TeliaSonera Production Certification Practice Statement

Date: 3rd April 2014

Version: 2.2

Published by: TeliaSonera

Table of Contents

Revision History

Version	Version date	Change	Author
1.0		The first version. Never officially published.	Telia CA Policy Management Team
2.0	2012-06-11	The first official version. Defines common CA policy elements for the multinational TeliaSonera CA hierarchy	TeliaSonera CA Policy Management Team
2.01	2012-09-11	Fixed minor errors in references	TeliaSonera CA Policy Management Team
2.1	2013-05-16	Offline Root CA addition	TeliaSonera CA Policy Management Team
2.2	2014-04-03	Changed chapters “Number of persons required per task” and “Sanctions for unauthorized actions”	TeliaSonera CA Policy Management Team

1 INTRODUCTION

1.1 Overview

A Certification Practice Statement (CPS) is a Certification Authority's (CA) description of the practices it follows when issuing certificates.

This Certification Practice Statement (CPS) describes the premises, procedures and routines which apply for the Production of TeliaSonera CA Services. The TeliaSonera CA Services will sign and issue certificates to TeliaSonera Customers. A Customer to TeliaSonera will be a part of the TeliaSonera CA Services or host their CA at the TeliaSonera site.

The CPS doesn't describe the content of the issued certificates or procedures and routines regarding the issuance, revocation and usage of the certificates. This CPS will be referred to in other CPS's that specifies the different TeliaSonera CA Services or Customers CAs that are produced in the TeliaSonera production systems. Such CPS will describe the content of the issued certificates and procedures and routines regarding the issuance, revocation and usage of the certificates.

The CPS's referring to this CPS may specify some of the sections mentioned in this CPS in a greater detail.

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

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

1.2 Document name and identification

This CPS is titled **TeliaSonera Production CPS**. The CPS name of this CPS is TELIASONERA-PRODUCTION-CPS-2 and the object identifier is 1.3.6.1.4.1.271.2.3.1.1.10.

This CPS is common for all TeliaSonera certificates so that other TeliaSonera CPS documents may refer to this document. Issued certificates will refer to the OID related to the specific other CPS.

1.3 PKI participants

TeliaSonera will issue certificates to Customers of TeliaSonera and to TeliaSonera employees. All the participating entities will have their CA hosted by TeliaSonera CA Services and all entities shall undertake what's stated in the TeliaSonera Production CPS.

This CPS applies to CAs, RAs contracted by CAs, system component suppliers and auditors.

1.3.1 Certification Authorities (CA)

TeliaSonera manages the CA Services. CA's are created for TeliaSonera services and TeliaSonera Customers. The CPS's of those CAs may refer to this CPS for the parts of the CPS describing the production premises and processes.

The TeliaSonera CA Services is responsible for managing the certificate life cycle of CAs and end entity certificates signed by the CAs. This will include:

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

More specific information regarding Certification Authorities will be specified in each CPS referring to this Production CPS.

1.3.2 Registration Authorities (RA)

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

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

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

More specific information regarding RAs will be specified in each CPS referring to this Production CPS.

1.3.3 Subscribers

The Subscriber makes an agreement with the CA about issuance of a certificate either to itself or to a natural person or function represented by it or to a Device in its possession (Subject). The Subscriber shall ensure that the Subject fulfils the obligations defined in this CPS and the conditions of the certification services. A Subject may be:

- an organization that is a Customer of TeliaSonera and hosting their CA at TeliaSonera.
- an individual employed by a Customer of TeliaSonera or by TeliaSonera
- an individual that is a Customer of TeliaSonera
- A device situated at a Customer to TeliaSonera or at TeliaSonera
- A function at a Customer to TeliaSonera or at TeliaSonera

1.3.4 Relying parties

A Relying Party may be either a Subscriber of any TeliaSonera CA or any other organization, individual, application or device that is relying on a certificate issued by a CA that is produced by the TeliaSonera CA Service.

1.3.5 Other participants

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

For example a certificate manufacturer within TeliaSonera PKI is the card manufacturer, responsible for the smart card life cycle.

1.4 Certificate usage

Certificates issued under this CPS can be used for many various applications like business transactions (server to server), encrypted and signed emails (S/MIME) and other applications where the need for integrity, authenticity and confidentiality is a strong requirement.

More specific information regarding Certificate usage will be specified in each CPS referring to this Production CPS.

1.5 Policy administration

1.5.1 Organization administering the document

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

Contact information:

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

1.5.2 Contact person

Contact point in matters related to this CPS:

TeliaSonera CA Policy Management Team
Email: cainfo@sonera.com
Phone: +358 (0) 20401
Internet: https://repository.trust.teliasonera.com/

1.5.3 Person determining CPS suitability for the policy

All stipulations regarding the section 1.5.3 Person determining suitability for the policy will be specified in each CPS referring to this Production CPS.

1.5.4 CPS approval procedures

TeliaSonera CA Policy Management Team will review any modifications, additions or deletions from this CPS that are obligated to be compliant with the CP's stated in all CPS's referring to this Production CPS.

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

1.6 Definitions and acronyms

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

2 PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 Repositories

2.1.1 CPS Repository

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

2.1.2 Revocation Information Repository

Certificate Revocation Lists (CRLs) are published in the TeliaSonera LDAP directory.

A relying party who wants to validate certificates by OCSP needs to make an agreement with TeliaSonera. OCSP requests may be signed or unsigned depending on the Customer agreement and the payment method.

