

Sonera CA

Certificate Policy

Sonera Class 1 Certificate

Valid as from January 22, 2004
Version 2.1

Object Identifier (OID) of the Certificate Policy:
1.3.6.1.4.1.271.2.3.1.1.1

High-level assurance certificates
– Private key stored in a smart card or USB token

This English version of "Sonera CA Certificate Policy, Sonera Class 1 Certificate" is an unofficial translation of the original Finnish document "Sonera CA Varmennepolitiikka, Sonera Class 1 -varmenne" which is the authentic version.

TeliaSonera Finland Oyj
 Enterprise Services

Version history of the Certificate Policy TeliaSonera Finland CP-Class1

Version number	Document name	Version Date	Description
V 1.0	Sonera CA, CP - Certificate Policy for Sonera Class 1 Certificates	1.3.2001	The first Sonera CA Certificate Policy for Class 1 Certificates
V 1.1	See above	1.3.2002	Changes to details
V. 2.0	Sonera CA, Varmennepolitiikka, Sonera Class 1 –varmenne, (in Finnish only)	22.9.2003	Change of structure
V. 2.1	Sonera CA Certificate Policy, Sonera Class 1 Certificate	22.1.2004	Changes to details

All published versions are available at:
<http://support.partnergate.sonera.com/>.

Contents

Terminology6

1 Introduction 8

1.1 Overview..... 8

1.2 Identification of the document 8

1.3 Community and applicability..... 8

 1.3.1 Certification Authority (CA) 9

 1.3.2 Certificate Manufacturer (CM)..... 9

 1.3.3 Registration Authority (RA) 9

 1.3.4 Subject..... 9

 1.3.5 Subscriber 9

 1.3.6 Relying Party 10

 1.3.7 Contractual relationships 10

 1.3.8 Applicability 10

1.4 Contact details 10

2 General provisions..... 12

2.1 Obligations 12

 2.1.1 CA obligations 12

 2.1.2 Registration Authority obligations 13

 2.1.3 Subscriber obligations 13

 2.1.4 Relying Party obligations 13

TeliaSonera Finland Oyj
Enterprise Services

2.2	Liability	13
2.3	Financial responsibility.....	14
2.3.1	Indemnification by Customer Organizations	14
2.4	Customer feedback	14
2.5	Interpretation and enforcement of Certificate Policy.....	14
2.6	Fees.....	14
2.7	Publication and repository	15
2.7.1	CA information and repositories	15
2.7.2	Frequency of publication.....	15
2.7.3	Access control.....	15
2.8	Compliance audit.....	16
2.8.1	Auditing carried out by the CA.....	16
2.8.2	Auditing carried out by external auditor	16
2.9	Confidentiality.....	16
2.10	Intellectual property rights	16
2.10.1	CA information intellectual property rights	16
2.10.2	License to use software and documents	16
3	Identification and authentication.....	18
3.1	Naming practices for CA certificates.....	18
3.2	Initial registration.....	18
3.2.1	Naming of Subjects	18
3.2.2	Meanings and interpretation of names	19
3.2.3	Uniqueness of names.....	19
3.2.4	Name claim dispute resolution procedure	19
3.2.5	Authentication of organization identity	19
3.2.6	Verifying of Subject identity and name	19
3.2.7	Method to prove possession of private key	19
3.3	Certificate renewal, rekey, and information update	20
3.4	Rekey after certificate revocation.....	20
3.5	Revocation request.....	20
3.6	Reinstatement of suspended certificate	20
4	Operational requirements	21
4.1	Certificate application.....	21
4.2	Certificate issuance	21
4.3	Certificate acceptance	21
4.4	Certificate revocation and suspension.....	22
4.4.1	Circumstances for revocation	22
4.4.2	Who can request revocation.....	22
4.4.3	Procedure for revocation request.....	22
4.4.4	Certificate suspension	22
4.4.5	CRL issuance.....	23

TeliaSonera Finland Oyj
 Enterprise Services

4.4.6	CRL checking requirements	23
4.5	Certificate reinstatement.....	23
4.6	Security audit procedures.....	23
4.7	Records archival.....	23
4.8	CA key changeover.....	24
4.9	Compromise and disaster recovery	24
4.9.1	Disaster recovery.....	24
4.9.2	Computing resources, software, and/or data are corrupted.....	24
4.9.3	CA private key compromise	24
4.9.4	Secure facility after a natural or other type of disaster	24
4.10	CA termination.....	25
5	<i>Physical, procedural and personnel security controls.....</i>	26
5.1	Physical and environmental controls.....	26
5.2	Procedural controls.....	26
5.2.1	Trusted roles	26
5.2.2	Number of persons required per task.....	27
5.2.3	Identification and authentication for each role.....	27
5.2.4	Internal documentation.....	27
5.3	Personnel controls	27
5.3.1	Background information, qualifications, experience, and other requirements	27
5.3.2	Background check procedures.....	27
5.3.3	Training requirements	28
5.3.4	Sanctions for unauthorized actions	28
5.3.5	Documentation supplied to personnel.....	28
6	<i>Technical security controls</i>	29
6.1	CA key pair generation, installation, and protection.....	29
6.1.1	CA key pair generation	29
6.1.2	CA public key delivery to users.....	29
6.1.3	CA key sizes and algorithm	29
6.1.4	Usage period for CA key pair	29
6.1.5	CA key usage purposes.....	29
6.1.6	CA private key protection	29
6.1.7	CA private key escrow.....	30
6.1.8	CA private key backup.....	30
6.1.9	CA private key archival.....	30
6.1.10	Method of activating CA private key.....	30
6.1.11	Method of deactivating CA private key.....	30
6.1.12	Method of destroying CA private key.....	30
6.1.13	CA public key archival.....	30
6.2	Subject key pair generation, installation, and protection.....	31
6.2.1	Subject key pair generation	31
6.2.2	Subject private key delivery to Subject.....	31
6.2.3	Subject public key delivery to CA.....	31
6.2.4	Subject key sizes and algorithm.....	31

TeliaSonera Finland Oyj
Enterprise Services

6.2.5	Usage periods for Subject keys	31
6.2.6	Subject key usage purposes.....	31
6.2.7	Subject private key protection.....	31
6.2.8	Subject private key escrow.....	32
6.2.9	Subject private key backup.....	32
6.2.10	Subject private key archival.....	32
6.2.11	Method of activating Subject private key.....	32
6.2.12	Method of deactivating Subject private key.....	32
6.2.13	Method of destroying Subject private key.....	32
6.2.14	Subject public key archival.....	32
6.3	Subject activation data.....	32
6.3.1	Activation data generation and installation	32
6.3.2	Activation data protection	33
6.4	Computer security controls.....	33
6.5	Life cycle technical controls	33
6.5.1	System development controls	33
6.5.2	Security management controls	33
6.6	Network security controls	35
7	<i>Sonera Class 1 Certificate and CRL profiles.....</i>	36
7.1	Certificate profile	36
7.1.1	Certificate fields and their contents	36
7.2	CRL profile	36
8	<i>CP administration.....</i>	38
8.1	Change procedures	38
8.1.1	Items that can change without notification	38
8.1.2	Changes with notification.....	38
8.1.3	Changes that require new CP	38
8.2	Publication policies	38
8.3	CPS approval procedures.....	38
9	<i>Certification Practice Statement (CPS).....</i>	39
	<i>References.....</i>	40

TeliaSonera Finland Oyj
Enterprise Services

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.

