer operating in the RA Office of the CA

Otherwise the CA uses its own discretion in having the backgrounds of its employees checked, based on the role of the employee in the CA's organization. The check is renewed when seen necessary, based on the consideration of the CA. The CA obliges, based on agreements, its subcontractors to take care of having checked the backgrounds of their employees serving in important roles.

5.3.3. Training requirements

New employees of the CA shall be familiarized with certification operations in general, with the associated security requirements, and especially with their own duties. The material to be covered includes, among others, the Security Policy, Certificate Policy, and Certification Practice Statement. If necessary, individual orientation and training adapted to a person's duties and role will be arranged.

If necessary, supplementary training is arranged for the employees of the CA.

Based on agreements, the subcontractors themselves are responsible for the training of their employees.

5.3.4. Sanctions for unauthorized actions

If the CA discovers a malpractice, the duties of the employee of the CA who has committed the malpractice will be changed immediately, and all his access rights to the systems related to certification operations will be cancelled. In regard to further measures, Sonera's existing practices are followed.

Procedures defined in agreements are followed in malpractice occurrences concerning subcontractors.

5.3.5. Documentation supplied to personnel

Every employee of the CA to be engaged to a task associated with certification operations will be given access to the documentation describing the certification operations and the CA functions. Furthermore, the employees will be given instructions and other material specifically necessary in the performing of their own tasks. On-line guidance is provided in electronic form by the systems and applications that employees are using.

The CA delivers to the subcontractors the necessary basic documentation, and the subcontractors are responsible for delivering the documentation further to their employees. Employees of certain subcontractors have access to directions maintained by the CA, through the applications they use.

Documentation is delivered by the CA personally to such employees of subcontractors that serve in certain roles. Furthermore, the subcontractors are obliged to deliver other necessary documentation to their employees.

6. Technical security controls

This chapter contains the policy for the management of public and private keys and the requirements for the associated technical security controls that apply to the CA, the Registration Authorities, the Certificate Manufacturers, and the Subjects.

The key pairs of the Subjects are generated on smart cards and on PKI SIM cards by a Certificate Manufacturer expressly approved by the CA for this task, the Card Manufacturer. On a USB token the key pair of the Subject can be generated by the Registration Authority of the CA's organization or by a Customer Organization that acts as a Registration Authority. The key pair related to a software certificate is generated by a Registration Officer that belongs to the CA's organization, a Registration Officer in a Customer Organization, or the Subject himself.

The key pairs of the Certificate Manufacturers, Registration Authorities, and Subjects are generated and delivered to the authorized users is such a way that no-one else but the user can have access to the private key.

6.1. CA key pair generation, installation, and protection

6.1.1. CA key pair generation

The CA key pair is generated according to the key generation procedures defined by the CA. The key pair is generated in the physically protected premises of the CA in a cryptographic module using the CA system (see paragraph 6.1.6 "CA private key protection"). The persons who participate in the key generation are individuals serving in trusted roles and authorized by the CA to do this task, and simultaneous control of at least two of those individuals is required. Additionally at least one supervisor authorized by the CA shall be present. The measures taken in the key generation procedure shall be recorded in minutes, and every person participating in the procedure shall confirm the minutes with his signature. The minutes are stored according to paragraph 4.7 "Records archival".

6.1.2. CA public key delivery to users

The public key of the CA is available on the internet at http://repository.trust.teliasonera.com, where the CA public key certificate signed by the CA itself, as well as the hash of the certificate, the so-called thumbprint, is published.

6.1.3. CA key sizes and algorithm

The CA is using a signing key the length of which is 4096 bits and which is based on the RSA algorithm to sign certificates and CRLs.

6.1.4. Usage period for CA key pair

The usage period of the CA private key shall not be longer than twentyfive (25) years. The usage period cannot be longer than the validity of the CA certificate related to the key. If the certificate of a Subject is revoked, the CRL shall be signed using the same key with which the certificate in question has been signed. It must be possible to use the CA private key, during the validity period of the related CA certificate, to revoke even the last Subject certificate signed by using the same CA private key, during the whole validity period of the Subject certificate. Therefore, the CA private key can be used for the signing of Subject certificates for the usage period of the key subtracted by the validity period of the Subject certificate. After this a new key pair has to be generated for the CA for the signing of certificates.

6.1.5. CA key usage purposes

The signing keys of the CA can be used only in the physically protected premises of the CA under the control of the persons serving in trusted roles of the CA by using the CA system and the cryptographic module defined in paragraph 6.1.6 “CA private key protection”.

The key usage purposes of the CA public key, which have been stated in the ”Key usage” field of the CA certificate, are as follows:

- keyCertSign (checking of the signature of the CA in Subject certificates),
- CRLSign (checking of the signature in the CRLs issued by the CA).