2.1.3 Certificate Repository

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

All issued CA certificates are published in TeliaSonera LDAP directory and in TeliaSonera HTTP server.

2.2 Publication of certification information

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

a) This CPS.

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

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

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

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

TeliaSonera supplies CA certificates for all public CA keys.

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

2.3 Time or frequency of publication

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

Revocation information publication provisions will be specified in each CPS referring to this Production CPS.

2.4 Access controls on repositories

This CPS, CRLs and CA certificates are publicly available.

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

3 IDENTIFICATION AND AUTHENTICATION

All stipulations regarding chapter **3 Identification and Authentication** will be specified in each CPS referring to this Production CPS.

4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

All stipulations regarding chapter **4 Certificate life-cycle operational requirements** will be specified in each CPS referring to this Production CPS except for the section mentioned below.

Key escrow and recovery

4.1.1 Key escrow and recovery policy and practices

CA Private Signing Keys will not be escrowed.

5 FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

5.1 Physical controls

5.1.1 Site location and construction

TeliaSonera's CA and RA operations are conducted within TeliaSonera's premises in Finland and Sweden, which meet the requirements of Security and Audit Requirements as stated in all CPS's referring to this Production CPS.

All TeliaSonera CA and RA operations are conducted within a physically protected environment designed to deter, prevent, and detect covert or overt penetration.

5.1.1.1 CA Site location and construction

The premises where central CA functions take place are physically located in a highly secure server rooms dedicated for CA operations, The physical protection of which corresponds at least with the requirements for "priority 1 premises" defined in the regulation on priority rating, redundancy, power supply and physical protection of communications networks and services (54/2008 M) issued by Ficora (Finnish Communications Regulatory Authority).Within these server rooms, key components are locked in separate, freestanding security cabinets.

The server rooms, which are locked and alarmed, are in secure buildings, which are also locked and alarmed. These are protected jointly by using active monitoring.

5.1.1.2 RA Site location and construction

The premises where central RA functions take place are physically located in highly secure server rooms.

Within these server rooms, key components are locked in separate, freestanding security cabinets.

The server rooms, which are locked and alarmed, are in secure buildings, which are also locked and alarmed. These are protected jointly by using active monitoring.

Certain RA functions comprising roles in accordance with section 5.2.1 may be carried out outside the physical environment of the protected premises detailed above. These are:

a. Identification on application of key holders who are present in person.
b. Issuing keys and codes.
c. Identifying key holders and ownership of the correct private key on electronic application.
d. Electronic registration of key holders.
e. Revocation service for revoking certificates.

Functions in accordance with a) do not involve any access to the central RA system. This environment therefore has no specific security provisions in terms of physical security.

Functions in accordance with b) to e) are carried out in well controlled office environments where access is restricted to authorized personnel. No keys or codes are left unmonitored.

In the case where the CA is a Customer's CA, the stipulations above for physical protection of the locality for RA functions may not be followed.

5.1.2 Physical access

For security reasons, detailed information on security procedures for physical access to the premises is not publicly available but is described in the TeliaSonera Operational Documentation. The security procedures are described in separate documentations belonging to the TeliaSonera CA Services.

The premises' external protection such as locks and alarm systems are monitored each day on a 24-hour basis by security staff on duty.

Unescorted access to the CA and RA sites and servers is limited to personnel identified on access lists. Personnel that is not included on the access lists will be escorted by authorized personnel and supervised during their work.

Site access is monitored in real time or access logs are inspected periodically at least quarterly by qualified personnel. The inspection documentation is retained for at least a one-year period to support audit requirements.

All access control and monitoring systems are tied to UPS's. The UPS systems are inspected and tested at least annually and the inspection documentation is retained for at least a one-year period.

5.1.2.1 CA Site Physical access

TeliaSonera CA facilities are protected by four tiers of physical security where the CA systems and other important CA devices have been placed in a security vault. The security vault has been placed in a rock shelter that provide good structural security and fire protection for the CA equipment. Progressively restrictive physical access privileges control access to each tier.
The characteristics and requirements of each tier are described in the table below.

Tier	*Description*	*Access Control Mechanisms*
Physical Security Tier 1 " Entrance to rock shelter"	Physical security tier one refers to the outermost physical security barrier for the facility.	Access to this tier requires the use of a proximity card employee badge and related PIN code. Physical access to tier one is automatically logged.
Physical Security Tier 2 "Rock shelter Tunnel"	Tier two includes common areas including restrooms and common hallways.	Tier two enforces individual access control for all persons entering the common areas of the CA facility through the use of a proximity card employee badge. Physical access to tier two is automatically logged.
Physical Security Tier 3 "CA Security area"	CA Security Area is the room that separates the Security Vault from the rock shelter tunnel.	Access to CA Security Area requires the usage of an individual access card combined with a PIN code. In addition a separate burglar alarm system has to be inactivated by individual access codes. Physical access is automatically logged, video recorded and a special notification is generated to the CA Security Board members about each access to CA Security Area.
Physical Security Tiers 4 "CA Vault"	The CA Security Vault is where the CA systems and other critical devices are placed and where sensitive CA operations occur. Tier four is the only tier where local maintenance access to servers is possible.	The tier four data center enforces individual access control with a PIN code and it enforces dual control if incoming persons have access also to Tiers 5. Dual control is enforced through special individual partial access control to doors and burglar alarm systems. To such person or to outsider the authorization for unescorted access to the tier four rooms is not given. Physical access to tier four is automatically logged and video monitored and a special notification is generated to the CA Security Board members. CA Security Board member will always check, grant and document each access to Tiers 4.