TeliaSonera Finland Oyj
Enterprise Services

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://support.partnergate.sonera.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 smart card or USB-token, which contains the Subject's private key.*

Sonera: *In this document the term refers to TeliaSonera Finland Oyj.*

Sonera Class 1 Certificate: *Certificate which is issued to a natural person. The Certificate and the related private key have been stored in a cryptographic device.*

Sonera PKI: *The infrastructure composed of software, hardware, practices, procedures, and policies, managed by Sonera CA to provide security services that leverage public key cryptosystems and certification methodology.*

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]*

TeliaSonera Finland Oyj
Enterprise Services

1 Introduction

1.1 Overview

This document is a Certificate Policy (CP) for certificates issued to natural persons (Subjects) within Sonera PKI (PKI = Public Key Infrastructure). This document is administered by Sonera CA Policy Authority. The document defines the policy for Sonera Class 1 Certificates. The certificates can be used for authentication, non-repudiation, integrity, and confidentiality.

The following requirements apply to Sonera Class 1 Certificates:

- The private key related to the Sonera Class 1 Certificate has been stored in a smart card or USB token that is used as a Signature-Creation Device.
- The certificate has been signed by Sonera Class1 CA.
- The certificate has been signed with a CA key, the length of which is at least 2048 bits.
- The validity period of the certificate is five (5) years at the most.

The structure of this CP is based on the document RFC 2527 "Certificate Policy and Certification Practices Framework".

The CA can outsource some of its functions to subcontractors, e.g. Certificate Manufacturers, Registration Authorities, Revocation Service providers. However, the CA shall bear overall responsibility and liability of the certificates issued by it.

This CP is intended to be used by Relying Parties in order to help in deciding whether a certificate is sufficiently trustworthy.

This CP is referenced in each Sonera Class 1 Certificate, using an Object Identifier (OID). By inspecting the OID field in a certificate, an application utilizing the certificate may be able to check automatically that the certificate is suitable for use for a particular purpose.

Users of this document may consult the Certification Practice Statement (CPS) to obtain further details of precisely how this CP is implemented.

1.2 Identification of the document

The name of this Certificate Policy is "**Sonera CA Certificate Policy, Sonera Class 1 Certificate**", and it is identified as "**TeliaSonera Finland CP-Class1 v. 2.1**". This Certificate Policy has been registered by Sonera CA Policy Authority, and the following unique Object Identifier (OID) has been allocated to it:
1.3.6.1.4.1.271.2.3.1.1.1

```
{iso(1) org(3) dod(6) internet(1) private(4) enterprise(1) telecomFinland(271) services(2)
serviceProducts(3) soneraCA(1) certificatePolicies(1) soneraClass1CAPolicy(1)}
```

1.3 Community and applicability

This Certificate Policy is binding on TeliaSonera Finland Oyj (later "the CA") that issues certificates referencing this Policy. The document also describes the rights and obligations of other participants in Sonera PKI: Certificate Manufacturers, Registration Authorities, Subscribers, Subjects and Relying Parties.

TeliaSonera Finland Oyj
Enterprise Services

The CA implements the Policy in accordance with the laws of Finland.

1.3.1 Certification Authority (CA)

The party trusted by users of certification services (i.e. Subscribers, Subjects as well as Relying Parties) to create and issue certificates is called the Certification Authority (CA). The CA has overall responsibility for the provision of the certification services. The services provided comprise the issuing and publishing of certificates as well as the Revocation Service and Revocation Status Service. The CA private key is used to sign certificates and Certificate Revocation Lists (CRLs), and the key holder's name (the CA name) is identified in the "Issuer" field of a published certificate or CRL. The CA complying with this Policy is TeliaSonera Finland Oyj, and the CA name in the "Issuer" field is "Sonera Class1 CA". No other CA has been granted the authority to issue certificates according to this Policy.

The CA may use other parties for the production of certification services. The CA shall, however, bear overall responsibility for complying with the requirements in the Policy.

1.3.2 Certificate Manufacturer (CM)

The CA has overall responsibility of certificate manufacturing and management. The CA may, however, outsource parts of its functions to Certificate Manufacturers.

1.3.3 Registration Authority (RA)

Only organizations approved by the CA can act as Registration Authorities.

The CA is, however, ultimately responsible for the certificates issued by it. An RA must therefore be bound to the obligations concerning registration, identification and authentication functions defined in this Policy, through a suitable contract with the CA.

NOTE An exception to the rule above may exist when a Relying Party chooses to accept the responsibility of performing the functions of the RA. In that case, the Relying Party is free to assume some part of the CA's responsibility by entering into a contractual arrangement.

1.3.4 Subject

The CA issues certificates to persons named by Customer Organizations. This Policy is referenced in these certificates. Only natural persons can hold these certificates, and in this Policy those persons are called Subjects.

Certificates may be issued to a person named by a Customer Organization, based on the contractual relationship between the person and the organization. The CA has the right to decline a certificate application at its own discretion.

1.3.5 Subscriber

The Subscriber is a customer of the CA, based on whose order the CA issues certificates. The Subscriber shall be bound to the obligations stated in this Policy on his own behalf or on behalf of one or more Subjects.

TeliaSonera Finland Oyj
Enterprise Services

1.3.6 Relying Party

This Certificate Policy is intended for the benefit of individuals and organizations (Relying Parties), which exploit certificates issued according to this Policy. By relying on such certificates, Relying Parties are bound to the obligations stated in this document.

1.3.7 Contractual relationships

The CA shall have contractual agreements with the Subscribers and with all parties that carry out elements of the CA operations. The CA shall be responsible for the operation of its subcontractors as of its own as far as certification operations are concerned. Those contracts shall clearly indicate the rights and obligations of the parties to the contract.

1.3.8 Applicability

Certificates may be used to support digital signatures.

Certificates may be used only for the following applications:

- Subject authentication,
- verification of digital data origin and integrity,
- confidentiality of digital data,
- non-repudiation with electronic signatures.

Applications using certificates issued under this Policy shall take into account the key usage purpose stated in the "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.

1.4 Contact details

This Certificate Policy has been registered by TeliaSonera Finland Oyj / Networking Solutions, and it is administrated by Sonera CA Policy Authority.

TELIASONERA FINLAND OYJ

NETWORKING SOLUTIONS

Security and Management Services

Kuortaneenkatu 1

P. O. Box 543

00051 SONERA

Phone: +358 (0) 20401

Contact person in matters related to this CP:

Sonera CA Product Manager

Email: cainfo@sonera.com

Phone: +358 (0) 20401



TeliaSonera Finland Oyj
Enterprise Services

Customer Service: 0800 188188 (Mon-Fri 8-17)

Technical Customer Service (24 h): 0800 180191

Revocation Service: 0800 156677

Internet: <http://support.partnergate.sonera.com/>

TeliaSonera Finland Oyj
Enterprise Services

2 General provisions

2.1 Obligations

2.1.1 CA obligations

The CA shall ensure that all requirements on the CA, as detailed in this document, are implemented.

The CA has the responsibility for conformance with the procedures prescribed in this Policy, even when some of the CA functions have been outsourced to subcontractors.