6.1.6. CA private key protection

The CA has built the protection of its private signing key on a combination of physical controls, defined procedures, access control, and user rights.

The CA system that is located in the physically protected premises of the CA contains a cryptographic module for protection of the signing key of the CA. The cryptographic module complies at least with the FIPS 140-2 level 3 standard.

With the help of technical controls and the defined procedures the CA ensures that no person alone can have means to access the environment where the private key is stored, nor can use the key in any way. Critical measures concerning the signing key, such as storing, copying, or recovering of the key always require more than one person to participate.

The recovery of the key requires the use of such activation data that has been stored in fragments in separate secure sites, and the means to get hold of the activation data have been divided among a number of persons, defined by the CA, which are serving in trusted roles. The recovery of the key provides that a certain number of those persons participate in the recovery procedure.

6.1.7. CA private key escrow

The private key of the CA is not copied and stored for key escrow purposes in any circumstances.

6.1.8. CA private key backup

To provide against destruction of the CA private key, there is an arrangement to recover the key. The back-up copying of the private key of the CA has been arranged in a way which guarantees in all circumstances at least the same protection level as is required of the maintenance of the private keys that are in use in the CA system (see paragraph 6.1.6, ”CA private key protection!).

6.1.9. CA private key archival

The private keys of the CA are not stored in archive.

6.1.10. Method of activating CA private key

The activation of the private key of the CA is included in the procedure described in paragraph 6.1.1 ”CA key pair generation”. At least one person serving in a trusted role of the CA and authenticated with a strong authentication method is required for the activation. The key remains active in the CA system until its use is interrupted for example because of maintenance operations.

6.1.11. Method of deactivating CA private key

At least one person serving in a trusted role of the CA is needed to deactivate the private key of the CA.

6.1.12. Method of destroying CA private key

When the use of the private key of the CA is terminated, all copies of it will be destroyed, or they will be retained in a way that prevents their further use.

6.1.13. CA public key archival

The CA stores the valid and the expired CA public keys according to paragraph 4.7 ”Records archival”.

6.2. Subordinate CA key pair generation, installation, and protection

6.2.1. Subject key pair generation

The same applies as for this CA, since they are generated in the same system.

6.2.2. Subject key sizes and algorithm

All subordinate CAs must have at least the RSA key length of 2048 bits or equivalent.

6.2.3. Usage periods for Subject keys

The usage periods for Subject keys have been given in the Certificate Policy.

6.2.4. Subject key usage purposes

Subordinate CA keys must only be used for certificate and CRL signing.

6.2.5. Subject private key protection

Same applies as for this CA.

6.2.6. Subject private key escrow

Same applies as for this CA.

6.2.7. Subject private key backup

Same applies as for this CA.

6.2.8. Subject private key archival

Same applies as for this CA.

6.2.9. Method of destroying Subject private key

Same applies as for this CA.

6.2.10. Subject public key archival

Same applies as for this CA.

6.3. Computer security controls

The requirements in the Security Policy of the CA shall be followed in the maintenance of the computer security.

6.3.1. Computer security rating

The multi-level computer security classification practices defined by Sonera are followed in the security classification of the systems of the CA.

6.3.2. User identification and access control

Access control is used to ensure the identity verification of users in different roles before access to the system (see paragraph 5.2.3, ”Identification and authentication for each role”). The system also ensures that the measures taken by different users are traceable.

6.3.3. Tasks that require multi-control

Certain tasks concerning the CA system require participation of several persons (see paragraph 5.2.2 ”Number of persons required per task”).

6.3.4. Capacity monitoring

The use of the resources of the system is under constant supervision, and an automatic monitoring system will generate an alarm when the preset limits are exceeded.

6.3.5. Security management controls

The requirements for the security management controls of the systems of the CA and the operations of the CA have been described in paragraph 4.6 ”Security audit procedures”.

6.3.6. Management of emergency

To be prepared for different states of emergency, reporting procedures and action plans have been defined. Measures to be taken when the business continuity of the CA is endangered have been described in the Business Continuity Plan drawn up by the CA.

6.3.7. Media storage security controls

The storage of records, the filing, and the handling of media that has become idle, have been described in paragraphs 5.1.6 ”Media storage” and 5.1.7 ”Waste disposal”.

6.4. Life cycle technical controls

6.4.1. System development controls

Two-phase testing is used in the development of the CA production system. The changes that have emerged as a result of development work will be first tested in a separate development system. After a successful testing the changes are taken into the test system that is identical with the production system. The final acceptance test is performed in the test system before the changes are taken into production.

All the changes in the system, which are to be taken into production, are properly documented.