Tier	Description	Access Control Mechanisms
Physical Security Tiers 5 "Key Management"	Key Management tiers five serve to protect CA HSMs keying material and other most critical components.	Online HSMs and other most critical components are protected through the use of locked cabinets that always require dual control to be accessed. Offline keying material like CA system or root key backups and secret shares are protected through the use of locked safes, cabinets and containers. Access to HSMs and keying material is restricted in accordance with TeliaSonera's segregation of duties requirements. The opening and closing of cabinets or containers in this tier is logged for audit purposes. All access is video monitored.

5.1.2.2 RA Site Physical access

The TeliaSonera RA systems are protected by four tiers of physical security, with access to the lower tier required before gaining access to the higher tier. In addition, the physical security system includes additional tiers for key management security. Progressively restrictive physical access privileges control access to each tier. The characteristics and requirements of each tier are described in the table below.

Tier	Description	Access Control Mechanisms
Physical Security Tier 1	Physical security tier one refers to the outermost physical security barrier for the facility.	Access to this tier requires the use of a proximity card employee badge. Physical access to tier one is automatically logged.
Physical Security Tier 2	Tier two includes common areas including restrooms and common hallways.	Tier two enforces individual access control for all persons entering the common areas of the RA facility through the use of a proximity card employee badge. Physical access to tier two is automatically logged.
Physical Security Tier 3	Tier three is the first tier at which sensitive central RA systems are located and where operational activity takes place.	Tier three enforces individual access control through the use of two factor authentication including biometrics or proximity card employee badge and PIN code. Unescorted personnel are not allowed into a tier-three secured area. Physical access to tier three is automatically logged.
Physical Security Tiers 4	Tier four is used only in TeliaSonera Sweden. Tier four is the tier at which especially sensitive RA operations occur. There are two distinct tier four areas: the online tier four data center and the offline tier four key storage room.	The tier four data center enforces individual access control and the key storage room enforces dual control, each through the use of two factor authentication including biometrics. Authorizations for unescorted access to both the tier four rooms are not given to any individual. Physical access to tier four is automatically logged and video monitored.

Tier	*Description*	*Access Control Mechanisms*
Key Management Tiers 5	Tier five is used only in TeliaSonera Sweden. Key Management tiers five serve to protect both online and offline storage of RA HSMs and keying material. RA HSMs are used to store OCSP signing keys and encryption keys protecting archived Subscriber private keys.	Online HSMs are protected through the use of locked cabinets that at least require dual control to be accessed. Offline keying material like RA system key backups and secret shares are protected through the use of locked safes, cabinets and containers. Access to HSMs and keying material is restricted in accordance with TeliaSonera's segregation of duties requirements. The opening and closing of cabinets or containers in this tier is logged for audit purposes. All access is video monitored.

5.1.3 Power and air conditioning

TeliaSonera secure premises are equipped with primary and backup:

a. power systems to ensure continuous, uninterrupted access to electric power and
b. heating/ventilation/air conditioning systems to control temperature and relative humidity.

5.1.4 Water exposures

TeliaSonera has taken reasonable precautions to minimize the impact of water exposure to TeliaSonera systems. Exposure to water damages is prevented with structural solutions.

5.1.5 Fire prevention and protection

TeliaSonera has taken reasonable precautions to prevent and extinguish fires or other damaging exposure to flame or smoke. TeliaSonera's fire prevention and protection measures have been designed to comply with local fire safety regulations and Inergen gaz are used as extinguishing method in certain data centers.

5.1.6 Media storage

All media containing production software and data, audit, archive, or backup information is stored within the TeliaSonera facilities or in a secure off-site storage premises with appropriate physical and logical access controls designed to limit access to authorized personnel and protect such media from accidental damage (e.g., water, fire, and electromagnetic).

5.1.7 Waste disposal

Sensitive documents and materials are shredded before disposal. Media used to collect or transmit sensitive information are rendered unreadable before disposal. Cryptographic devices are physically destroyed or erased in accordance the manufacturers' guidance prior to disposal. Other waste is disposed of in accordance with TeliaSonera's normal waste disposal requirements.

5.1.8 Off-site backup

TeliaSonera performs daily routine backups of critical system data, audit log data, and other sensitive information. The backups are either daily transported over a secure channel or periodically moved physically to an off-site storage facility.

5.2 Procedural controls

TeliaSonera is responsible for all procedures and circumstances defined in this section. This includes everything from production and logistics to the administration of the entire process.

Critical CA and RA operations is prohibited from being performed at distance over networks and must be performed locally at the CA and RA sites.

5.2.1 Trusted roles

Trusted Persons include all employees, contractors, and consultants that have access to or control authentication, cryptographic operations and information that may materially affect:

- the administration of CA private keys and central RA system private keys
- configurations of the CA and central RA systems
- the validation of information in Certificate Applications
- the acceptance, rejection, or other processing of Certificate Applications, revocation requests, or renewal requests, or enrollment information;
- the issuance, or revocation of Certificates, including personnel having access to restricted portions of its repository;
- or the handling of Subscriber information or requests.

Trusted Persons include, but are not limited to:

- Customer service personnel,
- cryptographic business operations personnel,
- security personnel,
- system administration personnel,
- designated engineering personnel, and
- executives that are designated to manage infrastructural trustworthiness.

TeliaSonera considers the categories of personnel identified in this section as Trusted Persons having a Trusted Position. Persons chosen to become Trusted Persons by obtaining a Trusted Position must successfully complete the screening requirements of section 5.3.