The CA shall provide all its certification services consistent with its Certification Practice Statement.

The CA is responsible for the terms of this Policy and its administration.

2.1.1.1 Legal requirements

The CA shall ensure compliance with legal requirements. In particular:

- All important data and records shall be protected from loss, destruction and falsification. Some records may need to be recovered later, to meet statutory requirements, as well as to support essential business activities.
- The requirements of the European data protection Directive shall be met as implemented through national legislation.
- Appropriate technical and organizational measures shall be taken by the CA against unauthorized or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
- The information that users contribute to the CA shall be completely protected from disclosure without the user's agreement, a court order or other legal authorization.

2.1.1.2 Organizational requirements

The CA shall ensure that its organization is reliable. In particular that:

- The CA is a legal entity according to national law.
- The CA has a system or systems for information security management appropriate for the certification services it is providing.
- The CA has adequate arrangements to cover liabilities arising from its operations and/or activities.
- The CA has the financial stability and resources required to operate in conformity with this Policy.
- The CA employs a sufficient number of personnel having the necessary education, training, technical knowledge and experience relating to the type, range and volume of work necessary to provide certification services.
- The CA has a properly documented agreement and contractual relationship in place where the provisioning of services involves subcontracting, outsourcing or other third party arrangements.
- The parts of the CA concerned with certificate generation and revocation management shall have a documented structure.

2.1.1.3 Notifications of certificate issuance and revocation

The CA will not separately notify the Subscriber, Subject, or other parties of a certificate issuance.

TeliaSonera Finland Oyj
Enterprise Services

When the information related to a revocation request is checked at the Revocation Service by phone, the person requesting revocation will be notified of successful transmission of the request to the CA system during the call.

2.1.2 Registration Authority obligations

The Registration Authority takes care of the identification and authentication of the Subject according to the CPS, on behalf of the CA. The obligations include:

- verify the identity of the Subject,
- ensure that the Subject is authorized to apply for the certificate,
- submit an appropriate and complete certificate request to the CA at initial registration, certificate renewal, and rekey.

Additionally, Registration Officers operating in Customer Organizations are obliged to, concerning Subjects in their own organizations:

- deliver revocation requests to the Revocation Service in circumstances requiring that.

2.1.3 Subscriber obligations

The CA shall oblige, through agreement, the Subscriber to ensure that the Subject fulfils the following obligations:

- submit accurate and complete information to the CA in accordance with the requirements of this Policy, particularly with regard to registration,
- only use the Subject private key for such purposes as correspond to the applications of certificates, as defined in paragraph 1.3.8 "Applicability", to the key usage purposes specified in the "Key usage" extension field of the certificate, and in accordance with any other limitations notified to the Subscriber,
- exercise reasonable care to avoid unauthorized use of the Subject private key,
- notify the CA without any reasonable delay, if any of the following occur up to the end of the validity period indicated in the certificate:
 - the Subject has a reason to believe that his private key has been lost, stolen, potentially compromised, or
 - control over the Subject private key has been lost due compromise of activation data (e.g. PIN code) or other reasons, and/or
 - inaccuracy or changes to the certificate content, as notified to the Subject,
- following compromise, the use of the Subject private key is immediately and permanently discontinued.

The CA will give the Subscriber access to separate directions on the responsibilities of a customer of certification services, and on how to comply with the aforementioned responsibilities.

2.1.4 Relying Party obligations

To be able to reasonably rely on a certificate, the Relying Party shall take at least the following measures:

- verify the authenticity and validity of the certificate either himself, or acquire the verification as a service, and
- take account of any limitations on the usage of the certificate indicated to the Relying Party either in the certificate, in this CP, or in the agreement.

TeliaSonera Finland Oyj
Enterprise Services

2.2 Liability

The CA has limited its liabilities for damages in the Certification Practice Statement. Limitations may also be included in agreements with Customer Organizations. Furthermore, what is stated about liability for damages in Sonera's general delivery terms for business customers concerning services, shall apply.

2.3 Financial responsibility

The CA shall bear the financial responsibility for the certification operations according to the CP, the CPS, and the terms and conditions, including production, management and development of services, both for its own part and on behalf of its subcontractors.

The CA shall not be responsible for the financial commitments arising when a certificate is used.

The CA shall not be responsible for the functioning or contents of applications where certification services are exploited. The Customer Organisation shall itself bear the financial risks associated with its applications and their use.

2.3.1 Indemnification by Customer Organizations

If a claim for damages will be presented against the CA based on the matters listed below, the Customer Organization shall be bound to compensate the CA for any damages and costs due to the claim and the necessary statement of defense, including any legal expenses. Therefore, the Customer Organization shall indemnify the CA for:

- the Subject's failure to protect his private key or prevent it from being lost, disclosed or compromised,
- the failure to submit a certificate revocation request to the Revocation Service under the conditions that require notification to the CA, as stated in paragraph 2.1.3 "Subscriber obligations",
- the Customer Organization's failure as a Relying Party to verify the validity of the certificate according to paragraph 2.1.4 "Relying Party obligations",
- the Customer Organization's otherwise non-justified trust on the certificate as Relying Party, in consideration of the circumstances.

The CA shall notify the Customer Organization of any such claim in writing within a reasonable time after being informed of a claim.

2.4 Customer feedback

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

2.5 Interpretation and enforcement of Certificate Policy

The interpretation, enforceability, and validity of this Policy shall be governed by the laws of Finland. Dispute resolution procedures have been described in the CPS.

TeliaSonera Finland Oyj
Enterprise Services

2.6 Fees

The fees stated in the agreement between the CA and the Customer Organization will be charged for certification services. The fees may be based on, e.g.:

- certificate issuance,
- certificate management,
- certificate renewal,
- certificate use,
- revocation or status information access,
- establishment of a service exploiting certificates.

The terms concerning refund policy have been stated in the CPS.

2.7 Publication and repository

2.7.1 CA information and repositories

2.7.1.1 Terms and conditions

The terms and conditions regarding use of certificates have been made available in this Policy and in the CPS. The terms and conditions defined include among other things the following:

- limitations on the use of certificates,
- Subscriber obligations, as defined in this Policy,
- information on how the validity of a certificate can be verified, including requirements to check the revocation status of the certificate, such that the Relying Party may reasonably rely on the certificate,
- retention period for registration information,
- retention period for log information of the systems of the CA,
- reclamation and dispute resolution procedures,
- governing law.

The information listed above shall be permanently available in the repository. The information may be delivered in electronic form.

2.7.1.2 Certificate dissemination

The CA shall ensure that certificates are made available as necessary to Relying Parties. In particular:

- A certificate is made available in the directory of the CA, unless otherwise agreed on with the Subscriber.
- Certificates shall be published promptly.

2.7.1.3 Revocation status information dissemination

Revocation status information has been made available through the Revocation Status Service.

2.7.2 Frequency of publication

All information to be published in the repository shall be published promptly after such information is available to the CA. The frequency of publication of CRLs is given in the CPS.

TeliaSonera Finland Oyj
Enterprise Services

2.7.3 Access control

The repository for this Policy and the associated CPS, as well as for the terms and conditions of the certification services, is freely and publicly accessible. Subjects certificates are available to Relying Parties as necessary. The Revocation Status Service is publicly accessible.