6.4.2. Security management controls

6.4.2.1. Security management

The CA follows the policies defined by Sonera’s Corporate Security Unit in security management. Furthermore, the CA follows the Security Policy, Certificate Policy, and Certification Practice Statement defied by it in all of its operations. The auditing of the operation has been described in paragraph 2.8 ”Compliance audit”.

Evaluation of business risks and establishment of reaction and recovery models for potential risks belong to the management of the Business Continuity Plan drawn up by the CA. The reporting of abnormal events and of detected or suspected weaknesses in security is carried out according to the procedures defined by the CA.

The CA ensures by contractual arrangements that the level of security is preserved also when the outsourced functions are concerned, and that the defined policies and practices are followed also when subcontractors are involved.

6.4.2.2. Management of resources

The CA follows the principles of the Security Policy it has drawn up in the protection of the resources it uses, and to protect the data created and used by it.

6.4.2.3. Operations management

The operations management is based on the implementation of the Security Policy of the CA, on the compliance with the instructions drawn up by the CA, and on complying with the responsibilities defined in the agreements made with the subcontractors, and on the supervision of the operations required by the Security policy, instructions and responsibilities.

6.4.2.4. System access control

The principles of the Security Policy and the practices defined by the CA are followed in the management of user rights and access control of the systems of the CA. Persons separately authorized for the task manage user rights of different systems.

6.4.2.5. Cryptographic module life cycle management

The CA has prepared a guideline for the life cycle management of the cryptographic module used for signing certificates and CRLs in order to comply with the requirements defined in the Certificate Policies.

6.5. Network security controls

The CA system has been separated from the public network with firewalls. The most critical parts of the system are totally disconnected from the public network. An intrusion detection system is also used.

For the traffic between the parts of the system of the CA strong identification and encryption are used.

7. Certificate and CRL profiles

7.1. Certificate profile

The information contents of different certificate types issued by the CA have been described below. The data in a certificate has been arranged in successive fields. Some of the fields contain identical data in all certificates of the same certificate type. Some of the fields contain individual Subject-specific data.

The contents definition of a certificate, in other words the certificate profile, defines the fields in a certificate. The certificate profile of the certificates that belong to Sonera PKI follows the version 3 profile defined in the ITU X.509 standard. The profile of the certificates also follows the document RFC 3280 ”Internet X.509 Public Key Infrastructure Certificate and CRL Profile".

7.1.1. Certificate fields and their contents

7.1.1.1. Basic certificate fields

In the certificates only all the mandatory fields of the basic certificate fields defined in the X.509 standard are used. The optional fields would make it possible to reuse the CA name or the Subject name for another CA or Subject later. However, it is seen desirable that the names remain unambiguous.

The basic fields used in certificates have been listed below:

Version
Serial number
Signature algorithm
Issuer
Validity
Subject
Subject public key info

7.1.1.2. Certificate extensions

The following extensions defined in the X.509 standard are used in the certificates:

Authority key identifier
Authority Information Access
Subject key identifier
Certificate policies
CRL distribution points
Key usage
Extended key usage
Basic constraints
Subject alternative name

An extension has been marked critical if it is desired that the system exploiting the certificate will reject the certificate if it does not recognize the extension marked critical. Of the extensions given above, the following have been marked critical:

Key usage
Basic constraints

7.1.1.3. Certificate field contents

The table below contains those fields of certificates that are in use in all the certificate classes which belong to Sonera PKI, except for the CA certificates.

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 certificates that belong to Sonera PKI conform to the version 3.
Serial number	The CA generates an individual 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 that belong to TeliaSonera PKI is sha1RSA.
Issuer	This field states the name of the Issuer of the certificate. The same CA can issue certificates of different classes by using different Issuer names. The Issuer name in the certificates of each certificate class has been described in paragraph 3.1 “Naming practices for CA certificates” of each Certificate Policy.
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 briefly described in paragraph 3.2 “Initial registration” of this CPS, and in more detail in paragraph 3.2 “Initial registration” of the appropriate Certificate Policy.

Subject public key info	This field gives the algorithm under which the public key of the Subject shall be used. In the certificates that belong to Sonera PKI the algorithm to be used is RSA. The Subject's public key itself is also given in this field. Within Sonera PKI, the length of the public key in the certificate of a Subject (not of the CA) is 1024 bits (with the exception mentioned in paragraph 6.2.4 "Subject key sizes and algorithm").
Authority key identifier	The identifier of the CA public key 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 certificate. Within Sonera PKI the SHA-1 hash algorithm is used to calculate the identifier.
Authority Information Access	The url to the CA certificate of a the certificate is given in this field.
Subject key Identifier	The identifier of the Subject public key that is contained in the certificate is given in this field. The identifier can be used to pick up those certificates that contain a given public key. Within Sonera PKI the SHA-1 hash algorithm is used to calculate the identifier.
Certificate policies	This field states the policies according to which the certificate has been issued. A Certificate Policy is identified based on an individual identifier (object identifier, OID) assigned to it. The identifier has been given in paragraph 1.2 "Identification of the document" of each Certificate Policy.
CRL distribution points	This field gives the location where the CRL is available. In the certificates that belong to Sonera PKI there is a CRL address of the type URI in this field. The exact addresses of the CRLs corresponding the different certificate classes are given in paragraph 4.4.6 "CRL checking requirements".