Examples of roles defined for CA and RA operations and maintenance are:

Certification Authority Administrator (CAA)
Administrative production/operational staff for the CA and RA systems.

Typical duties which may be administered by the CAA include:

- creating CA certificates
- personalising cards
- generating CA and central RA keys
- configuration of CA and RA applications
- generating revocation lists
- Checking the certificate issue log

System Administrator (SA):
Technical production/operational staff for the CA and RA systems.

Typical duties which may be administered by the SA include:

- installations of hardware and software
- system maintenance
- changing of backup media

Security Manager:
Overall responsibility for the security of the TeliaSonera CA Service.

Information Systems Security Officer (ISSO):
Typical duties which may be administered by the ISSO include:

- works in conjunction with the SAs to get physical access to the systems where dual control is required
- supervision of the SAs work at the operational system level where dual control is required and responsible for that the SAs are carrying out their role within the framework of their authority

- may have a degree of delegated security responsibility for the CA and RA services.

Registration Officer:
RA Office and Customer Service staff of the CA. Registration Officers in the Customers are not trusted persons. Typical duties of the Registration Officer include processing and approving certificate applications and submitting certificate requests to the CA system that issues and signs the certificates.

TeliaSonera has chosen to divide the responsibility for the above roles into sub-roles in order to increase security. These roles are described in the TeliaSonera Operational Documentation.

5.2.2 Number of persons required per task

TeliaSonera maintains a policy and rigorous control procedures to ensure segregation of duties based on job responsibilities. The most sensitive tasks, such as access to and management of CA and central RA cryptographic modules and associated key material, require multiple Trusted Persons.

These internal control procedures are designed to ensure that at a minimum, two trusted personnel are required to have either physical or logical access to the device. Access to CA and central RA cryptographic hardware is strictly enforced by multiple Trusted Persons throughout its lifecycle, from incoming receipt and inspection to final logical and/or physical destruction. Once a module is activated with operational keys, further access controls are invoked to maintain split control over both physical and logical access to the device. No persons have alone both physical access to cryptographic modules and hold activation data. Requirements for CA private key activation data is specified in section 6.2.2.

Physical and operational system access to the central CA and certain RA servers require the participation of at least 2 Trusted Persons that works in conjunction. Either person work physically together or the other Trusted Person is involved via following security controls:

- Each administrative login or physical access to critical servers or environments is causing alarm to be inspected by security supervisors.
- Each operation and command entered by operator is logged on the separate log server.
- All operational remote access to critical systems is done only via secure management hosts.
- Root/admin privilege of log and management hosts are guarded by persons who have no root access to CA servers. If maintenance to log/maintenance server is required the normal system operators may get temporary root access from the root guards.
- Critical files and directories are monitored by checksum tests so they are not modified during operational access. Security supervisors get alarm if modifications are done.
- Access controls and other security measures take care that no one person can alone install software that can access CA keys at least without being immediately detected. Either person can only install or person can only access CA keys or there are security supervisors monitoring the critical activity.

Other requirements in terms of the presence of people when carrying out other tasks involving the CA and RA operations are detailed in the TeliaSonera CA Operational Documentation.

The Trusted roles in section 5.2.1 are fulfilled by at least one person each. Those working in the role of SA or RO do not simultaneously work in any of the other roles involving the system.

5.2.3 Identification and authentication for each role

For all personnel chosen to become Trusted Persons, verification of identity is performed through the personal (physical) presence of such personnel before Trusted Persons performing TeliaSonera HR [or equivalent] or security functions and a check of well-recognized forms of identification (e.g., passports, driver licenses and other nationally accepted identification cards). Identity is further confirmed through the background checking procedures described in section 5.3.1.

TeliaSonera ensures that personnel have achieved Trusted Status and departmental approval has been given before such personnel are:

- included in the access list for the CA and RA sites;
- included in the access list for physical access to the CA and RA system;
- given a certificate for the performance of their CA or RA role; or
- given a user account on the CA or RA system.

Each of these certificates and accounts (with the exception of the CA signing certificates) is:

- personal and directly attributable to the Trusted Person;
- restricted to actions authorized for that role through the use of CA and RA software, operating system and procedural controls.

Identification of roles in the CA and RA systems takes place as follows:

Identification of SA roles takes place within the operating system in the CA and RA systems.

Identification of the CAA roles (where applicable) takes place within the CA system applications and is based on strong authentication using personal operator smart cards.

Identification of the RA roles takes place within the CA and RA system applications and it is based on strong authentication either using personal operator cards, software based keys and certificates or other two factor authentication mechanisms depending on the policy requirements of the applicable CA.

5.2.4 Roles requiring separation of duties

TeliaSonera maintains a policy and rigorous control procedures to ensure a separation of duties for critical CA and RA functions to prevent one person from maliciously using the CA or RA system without detection.

Complete documentation of all roles and what roles are allowed for a single person can be found from TeliaSonera CA Operational Documentation.

5.3 Personnel controls

5.3.1 Qualifications, experience, and clearance requirements

The Trusted roles according to section 5.2.1 are assigned only to specially selected and reliable persons who have proved their suitability for such a position. Same personnel controls apply to TeliaSonera personnel and to affiliate or partner company personnel if TeliaSonera is outsourcing any Trusted roles.

Trusted persons may not have other roles which may be deemed to be in opposition to the role assigned.