2.8 Compliance audit

2.8.1 Auditing carried out by the CA

The CA supervises the security of its operations by internal inspections. The CA has the right to audit also the operations of Registration Authorities in Customer Organizations. The CA's subcontractors follow their own inspection procedures in the audit of their own operations.

2.8.2 Auditing carried out by external auditor

The CA has its operations regularly audited by a third party. An external audit is carried out at least once a year. The audit covers the operations of the CA and its subcontractors, but the operations of RAs in Customer Organizations are not included.

The audit is performed by an information security auditor approved by Sonera CA Policy Authority. The purpose of such an audit is to ensure at least the following:

- The CA and its subcontractors have a system in place to assure the quality of the services provided.
- The CA and its subcontractors are operating in compliance with all requirements in this Policy.
- The Certification Practice Statement of the CA is consistent with the requirements of this Policy.

If defects will be found during audit, the CA shall take appropriate measures to correct them.

2.9 Confidentiality

Information regarding Subscribers and Subjects that is received at registration by the CA and RA will be kept confidential and shall not be disclosed to third parties without the prior consent of the person in question, unless otherwise required by law. A certificate itself is public, thus Subject information appearing in it is also public.

2.10 Intellectual property rights

2.10.1 CA information intellectual property rights

The title and intellectual property rights of the following information belong to the CA:

- trademarks and names used by the CA in connection with certification services,
- this Certificate Policy and the related Certification Practice Statement,
- other documentation related to certification services and established by the CA,
- certificates and CRLs generated by the CA,
- key pairs generated by the CA, and used by the CA or delivered to Subjects by the CA.

TeliaSonera Finland Oyj
Enterprise Services

2.10.2 License to use software and documents

The title and the intellectual property rights of all the software, documents and other material that is part of the entity necessary for producing certification services belong to the CA or a third party. The CA shall grant a Subscriber or Relying party a license for restricted right to use, according to this Policy, the object code versions of software and documents delivered by the CA and the material and information provided for testing the service. The license gives the Subscriber or Relying party the right to use the software and documents and the test material and information only according to the instructions given by the CA and only for purposes directly connected with the use of the service or its testing. The title and all intellectual property rights to the software, documents, the test material and information, and any revised versions thereof, shall belong to the CA or a third party (such as the CA's principal or subcontractor). The Subscriber or Relying party is not entitled, without the prior written consent of the CA, to copy, translate, or modify the material, documents or software, or to place them at a third party's disposal unless otherwise provided by mandatory legislative provisions.

Upon the expiration of the license the Subscriber or the Relying party shall, at his own expense, either return or, at the CA's request, destroy the originals and copies and the data media and documentation that are in his possession.

TeliaSonera Finland Oyj
Enterprise Services

3 Identification and authentication

3.1 Naming practices for CA certificates

The CA issuing certificates according to this Policy is given a unique X.501 Distinguished Name (DN), which is stated both in the "Issuer" field and "Subject" field of the CA certificate, and also in the "Issuer" field of all the other certificates issued by the CA. The name is comprised of the following attributes:

Attribute	Value
commonName (CN)	Sonera Class1 CA
Organization (O)	Sonera
Country (C)	FI

3.2 Initial registration

3.2.1 Naming of Subjects

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)	Name of the Subject
Organization (O)	Customer Organization in relation to which the Subject is identified
Country (C)	Country where the Customer Organization is running its main operations

Additionally, the "Subject" field may include following attributes depending on the usage purpose of the certificate.

Attribute	Description of value
givenName (GN)	First name(s) of the Subject
Surname (S)	Family name of the Subject
serialNumber (SN)	Character string for differentiation between names that would otherwise be identical

TeliaSonera Finland Oyj
Enterprise Services

Additional attributes may be used as necessary.

3.2.2 Meanings and interpretation of names

The "commonName" attribute can include the real name or a pseudonym of the Subject.

When the attribute contains the real name of the Subject, the name shall be composed of the first and last name of the person, and it can additionally contain other given names or initials of the person.

When the attribute contains a pseudonym, that shall be one single word comprising of a sequence of characters without any spaces.

Note: The name of the Subscriber's organization is included in the certificate only for informative purposes, thus its presence in the certificate does not grant any authorities or other rights.

3.2.3 Uniqueness of names

The Subject name stated in a certificate shall 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 shall 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.

3.2.4 Name claim dispute resolution procedure

The CA provides that the Customer Organizations do not violate the title to names of others when applying for certificates. The CA does not, however, check the right of the Customer Organization to use the names it gives in its certificate applications, nor does the CA participate in any name claim dispute resolution procedures concerning brand names, domain names, trademarks, or service names. The CA 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.

3.2.5 Authentication of organization identity

The CA verifies the identity of the Customer Organization and the authorities granted in the organization, when the organization becomes a Subscriber and when the rights needed by the Registration Officers operating in the Customer Organizations are granted to these persons. The identity of a Registration Officer is always verified, when he applies for a certificate. The methods for authentication and verification are described in the CPS in more detail.

3.2.6 Verifying of Subject identity and name

The Subject identity and name are verified at registration by the Registration Officer in the Customer Organization according to the procedures defined in the CPS.

TeliaSonera Finland Oyj
Enterprise Services

3.2.7 Method to prove possession of private key

If the CA does not generate the Subject key pair but it is generated in the Customer Organization, then the certificate request is accepted only when signed with the private key of the same key pair.

3.3 Certificate renewal, rekey, and information update

The CA shall ensure that the requests for measures concerning certificates are appropriate and permitted. This concerns certificate renewal, generation of a new key pair before the certificate is expired, and updates to the information in a Subject certificate. The Customer Organizations acting as Registration Authorities are for their part bound to perform the checks and verifications concerning registration, by contract and related directions. In particular:

- The validity of the information used to verify the identity and attributes of the Subject shall be checked. If there are changes to this information, they shall be verified in the same way as at initial registration.
- If any of the terms and conditions set by the CA has changed, they shall be communicated to the Subscriber.
- The CA shall issue a new certificate for the Subject's previously certified public key, only if its cryptographic security is still considered sufficient for the new certificate's intended lifetime and no indications exist that the Subject's private key has been compromised.

3.4 Rekey after certificate revocation

Revoked and expired certificates cannot be renewed. If the Subject does not have a valid Sonera Class 1 certificate, then the same registration procedure will be followed as at initial registration.

3.5 Revocation request

Only a Revocation Officer of the CA has the right to submit a certificate revocation request to the CA system. The identity of the Revocation Officer is verified based on a certificate.

The identity of the person requesting revocation shall be verified at the Revocation Service. The verification shall be made such that the right of the person to request revocation can be verified on a sufficient level. These authentication mechanisms must balance the need to prevent unauthorized revocation requests against the need to quickly revoke certificates. The verification methods have been described in the CPS.

3.6 Reinstatement of suspended certificate

If a certificate has been suspended, it can be reinstated on the Customer Organization's request. The identity of the person requesting reinstatement shall be verified. The verification shall be made such that the right of the person to request reinstatement can be verified. The verification methods have been described in the CPS.

The persons authorized to verify reinstatement requests are separately appointed by the CA. Only upon approval from such an authorized person a Revocation Officer of the CA has the right to reinstate a certificate. The identity of the Revocation Officer is verified based on a certificate.