CA certificate

The table below includes those certificate fields that are used in the CA certificates within Sonera PKI.

Field name	Field description and contents
Version	The description can be found in the tables above.
Serial number	The description can be found in the tables above.
Signature algorithm	The description can be found in the tables above.
Issuer	The description can be found in the tables above.

Validity	The description can be found in the tables above.
Subject	This field identifies the CA in whose possession the private key is. The field contents have been described in paragraph 3.1 "Naming practices for CA certificates" of each Certificate Policy.
Subject public key info	The description can be found in the tables above. Within TeliaSonera PKI the length of the public key in CA certificates is 4096 bits.
Subject key identifier	The description can be found in the tables above.
Key usage	Within TeliaSonera PKI the key usage purposes of the public key of the CA are: KeyCertSign, CRLSign
Basic constraints	This field expresses that the certificate is a CA certificate, i.e. the Subject is the CA.

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.

The CRLs conform to the version 2 defined in the X.509 standard. They also conform to the document RFC 3280.

7.2.1. Basic CRL fields

All basic CRL fields defined in the X.509 standard are used, both mandatory and optional.

The CRL basic fields have been listed below:

Version
Signature algorithm
Issuer
This update
Next update
Revoked certificates

7.2.2. CRL extensions

The following CRL extensions defined in the X.509 standard are used:

Reason code
- a CRL entry extension

Authority key identifier
CRL number

A CRL extension is marked critical if it is desired that the system checking the validity of a certificate from the CRL will regard the checking as failed if it does not know how to interpret the extension. None of the above-mentioned CRL extensions have been defined critical within Sonera PKI.

Private CRL extensions are not used.

7.2.3. CRL field contents

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 that belong to Sonera PKI conform to the version 2.
Signature algorithm	The CRLs are signed by using the same algorithm as is used for signing of the certificates. The algorithm used is sha1RSA.
Issuer	This field states the name of the Issuer of the CRL. Within Sonera PKI the 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. Within Sonera PKI the time difference between "This update" and "Next update" is 48 hours.
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. The reason for revocation can be one of the following: KeyCompromise, CACompromise*, AffiliationChanged, Superseded, CessationOfOperation, CertificateHold * only for a revoked CA certificate
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 Sonera 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.

8. CPS administration

Whenever a paragraph in a Certificate Policy is changed, the effects of the changes on the Certification Practice Statement are estimated. The same action will be taken when a new object identifier (OID) is assigned to a changed Certificate Policy. Sonera CA Policy Authority is responsible for the commencement of the estimation. There can be other reasons to change the document as well, with no relation to changes in a Certificate Policy.

8.1. Change procedures

8.1.1. Items that can change without notification

Typographical or editorial corrections, or changes to contact information, may be made to this document without notification to the users of the document. Translations of the document into different languages may also be published without a separate notification.

8.1.2. Changes with notification

The following changes require a notification:

- Changes affecting the terms of the agreement between the parties shall be notified according to the aforesaid terms.
- Any paragraph in the CPS may be changed with 15 days prior notice.

All the proposed changes requiring notification shall be published at: http://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.

8.2. Publication policies

A copy of this Certification Practice Statement is available in electronic form on the internet at: http://repository.trust.teliaonera.com.

8.3. CPS approval procedures

The Certification Practice Statement and all the changes to it shall be published upon acceptance by Sonera CA Policy Authority.

9. References

[ISO/IEC 9594-8; ITU-T X.509] Information Technology – Open Systems Interconnection – The Directory: Authentication Framework. Also published as ITU-T Rec. X.509: Public key and attribute certificates frameworks

[RFC 2527] IETF document: Internet X.509 Public Key Infrastructure – Certificate Policy and Certification Practices Framework

[EU Directive] Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures

[PKIX Roadmap] IETF document: Internet X.509 Public Key Infrastructure: Roadmap

[ETSI TS 101 456 v1.2.1] ETSI Technical Standard: Policy Requirements for certification authorities issuing qualified certificates

[RFC 3280] IETF document: Internet X.509 Public Key Infrastructure – Certificate and Certificate Revocation List (CRL) Profile