Personnel identified to become Trusted Persons must present proof of the requisite background, qualifications, and experience needed to perform their prospective job responsibilities competently and satisfactorily.

5.3.2 Background check procedures

Prior to commencement of employment in a Trusted Role, TeliaSonera conducts background checks. The actual background checks conducted depend on the local law and other circumstances. In Sweden the following background checks are conducted for persons in Trusted Roles:

- confirmation of previous employment,
- check of professional reference,
- search of criminal records (local, state or provincial, and national),
- check of credit/financial records,
- search of driver's license records

In Finland, the background checks include:

- confirmation of previous employment,
- check of professional reference,
- security clearance from the Finnish Police

Background checks are repeated periodically for personnel holding Trusted Positions, if permitted by the local laws. The factors revealed in a background check that may be considered grounds for rejecting candidates for Trusted Positions or for taking action against an existing Trusted Person generally include the following:

- Misrepresentations made by the candidate or Trusted Person,
- Highly unfavorable or unreliable personal references,
- Certain criminal convictions, and
- Indications of a lack of financial responsibility.

Reports containing such information are evaluated by human resources and security personnel, who determine the appropriate course of action in light of the type, magnitude, and frequency of the behavior uncovered by the background check. Such actions may include measures up to and including the cancellation of offers of employment made to candidates for Trusted Positions or the termination of existing Trusted Persons.

The use of information revealed in a background check to take such actions is subject to the applicable federal, state, and local laws.

5.3.3 Training requirements

TeliaSonera provides its personnel with courses and training needed for personnel to perform their job responsibilities competently and satisfactorily. TeliaSonera periodically reviews and enhances its training programs as necessary.

TeliaSonera's training programs are tailored to the individual's responsibilities and include the following as relevant:

- Basic PKI concepts,
- Job responsibilities,
- TeliaSonera security and operational policies and procedures,
- Use and operation of deployed hardware and software,
- Incident and Compromise reporting and handling.

5.3.4 Retraining frequency and requirements

TeliaSonera provides refresher training and updates to its personnel to the extent and frequency required to ensure that such personnel maintain the required level of proficiency to perform their job responsibilities competently and satisfactorily.

5.3.5 Job rotation frequency and sequence

No stipulation.

5.3.6 Sanctions for unauthorized actions

All employees and external resources working for TeliaSonera are informed about their obligation to report details immediately to superior, Group Security, Corporate Internal Audit on suspected security events, criminal activity or fraud acts. Appropriate disciplinary actions are taken for unauthorized actions or other violations of TeliaSonera policies and procedures. Disciplinary actions may include warning, role change or termination of employment and are dependent on the frequency and severity of the unauthorized actions.

5.3.7 Independent contractor requirements

In limited circumstances, independent contractors or consultants may be used to fill Trusted Positions. Any such contractor or consultant is held to the same functional and security criteria that apply to a TeliaSonera employees in a comparable position.

Independent contractors and consultants who have not completed the background check procedures specified in section 5.3.2 are permitted access to TeliaSonera's secure facilities only to the extent that they are escorted and directly supervised by Trusted Persons.

5.3.8 Documentation supplied to personnel

TeliaSonera personnel involved in the operation of TeliaSonera CA Services will be made aware of the requirements of applicable Certificate Policies, Certification Practice Statements and any other specific policies, procedures, documents, and/or contracts needed to perform their job responsibilities competently and satisfactorily

5.4 Audit logging procedures

5.4.1 Types of events recorded

TeliaSonera manually or automatically logs at least the following significant events relating to the CA and RA systems:

- CA and system keys life cycle management events, including:
  - Key generation, backup, storage, recovery, archival, and destruction
  - Cryptographic device life cycle management events.
- CA, RA, Subscriber and system certificate life cycle management events, including:
  - Certificate Applications, renewal and rekey
  - Certificate revocation, suspension and re-instatement
  - Successful or unsuccessful processing of requests
  - Generation and issuance of Certificates and CRLs.
- Security-related events including:
  - Creation of system user accounts
  - Initiation of operations at operating system level by system users with details of who requested the operation, the type of operation and indication of the initiation results
  - Security system actions performed by TeliaSonera personnel
  - System crashes, hardware failures and other anomalies
  - Firewall, router and intrusion detection system activity
- CA and RA system events including:
  - Software installation and updates
  - Relevant information on backups
  - Booting up and shutting down the system
  - Time and date of all hardware upgrades
  - Time and date of backups and emptying of logs
  - Time and date of backups and emptying of archive data (in accordance with section 5.5.1)

Log entries include at least the following elements:

- Date and time of the entry
- Identity of the entity making the journal entry
- Kind of entry.

TeliaSonera RAs log Certificate Application information including:

- Kind of identification document(s) presented by the Certificate Applicant
- Storage location of copies of applications and identification documents
- Identity of entity accepting the application
- Method used to validate organization and individual identity and authority

The following information concerning revocation requests is recorded at the TeliaSonera's 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.

In the case where the CA is a Customer's CA or the registration or revocation functions are performed by Registration Officer in a Customer, the information above may not be logged by the RAs.

5.4.2 Frequency of processing log

In the CA system the audit logs are reviewed at least monthly to check for any unauthorised activity.

Audit log reviews include a verification that the log has not been tampered with, a brief inspection of all log entries, and a more thorough investigation of any alerts or irregularities in the logs. Actions taken based on audit log reviews are also documented.