TeliaSonera Finland Oyj
Enterprise Services

4 Operational requirements

4.1 Certificate application

Certificate applications and certificate requests shall be filled and submitted according to the given instructions, and they shall be complete and accurate. Certificate applicants shall be properly authenticated. In particular:

- Before entering into a contractual relationship with a Subscriber, the CA shall deliver the Subscriber the terms and conditions regarding use of the certificate.
- The terms and conditions shall be permanently available. They may be delivered in electronic form.
- The Subscriber shall give his address and other contact information in order to get hold of him.
- The identity of the Subject shall be verified according to the procedure described in the CPS in paragraph 3.2 "Initial registration".
- The requirements of the national legislation on privacy protection shall be followed.

The CPS includes a more detailed description of the certificate application procedure.

4.2 Certificate issuance

The CA system generates a certificate based on an electronically signed certificate request it has received, and the certificate will be signed by the CA. The CA is responsible for the authenticity of certificates issued.

The validity period of Sonera Class 1 certificates issued by the CA is at most **five (5) years**. The contents of a certificate have been depicted in paragraph 7.1 "Certificate profile". A detailed description can be found in the CPS.

In particular:

- The procedure of issuing the certificate is securely linked to the associated registration, certificate renewal, or rekey processes.
- When generating the Subject key pair the CA shall ensure the following:
 - The procedure of issuing the certificate is securely linked to the generation of the key pair.
 - The private key (or Signature-Creation Device) is securely passed to the Subscriber or registered Subject.
- The CA shall ensure over time the uniqueness of the distinguished name assigned to the Subject within the domain of the CA (i.e. over the lifetime of the CA a distinguished name which has been used in an issued certificate shall never be re-assigned to another entity).
- The confidentiality and integrity of registration data shall be protected especially when exchanged with the Subscriber, Subject or between distributed CA system components.
- The CA shall ensure that registration data is exchanged only with authorized Registration Authorities, whose identity is verified, when external Registration Authorities are used.

4.3 Certificate acceptance

The Subject is considered to have accepted the certificate when the private key associated with it has been used.

TeliaSonera Finland Oyj
Enterprise Services

4.4 Certificate revocation and suspension

4.4.1 Circumstances for revocation

A Subject or Subscriber shall promptly request revocation of a certificate if any of the circumstances realize, that have been listed in paragraph 2.1.3 "Subscriber obligations" in the item stating the obligation of the Subject to notify the CA.

The Revocation Service will send a revocation request to the CA, and the CA revokes or suspends the certificate:

- upon request from the Subscriber or Subject,
- upon failure of the Subscriber or Subject to meet its material obligations under this Policy, the CPS, or any other agreement, regulation, or law applicable to the certification services,
- if there are reasons to suspect that the Subject private key is compromised,
- if there are reasons to suspect that the information in the certificate is inaccurate or has changed,
- if the CA determines that the certificate was not properly issued in accordance with this Policy and the CPS,
- if there is another justified reason to revoke the certificate.

4.4.2 Who can request revocation

The only parties permitted to request revocation of a certificate issued pursuant to this Policy are the Subscriber, the Subject, the Registration Officer of the Customer Organization, and the issuing CA.

The Revocation Service shall send the revocation request to the CA only upon verification of the identity of the person requesting revocation.

4.4.3 Procedure for revocation request

The CA shall ensure that certificates are revoked or suspended (i.e. cancelled for the time being, see paragraph 4.4.4 "Certificate suspension") in a timely manner based on authorized and validated certificate revocation requests. In particular:

- Requests relating to revocation (e.g. due to compromise of Subject private key, death of the Subject, unexpected termination of a Subscriber's or Subject's agreement or business functions, or violation of contractual obligations) shall be processed in a timely manner on receipt.
- Requests relating to revocation shall be authenticated and checked to be from an authorized source. The requests shall be checked according to the CA's defined practices.
- Once a certificate is definitively revoked (i.e. not suspended), it can no more be reinstated.

4.4.4 Certificate suspension

A Subscriber or Subject cannot request suspension (i.e. temporary cancellation) of a certificate. The CA will make the decision on certificate suspension.

A certificate may be suspended, on the CA's decision, until an appropriate certificate reinstatement request has been received and the certificate has been reinstated, or the revocation request has been finally confirmed, or after the pre-defined time period has passed since the reinstatement, when the certificate shall be revoked for good.

TeliaSonera Finland Oyj
Enterprise Services

4.4.5 CRL issuance

The CA provides the Revocation Status Service, where information on revoked certificates is permanently and publicly available. Certificate Revocation Lists are published regularly (also when no new revocation requests have been received). CRL issuance practices, frequencies and validity periods have been specified in the CPS. The integrity and authenticity of the CRL information shall be ensured.

Instead of publishing a complete CRL, a variant of it called delta CRL may be published. A delta CRL contains merely the revocation information that has changed since the publication of the previous CRL.

4.4.6 CRL checking requirements

A Relying Party is obliged to check the revocation status information on the CRL either itself or by acquiring the verification as a service. The verification shall be based on valid CRL information, which is available for Relying Parties. The validity of the certificate, its suspension status (temporary cancellation) and revocation status shall be checked from the CRL. The checking procedure has been described in the CPS.

The address for accessing the CRL is stated in the CPS. A certificate must not be relied on in the absence of valid CRL information.

4.5 Certificate reinstatement

If a certificate has been suspended, or temporarily cancelled, it can be reinstated on the Customer Organization's request. The procedure for reinstatement has been described in the CPS.

4.6 Security audit procedures

The CA records and monitors regularly essential information originating from or associated with certification operations. To a certain extent these audit logs are automatically stored in the systems of the CA, and for the rest the CA personnel records information manually.

The information to be recorded contains among other things audit logs on the life cycle of the CA signing key, the life cycle events of all certificates, and events related to information security management

The audit logs to be recorded, their collection, retention, protection, backup, and processing, as well as the CA system vulnerability assessment against external intrusion attempts have been described in the CPS in more detail.

4.7 Records archival

The CA stores in the archive records of the most essential information related to certification operations. In particular:

- The CA shall store in the archive records of all events related to the CA key pair life cycle, to the life cycle of each certificate issued by it, as well as of requests associated with certificate revocation and measures taken thereupon.
- The CA shall ensure that records of all events related to registration are stored in the archive, including certificate renewal requests and rekey requests.
- The precise time of significant CA environmental, key management and certificate management events shall be recorded and stored in the archive.

TeliaSonera Finland Oyj
Enterprise Services

- Records of essential information concerning each certificate issued by the CA shall be stored in the archive for a sufficiently long period of time.
- The confidentiality and integrity of the records containing data related to certificates shall be ensured.
- Records related to certificates may be handed over on request for the purpose of providing evidence of certification for legal proceedings.
- The events shall be logged in a way that they cannot be easily deleted or destroyed during their retention period.
- The CA shall ensure the privacy protection of the Subject's personal data.

The implementation of the requirements given above has been described in more detail in the CPS, where the information to be stored in the archive, the retention period for the archive, its protection and backup, as well as procedures to obtain and verify archive information have been defined.

4.8 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.

4.9 Compromise and disaster recovery

The CA shall ensure in the event of a disaster, including disclosure or compromise of the CA private signing key and corruption of computer resources, software, or data, that operations are restored as soon as possible.

4.9.1 Disaster recovery

The CA must have in place a business continuity plan or another appropriate plan to provide against disaster. The CA must be capable of providing CA services in accordance with this Policy within reasonable time of an unanticipated emergency. Such a plan shall include a periodic test of readiness for such facility.

4.9.2 Computing resources, software, and/or data are corrupted

The CA shall arrange for backup of its systems that are most critical regarding operations continuity, and of the software and data, such that they can be recovered from backup copies.

4.9.3 CA private key compromise

The Business Continuity Plan of the CA or another plan drawn up to provide against disaster shall include instructions on measures to be taken in the case of compromise or suspected compromise of a CA private key.

In the case of a CA private key compromise at least the following measures shall be taken by the CA:

- Inform immediately all Subscribers and other CAs with which it has agreements of the compromise.
- Declare that certificates and revocation status information signed using the compromised CA key are no longer valid.

TeliaSonera Finland Oyj
Enterprise Services

4.9.4 Secure facility after a natural or other type of disaster

The systems of the CA are located in premises that are secure enough taking into account the requirement for uninterrupted operations.

4.10 CA termination

The CA shall ensure that disruptions to Subscribers and Relying Parties are minimized as a result of the termination of the certification operations. The CA does not ensure retention of the archive after the termination.

Before the CA terminates its operations the following procedures shall be executed as a minimum:

- The CA shall inform all Subscribers and other CAs with which it has agreements.
- The CA shall terminate all authorizations concerning outsourced operations related to the process of issuing certificates.
- The CA shall ensure that certificates issued by it cannot be used any more or reasonably relied on.
- The CA private keys shall be destroyed or taken out of use.

TeliaSonera Finland Oyj
Enterprise Services

5 Physical, procedural and personnel security controls

5.1 Physical and environmental controls

The CA shall ensure that physical access to critical services is controlled and physical risks to the CA production system are minimized. In particular:

- Physical access to premises concerned with certificate generation, Signature-Creation Device provision, and revocation management services shall be limited to properly authorized individuals.
- Adequate controls shall be implemented to avoid loss, damage, or compromise of hardware or software used in the systems of the CA, or interruption to business activities as a consequence of those events.
- Equipment, information, media, and software relating to certification services shall be protected against being taken off-site without authorization.
- Adequate controls shall be implemented to avoid compromise or theft of information and breaking into the information processing premises.
- Physical and environmental security controls shall be implemented to protect the facility housing system resources, the system resources themselves, and the facilities used to support their operation. The CA shall establish and implement security controls related to the certification services production environment, including physical access control, fire safety control, protection against failure of supporting utilities (e.g. power, telecommunications), plumbing leaks, theft, breaking and entering, as well as security measures for disaster recovery.

In order to meet the requirements given above, measures shall be taken concerning the following areas, which are described in the CPS in more detail:

- site location and construction,
- physical access,
- power and air conditioning,
- water exposures,
- fire prevention and protection,
- media storage,
- waste disposal,
- off-site backup.

5.2 Procedural controls

5.2.1 Trusted roles

The trusted roles related to the operations of the CA shall be clearly identified.

The trusted roles involve the following responsibilities:

- **Security Manager:** Overall responsibility for administering the implementation of the security practices,
- **PKI Administrator:** Authorized to install, configure and maintain the CA trustworthy systems for registration, certificate generation, Signature-Creation Device provision, and revocation management,
- **PKI Operator:** Responsible for operating the CA trustworthy systems on a day-to-day basis. Authorized to perform system backup and recovery,
- **Audit Manager:** Authorized to view and maintain archives and audit logs of the CA trustworthy systems,

TeliaSonera Finland Oyj
Enterprise Services

- **Registration Officer:** Responsible for approval of certificate generation and dissemination procedures,
- **Revocation Officer:** Responsible for approval of revocation and revocation list procedures.

The persons in trusted roles agree to be bound by this Policy.

5.2.2 Number of persons required per task

The following tasks shall require at least dual control:

- Changes in the CA system environment.

Simultaneous control of at least three persons is required for the tasks below:

- CA key generation
- backup and recovery of the CA private signing key.

5.2.3 Identification and authentication for each role

Verification of identity of the persons in the most important trusted roles requires use of certificates. Identity verification for each role has been described in the CPS.

5.2.4 Internal documentation

The internal documentation has been described in the CPS.

5.3 Personnel controls

5.3.1 Background information, qualifications, experience, and other requirements

The CA shall ensure that its personnel policy supports the trustworthiness of the CA operations. In particular:

- The CA shall employ personnel, which possess the expert knowledge, experience and qualifications necessary for the offered services and as appropriate to the job function.
- Managerial personnel shall be employed who possess expertise in the electronic signature technology and familiarity with security procedures for personnel with security responsibilities and experience with information security and risk assessment.
- Security roles and the related responsibilities shall be stated in the Security Policy of the CA.
- CA personnel shall be appointed to trusted roles by senior management responsible for security.
- The CA shall not appoint to trusted roles or management any person who is known to have a conviction for a serious crime or other offence, which affects his/her suitability for the position. Personnel shall not have access to the trusted functions until any necessary checks are completed.
- Responsibilities shall be delegated to CA personnel from the viewpoint of separation of duties and principle of least privilege.
- CA personnel shall discharge their duties related to system administration and management, and maintain the processes according to the procedures described by the CA.

TeliaSonera Finland Oyj
Enterprise Services

5.3.2 Background check procedures

The CA shall conduct appropriate investigations of all personnel that it employs. The purpose of the investigation is to verify the trustworthiness and competence of a person according to the personnel practices of the CA.

A background check by a third party shall be conducted when a person serves in one of the most important trusted roles. These roles have been specified in the CPS. All personnel who fail an initial or periodic investigation shall not serve or continue to serve in a trusted role.

5.3.3 Training requirements

All personnel participating in the CA operations, RA operations, or certificate manufacturing, must receive proper training in order to perform their duties. Expertise shall be maintained by update briefings thereafter.

5.3.4 Sanctions for unauthorized actions

If the CA discovers a malpractice in certification operations, it shall immediately take the necessary measures to eliminate the resultant damage and to prevent further malpractice.

5.3.5 Documentation supplied to personnel

All personnel participating in the CA operations, RA operations, or certificate manufacturing shall receive comprehensive user manuals detailing the procedures for certificate registration, generation, update, renewal, suspension, and revocation, and software functionality

TeliaSonera Finland Oyj
Enterprise Services

6 Technical security controls

6.1 CA key pair generation, installation, and protection

6.1.1 CA key pair generation

The CA shall ensure that CA keys are generated in controlled circumstances.

In particular, the CA shall ensure that Certification Authority key generation is undertaken in a physically secure environment by persons in trusted roles. Simultaneous control of at least three individuals is required to perform the task. The CA shall keep to a minimum the number of personnel authorized to carry out this function, according to its practices.

6.1.2 CA public key delivery to users

The CA shall ensure that the integrity and authenticity of the CA public key and any associated parameters are maintained when the key is made available to Relying Parties.

The CA public key is available on the internet at the address given in the CPS.

6.1.3 CA key sizes and algorithm

The length of the CA signing key and the algorithm used with the key shall be chosen such that they are generally considered to be acceptable for certification purposes.