In the RA systems the audit logs are automatically and continously analysed or logs are reviewed monthly to check for any unauthorized activity. The audit logs are also manually reviewed to search for any alerts or irregularities that for any reason have been missed by the automatic reviews. If such an irregularity is found the application for the automatic reviews will be updated to handle future irregularities of that type.

TeliaSonera also reviews its audit logs for suspicious or unusual activity in response to alerts generated based on irregularities and incidents within TeliaSonera CA and RA systems.

5.4.3 Retention period for audit log

Audit logs in accordance with section 5.4.1 are retained onsite at least two months after processing and thereafter archived for at least ten years after the last Subscriber certificate has expired.

5.4.4 Protection of audit log

Logs are protected against improper alteration through the logical protection mechanism of the operating system and through the system itself not being physically or logically accessible other than by authorized personnel.

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

5.4.5 Audit log backup procedures

Back-up copies of the system audit logs are made regularly according to defined schedules. Copies of the audit log and summaries of the inspection of audit logs are stored in physically secure locations in two physically separate places.

The logs are stored in such a way that they can, in the event of serious suspicion of irregularities, be produced and made legible for auditing during the stated storage time.

5.4.6 Audit collection system (internal vs. external)

Automated audit data is generated and recorded at the application, network and operating system level.

Manually generated audit data is recorded by TeliaSonera personnel.

5.4.7 Notification to event-causing subject

Where an event is logged by the audit collection system, no notice is required to be given to the individual, organization, device, or application that caused the event.

5.4.8 Vulnerability assessments

The CA assesses the vulnerability of its critical systems regularly. 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.

5.5 Records archival

TeliaSonera archives relevant materials which affect the operation of the CA service. Procedures and prerequisites for this archiving are detailed in the following subsection.

5.5.1 Types of records archived

The following information is archived on an ongoing basis:

a. Transactions containing signed requests for certificate production and revocation of certificates from authorized operators.
b. Certificate application documentation signed by applicant commissioners and by persons responsible for receiving and accepting applications.
c. Signed receipt confirmations when issuing keys and codes.
d. Issued certificates and related catalogue updates.
e. History of previous CA keys, key identifiers and cross certificates between different CA key generations.
f. Revocation, suspension and re-instatement requests and related information received by the revocation service.
g. CRL creation times and CRL catalogue updates.
h. Results of reviewing TeliaSonera compliance with this CPS and other audits.
i. Applicable terms and conditions and contracts (in all versions applied).
j. All CP and CPS versions published by the CA.

In those cases where the archived information constitutes a digitally signed volume of information, the necessary information required for verifying the signature during the stated archiving time is also archived.

5.5.2 Retention period for archive

All archived information in accordance with section 5.5.1 is stored for at least fifteen years from the day of occurance or issuance.

5.5.3 Protection of archive

The archives are stored in locations other than the CA and RA sites. The archives are stored under such conditions that the archived material is protected from unauthorized viewing, modification or deletion by physical protection and in some cases combined with cryptographic protection.

Archived material which is classified as confidential in accordance with section 9.3 is not accessible to external parties in its entirety other than as required by law and court orders.

Individual pieces of information relating to a specific key holder or transaction may be released after individual investigations.

The archive is stored under such conditions that it remains legible for auditing during the stated storage time.

However, the parties are made aware that technology for storing archived material may be changed and, in such an event, the CA is not obliged to retain functioning equipment for interpreting old archived material if this is more than five years old. In such an event, the CA is however instead obliged to be prepared to set up the necessary equipment on payment of a charge corresponding to the costs of TeliaSonera.

In the event that changes in procedures for access to archived material have been caused by TeliaSonera ceasing its operations, information on procedures for continued access to archived material shall be supplied by TeliaSonera through the notification procedures in accordance with section 5.8.

5.5.4 Archive backup procedures

Information to be archived is collected from the places of origin at defined intervals and transferred to the archives.

No further backups are made of the archived information except for normal backups of the data in the systems at the CA and RA sites that are done for recovery purposes. Backups are taken to off-site location or copies of the backups are brought outside the CA and RA sites at defined intervals and stored at locations separated from the CA and RA sites.

5.5.5 Requirements for time-stamping of records

All documents archived pursuant to this section will be marked with the date of their creation or execution.

The date and time information in the CA system and certain other system logs is synchronized with an external UTC time source.

5.5.6 Archive collection system (internal or external)

No stipulation.

5.5.7 Procedures to obtain and verify archive information

TeliaSonera will verify the integrity of the backups at least once every 12 months to ensure usability of these backups. Material stored off-site will be periodically verified for data integrity.

5.6 Key changeover

TeliaSonera CA key pairs are retired from service at the end of their respective maximum lifetimes as defined in section 6.3.2. CA certificates may be renewed as long as the cumulative certified lifetime of the CA key pair does not exceed the maximum CA key pair lifetime. New CA key pairs will be generated as necessary, for example to replace CA key pairs that are being retired, to supplement existing, active key pairs and to support new services in accordance with section 6.1.

A new set of CA key pairs is created at least three months before the point when the existing CA keys ceases to be used for issuing of new certificates.

5.6.1 Self-Signed CA

Changing of CA keys for a self-signed CA will be done, for example, using the following procedure:

a. a new CA key pair is created,
b. a new self-signed certificate is issued for the new public CA key,
c. a cross certificate is issued where the old public CA key is signed using the new private CA key,
d. a cross certificate is issued where the new public CA key is signed using the old private CA key, and
e. the certificates in accordance with b) to d) is published in the relevant directory.
f. new Subscriber certificates are signed with the new private CA key.
g. the old CA private key is used to issue CRLs until the expiration date of the last certificate issued using the old key pair has been reached.