6.1.4 Usage period for CA key pair

The usage period of the CA private key and the validity period of the CA certificate shall not be longer than twenty (20) years. The CA private key can be used for the signing of Subject certificates for the usage period of the CA key pair 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. CRLs can be signed with the CA private key throughout the usage period of the CA key pair.

6.1.5 CA key usage purposes

The CA shall ensure that CA signing keys are not used for other purposes than for issuing certificates and revocation status information, and that the keys are used only within physically secure premises.

6.1.6 CA private key protection

The CA shall ensure that CA private keys remain confidential and maintain their integrity.

TeliaSonera Finland Oyj
Enterprise Services

When outside the secure Signature-Creation Device the CA private signing key shall be encrypted using an algorithm and key-length that, according to the state of the art, are capable to withstand cryptanalytic attacks for the residual life of the encrypted key or key part.

The CA private signing key shall be backed up, stored and recovered only by personnel in trusted roles using, at least, dual control in a physically secure environment. The CA shall keep to a minimum the number of personnel authorized to carry out this function, according to its practices.

Backup copies of the CA private signing keys shall be subject to the same or greater level of security controls as keys currently in use.

Where the keys are stored in a dedicated key processing hardware module, access controls shall be in place to ensure that the keys are not accessible outside the hardware module.

A cryptographic module conforming at least to the FIPS 140-1 level 2 standard shall be used to protect the CA private signing keys.

6.1.7 CA private key escrow

Copies of CA private signing keys shall not be delivered to be maintained by third parties in a way, which, under certain conditions, provides for the keys to be used by persons not involved in the CA operations (commonly called key escrow).

6.1.8 CA private key backup

The CA makes copies of its private keys such that the same security level is ensured for recovery from backup copies as is applied to private key generation.

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

A private key of the CA is activated in pursuance of its generation in accordance with paragraph 6.1.1 "CA key pair generation". The key will stay active until its use is interrupted for e.g. maintenance measures.

6.1.11 Method of deactivating CA private key

The CA private key is deactivated when needed, e.g. for maintenance measures, by the personnel in trusted roles of the CA.

6.1.12 Method of destroying CA private key

The CA shall ensure that the private keys of the CA are destroyed, or they will not be used, after the end of their life cycle.

TeliaSonera Finland Oyj
Enterprise Services

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 Subject key pair generation, installation, and protection

6.2.1 Subject key pair generation

Key pairs for Sonera Class 1 certificates are generated by the CA or in Customer Organizations.

The CA shall ensure, when on its own responsibility, that the key pair is generated securely maintaining the confidentiality of the private key.

6.2.2 Subject private key delivery to Subject

If the CA generates the key pair, the private key will be delivered to the Subject in a manner such that the secrecy of the key is not compromised.

The Signature-Creation Device containing the private key shall be manufactured securely. The CA shall ensure that the Signature-Creation Device is properly stored and distributed.

6.2.3 Subject public key delivery to CA

An organization operating as Registration Authority or Certificate Manufacturer generates the keys related to a Sonera Class 1 certificate and delivers the public key in a certificate request electronically signed to the CA system.

6.2.4 Subject key sizes and algorithm

The length of the Subject private key and the algorithm used with the key shall be chosen such that they are generally considered to be secure enough.

6.2.5 Usage periods for Subject keys

The usage period of the Subject public and private keys shall not be longer than **ten (10) years**. The same keys may be certified again on expiration of a certificate. 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.

6.2.6 Subject key usage purposes

The private keys associated with certificates issued according to this Policy shall only be used to support the following security services:

- Subject authentication,
- verification of digital data origin and integrity,

TeliaSonera Finland Oyj
Enterprise Services

- confidentiality of digital data,
- non-repudiation with electronic signatures.

6.2.7 Subject private key protection

The private key associated with a Sonera Class 1 certificate shall be protected as follows:

- The Subject can maintain the private key under his sole control after delivery to the Subject.
- The secrecy of the private key is reasonably assured.
- The private key can be reliably protected by the Subject against the use of others.

When the CA generates the keys it shall ensure their secrecy until delivery to the Subscriber or Subject. The CA shall give necessary advice to the Subscriber or Subject for key protection.

6.2.8 Subject private key escrow

Copies of the private key of the Subject are not delivered to be maintained or used by third parties.

6.2.9 Subject private key backup

The Subject private key used for non-repudiation purposes shall not be backed up. A backup copy may be made of the private key used for confidentiality purposes, provided there is an agreement on this with the Subscriber.

6.2.10 Subject private key archival

The Subject private key shall not be archived.

6.2.11 Method of activating Subject private key

The Subject private key requires activation by using a PIN code.

6.2.12 Method of deactivating Subject private key

After a predefined number of failed activation attempts, the Subject private key will be locked.

6.2.13 Method of destroying Subject private key

The Subject private keys are not destroyed after their usage period, but they remain in the possession of the Subject after the end of their life cycle.

6.2.14 Subject public key archival

The CA stores the Subject public keys according to paragraph 4.7 "Records archival".

TeliaSonera Finland Oyj
Enterprise Services

6.3 Subject activation data

6.3.1 Activation data generation and installation

The activation data (PIN code) that is generated at the same time with the key pair generation, and that is used to activate the private key, will be delivered to the Subject in a way that allows him alone to access it, or failing that can be clearly noticed by the Subject, or the Subject is advised to change the activation data immediately.

The activation data is comprised of **at least four (4) characters or digits**.

When a Subject is given the choice to change the activation data, the Subscriber is obliged to ensure that an adequate number of characters comprise the new activation data which shall not be easy to guess or deduce.

6.3.2 Activation data protection

It is the Subscriber's responsibility to ensure that the Subject is bound to keep his activation data secure enough.

6.4 Computer security controls

The CA shall use trustworthy systems and products that are protected against modification.

In particular, the systems shall provide the following functions:

- authentication of all users,
- role-based access control,
- control by several individuals required for certain security-related operations,
- audit log generation, audit review, and storing of all security-related events in archive,
- backup and recovery,
- secure disposal of information when no longer needed.

6.5 Life cycle technical controls

6.5.1 System development controls

The CA uses trustworthy systems and products that are protected against modification.

Change control procedures exist for releases, modifications and emergency software fixes for any operational software.

6.5.2 Security management controls

6.5.2.1 Security management

The CA shall ensure that administrative and management procedures are applied which are adequate and correspond to recognized standards. In particular:

TeliaSonera Finland Oyj
Enterprise Services

- The CA shall carry out risk assessments to evaluate business risks and determine the necessary security requirements and operational procedures.
- The CA shall retain responsibility for all aspects of the provision of certification services, even if some functions are outsourced to subcontractors. Responsibilities of third parties shall be clearly defined by the CA and appropriate arrangements made to ensure that third parties are bound to implement any practices defined by the CA. The CA shall retain responsibility for the disclosure of relevant practices to all parties.
- The management of the organization of the CA shall direct the operations related to information security and shall be responsible for defining the Security Policy of the CA and ensuring publication and communication of the Security Policy to all employees who are impacted by it.
- The information security infrastructure necessary to manage the security within the CA shall be maintained continuously. Any changes that will impact on the level of security provided shall be approved by the management of the organization of the CA.
- The security controls and operating procedures for CA facilities, systems and information assets providing certification services shall be documented, implemented and maintained.
- The CA shall ensure that the security of information shall be maintained when the responsibility for CA functions has been outsourced to another organization or entity.