5.6.2 CA Hierarchies

Changing of CA key pairs for a subordinate CA will be done, for example, using the following procedures:

a. a new subordinate CA key pair is created
b. a new subordinate CA certificate is issued for the new public CA key by the superior CA on the next level of the hierarchy,
c. the certificate in accordance with b) is published in the relevant directory.
d. new subordinate CA certificates or Subscriber certificates issued by the new subordinate CA are signed with the new private subordinate CA key.
e. the old subordinate CA private key is used to issue CRLs until the expiration date of the last certificate issued using the old key pair has been reached.

A superior CA ceases to issue new subordinate CA certificates no later than three months before the point in time where the remaining lifetime of the superior CA key pair equals the approved certificate Validity Period for the specific type of certificates issued by subordinate CAs in the superior CA's hierarchy.

5.7 Compromise and disaster recovery

TeliaSonera has implemented a robust combination of physical, logical, and procedural controls to minimize the risk and potential impact of a key compromise or disaster. TeliaSonera has implemented disaster recovery procedures and key compromise response procedures described in this CPS. TeliaSonera's compromise and disaster recovery procedures have been developed to minimize the potential impact of such an occurrence and restore TeliaSonera's operations within a commercially reasonable period of time.

5.7.1 Incident and compromise handling procedures

TeliaSonera has implemented detailed change and incident management procedures to allow for controlled and accountable handling of incidents and recovery from system and application disasters. Regarding disaster recovery at the site level TeliaSonera has implemented disaster recovery plans.

Detailed instructions are provided in the TeliaSonera Operation Procedures with a Disaster Recovery Plan outlining the steps to be taken in the event of an incident and the incident reporting caused by such an incident.

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

In the event of the corruption of computing resources, software, and/or data, such an occurrence is reported to TeliaSonera Security staff and TeliaSonera's incident handling procedures are initiated. Such procedures require appropriate escalation, incident investigation, and incident response. If necessary, TeliaSonera's key compromise or disaster recovery procedures will be initiated.

5.7.3 Entity private key compromise procedures

Upon the suspected or known compromise of a TeliaSonera CA private key, Customer CA private key or the TeliaSonera infrastructure, TeliaSonera's Key Compromise Response procedures are followed. Detailed instructions are provided in the TeliaSonera Operation Procedures.

TeliaSonera undertakes, on suspicion that TeliaSonera no longer has full and exclusive control of a CA's private key, to take the following action:

a. Revoke the CA certificate associated to the compromised CA private key if the CA is a part of a CA hierarchy and make the updated ARL (ARL is CRL for CA certificates) publicly available.
b. Cease all revocation checking services relating to certificates issued using the compromised key and all revocation checking services signed using the comprised key or keys certified using the compromised key. This means that all associated revocation lists are removed from their assigned locations.
c. Inform all key holders and all parties with which TeliaSonera has a relationship that the CA's private key has been compromised and how new CA certificates can be obtained.
d. In the event that TeliaSonera has cross certified the compromised CA key with another operational CA key, revoke any such cross certificates.

Subscriber key holders will be informed that they should immediately cease using private keys which are associated with certificates issued using the compromised CA's private key.
Key holders are furthermore informed how they should proceed in order to obtain replacement certificates and any new private keys, and the circumstances under which old private keys can be used in connection with other certificates which have not been issued using the compromised CA key.

Information will be made available to relying parties, who are clearly informed that the use of the affected certificates and the CA's issuer certificate has been revoked.

The action of relying parties is outside TeliaSonera's influence. Through TeliaSonera's revocation information process, they will receive the necessary information to be able to take the correct action.

5.7.4 Business continuity capabilities after a disaster

TeliaSonera will provide business continuity procedures in a Disaster Recovery Plan that outline the steps to be taken in the event of corruption or loss of computing resources, software and/or data.

TeliaSonera has implemented mission critical components of its CA infrastructure in redundant configurations. This applies both to hardware and software components. The main CA system components have been implemented in two data centers located in different cities.

TeliaSonera maintains offsite backup of important CA information for CAs issued at the TeliaSonera's premises. Such information includes, but is not limited to: Backups of CA key pairs, application logs, certificate application data, audit data and database records for all certificates issued. In addition, CA private keys are backed up and maintained for disaster recovery purposes.

5.8 CA or RA termination

In the event that it is necessary for a TeliaSonera CA or a Customers CA to cease operation, TeliaSonera makes a commercially reasonable effort to notify Subscribers, Relying Parties, and other affected entities of such termination in advance of the CA termination. Where CA termination is required, TeliaSonera and, in the case of a Customer CA, the applicable Customer, will develop a termination plan to minimize disruption to Customers, Subscribers, and Relying Parties. Such termination plans may address the following, as applicable:

a. Provision of notice to parties affected by the termination, such as Subscribers, Relying Parties, and Customers, informing them of the status of the CA.
b. In case that the CA is publicly used, make public announcement at least three months in advance that operations will cease for the CA.
c. Cease all revocation checking services relating to certificates issued using the CA keys of which use will cease. This means that all associated revocation lists are removed from their assigned locations and that no new revocation lists are issued to replace those that are removed.
d. Terminate all rights for subcontractors to act in the name of the CA which will cease to operate.
e. Ensure that all archives and logs are stored for the stated storage time and in accordance with stated instructions.