6.5.2.2 Management of resources

The CA shall ensure that the level of protection of its assets and information is sufficiently high.

6.5.2.3 Operations management

The CA shall ensure that its systems are secure and correctly operated, with minimal risk of failure. In particular:

- The integrity of the systems and information of the CA shall be protected against viruses and malicious and unauthorized software.
- Damage from security attacks and malfunctions shall be minimized through the use of incident reporting and response procedures.
- All storage equipment and media used within the CA shall be securely handled to protect media from damage, theft and unauthorized access.
- Adequate operations models and procedures shall be established and implemented for all roles defined in paragraph 5.2.1 "Trusted roles".

Media handling and security

All media shall be handled securely. Media containing sensitive data shall be securely stored for disposal or disposed of when no longer needed.

System planning

Capacity usage is monitored and projections of future capacity requirements made to ensure that adequate processing power and storage are available.

Incident reporting and response

The CA shall act in an accurate and co-ordinated manner in order to respond quickly to incidents and to limit the impact of breaches of security. All incidents shall be reported as soon as possible after the incident.

Operations procedures and responsibilities

CA security operations shall be separated from normal operations.

TeliaSonera Finland Oyj
Enterprise Services

6.5.2.4 System access control

The CA shall ensure that CA system access is limited to properly authorized individuals. In particular:

General CA operations

- The CA shall ensure effective administration of user access to maintain system security, including user account management, auditing, and timely modification or removal of access. The user access administration includes access for system operators, administrators and any users given access to the system.
- The CA shall ensure access to information and application system functions are restricted in accordance with the access control policy and that the CA system provides sufficient computer security controls for the separation of roles defined in paragraph 5.2.1 "Trusted roles". Particularly the Security Manager role shall be separated from operation functions, and use of system utility programs shall be restricted and tightly controlled.
- CA personnel shall be successfully authenticated before using critical applications related to certificate management.
- CA personnel shall be accountable for their activities, for example by reviewing event logs.
- Sensitive data shall be protected against being revealed through re-used storage objects (e.g. deleted files) being accessible to unauthorized users.

Certificate dissemination

- Dissemination application shall enforce access control on attempts to add or delete certificates and modify associated information.

Revocation Status Service

- Revocation status application shall enforce access control on attempts to modify revocation status information.

6.5.2.5 Cryptographic module life cycle management

The CA shall ensure the security of the cryptographic module used in issuance of certificates and CRLs throughout its lifecycle. In particular the CA shall ensure that:

- the cryptographic module is not tampered with during shipment or while stored in a way not detectable,
- the installation, activation, back-up, and recovery of the CA signing keys in cryptographic module shall require simultaneous control of at least two trusted employees,
- the cryptographic module is functioning correctly,
- CA private signing keys stored on the cryptographic module are destroyed upon device retirement.

6.6 Network security controls

The CA shall ensure the secure management of the network with the following arrangements:

- The internal network of the CA shall be protected from external networks used by third parties.
- Sensitive information shall be protected when transmitted through insecure networks.
- The CA shall ensure that local network components (e.g. routers) are kept in a physically secure environment.
- The CA shall provide against security incidents by continuously monitoring its systems and using alarm equipment. Such incidents include among other things unauthorized or irregular attempts to access the CA's resources.

TeliaSonera Finland Oyj
Enterprise Services

7 Sonera Class 1 Certificate and CRL profiles

7.1 Certificate profile

All certificates referencing this Policy shall be issued in conformity with version 3 profile of the X.509 standard.

The certificates comply with the requirements in the document RFC 3280 "Internet X.509 Public Key Infrastructure Certificate and CRL Profile".

7.1.1 Certificate fields and their contents

The fields of a Sonera Class 1 certificate have been specified in the CPS. Contents of some of the most important fields have been depicted below.

7.1.1.1 Basic certificate fields

7.1.1.1.1 Version

The version of a Sonera Class 1 certificate is v3.

7.1.1.1.2 Issuer field

The contents of the "Issuer" field have been described in paragraph 3.1 "Naming practices for CA certificates".

7.1.1.1.3 Subject field

The contents of the "Subject" field have been described in paragraph 3.2 "Initial registration".

7.1.1.2 Certificate extensions

7.1.1.2.1 Object identifier of the Policy (OID)

Sonera Class 1 certificates shall contain the Object Identifier corresponding to this Certificate Policy as specified in paragraph 1.2 "Identification of the document".

A certificate may contain also additional OIDs of other certificate policies that the CA is conforming to.

7.1.1.3 Certificate field contents

Contents of the fields in a certificate have been specified in detail in the CPS.

TeliaSonera Finland Oyj
Enterprise Services

7.2 CRL profile

Certificate Revocation Lists are issued in conformity with version 2 profile of the X.509 standard. The CRLs comply with the requirements in the document RFC 3280 "Internet X.509 Public Key Infrastructure Certificate and CRL Profile".

The fields and their contents have been specified in the CPS.

TeliaSonera Finland Oyj
Enterprise Services

8 CP administration

8.1 Change procedures

8.1.1 Items that can change without notification

Typographical or editorial corrections, or changes to the 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 CP may be changed with 15 days prior notice.

All the proposed changes requiring notification shall be published at:

<http://support.partnergate.sonera.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.

8.1.3 Changes that require new CP

If a policy change is determined by Sonera CA Policy Authority to have a material impact on a significant number of users of the Policy, the Policy Authority may, at its sole discretion, assign a new object identifier to the modified Policy. The CA shall make the new Policy available to those impacted by it.

8.2 Publication policies

A copy of this Certificate Policy is available in electronic form on the internet at:

<http://support.partnergate.sonera.com/>.

8.3 CPS approval procedures

Sonera CA Policy Authority is responsible for the contents of this document and approval by the Policy Authority is required for any change to it.

TeliaSonera Finland Oyj
Enterprise Services

9 Certification Practice Statement (CPS)

The CA shall ensure that it demonstrates the reliability necessary for providing certification services. In particular:

- a) The CA shall have a public statement of the practices and procedures used to address all the requirements identified in this Certificate Policy.
- b) The Certification Practice Statement shall identify the obligations of all external organizations involved in the CA operations including the applicable policies and practices.
- c) The CA shall make available to Subscribers and Relying Parties its CPS, and other relevant documentation, as necessary to assess conformance to this Certificate Policy.
- d) The CA shall disclose to all Subscribers and potential Relying Parties the terms and conditions regarding use of the certificate.
- e) The CA shall have a high-level management body with final authority and responsibility for approving the CPS.
- f) The senior management of the CA has responsibility for ensuring the practices are properly implemented.
- g) The CA shall define a review process for certification practices including responsibilities for maintaining the CPS.
- h) The CA shall give due notice of changes it intends to make in its CPS and shall, following approval as in (e) above, make the revised CPS immediately available as required under (c) above.

The Certification Practice Statement is a document where the CA describes how it implements a certain Certificate Policy. The practices and procedures corresponding to this Certificate Policy have been described in the document "Sonera CA Certification Practice Statement" that is available on the internet at <http://support.partnergate.sonera.com/>.

TeliaSonera Finland Oyj
Enterprise Services

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