6 TECHNICAL SECURITY CONTROLS

6.1 Key pair generation and installation

6.1.1 Key pair generation

6.1.1.1 Specific requirements for the CA's issuer keys

The CA's issuer keys are generated in hardware modules which are dedicated to storing and processing such keys. When generating issuer keys, a number of people's presence is required. The hardware modules are physically protected as per section 5.1 which, among other things, means that physical access to these requires the simultaneous presence of at least two authorized operators.

Some CA keys are stored in offline state (e.g. "TeliaSonera Root CA v1"). They are activated only when needed. Two privileged CA Officers are required to temporarily activate an offline key.

6.1.1.2 Specific requirements for private Subscriber keys

Subscriber key pairs are typically generated by the Subscriber. Unless stated otherwise in CPS referring to this CPS, private Subscriber keys are generated in accordance to this section.

Where private keys are stored on smart cards or equivalent chip based hardware, key generation is normally carried out by onboard key generation or generated outside the chip and loaded with a secure vendor specific method.

In those cases where the Subscriber keys are created by CA, these are generated in a strongly protected server and stored in a suitable format, then erased from the server's primary memory.

6.1.2 Private Key delivery to Subscriber

Private key delivery process is described in each CPS referring to this CPS.

6.1.3 Public key delivery to certificate issuer

Subscribers and RAs submit their public key to TeliaSonera for certification electronically through the use of a PKCS#10 Certificate Signing Request (CSR), Certificate Request Syntax (CRS) or other digitally signed package in a session secured by Secure Sockets Layer (SSL). Where CA, RA, or end-user Subscriber key pairs are generated by TeliaSonera, this requirement is not applicable.

6.1.4 CA public key delivery to relying parties

TeliaSonera makes the CA certificates for TeliaSonera CAs and for Customer CAs, if the Customers so agrees, available to Subscribers and Relying Parties through the TeliaSonera CA Service repository https://repository.trust.teliasonera.com or through the TeliaSonera CA Service LDAP directory at ldap://crl-1.trust.teliasonera.com.

Certain TeliaSonera root CA certificates are delivered to Subscribers and Relying Parties through the web browser software.

TeliaSonera generally provides the full certificate chain (including the issuing CA and any CAs in the chain) to the end-user Subscriber upon Certificate issuance.

6.1.5 Key sizes

The CAs' issuer keys are generated as RSA keys with a minimum length of 2048 bits.

The Subscribers' and operators' RSA keys are generated with a minimum length of 1024 bits. In most cases minimum length for Subscriber and operator RSA keys is 2048 bits.

6.1.6 Public key parameters generation and quality checking

All CA Signature keys will be generated using a random or pseudo-random process as described in ISO 9564-1 and ISO 11568-5 that are capable of satisfying the statistical tests of FIPS PUB 140-2, level 3. CA keys are protected by a secure cryptographic hardware module rated at least FIPS 140-2, Level 3.

Key pairs for all other Subscribers will be generated and stored in software or by secure cryptographic a hardware module (e.g. Smart cards) at the discretion of the issuing CA.

6.1.7 Key usage purposes (as per X.509 v3 key usage field)

Issued certificates contain information which defines suitable areas of application for the certificate and its associated keys. Area of application labeling takes place in accordance with X.509 and chapter 7.

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

a. Signing of Subscriber certificates and OCSP response certificates (keyCertSign (5))
b. Signing of CRLs (cRLSign (6))

Subscriber certificates issued according to this CPS may include the following areas of application:

a. Identification and authentication (Key Usage Digital Signature (0))
b. Encryption (Key Usage Key Encipherment (2) and/or Key Agreement (4) and/or Data Encipherment (3))
c. Verification of digital signatures in connection with non-repudiation services (Key Usage Non-Repudiation (1))

Alternatives a) and b) usually applies to a single certificate which is called Confidentiality certificate in this document.

Alternative c) applies to certificate called Digital Signature certificate in this document. It may be combined with a) and b) if user has only one certificate for all key usage purposes.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

TeliaSonera has implemented a combination of physical, logical, and procedural controls to ensure the security of TeliaSonera and Customers CA private keys. Logical and procedural controls are described here in section 6.2. Physical access controls are described in section 5.1.2. Subscribers are required by contract to take necessary precautions to prevent the loss, disclosure, modification, or unauthorized use of private keys.

The Subscriber is required to protect its private key from disclosure according to the requirements as defined by the issuing CA. The Subscriber is responsible for its private keys.

6.2.1 Cryptographic module standards and controls

All CA Digital Signature key generation, CA Digital Signature key storage and certificate signing operations will be performed in a hardware cryptographic module rated to at least FIPS 140-2 Level 3. The cryptographic module is physically protected in a separate safe which is stored within the protected environment defined in section 5.1.

All other CA cryptographic operations, such as certificates and keys used for administering the CA, will be performed in a cryptographic module in smart cards.

End entities private keys can be enclosed and protected in two different ways:

a. Hardware protected private keys which are created and stored in smart cards or equivalent chip based hardware. In some hardware cases keys in smart cards are generated outside the smart card but pre-installed by a smart card factory with vendor specific methods.
b. Software protected private keys generated by the CA or by the Subscriber.

Software protected keys shall be stored in encrypted form with a security level which makes it unfeasible to crack the encryption protection through logical attacks. For this reason, key holders shall use methods and tools approved by the CA. However, for locally-generated software-protected keys, it is the key holder (and the key holder's organization) who takes sole responsibility for satisfactory security being achieved in the user's local environment.

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

TeliaSonera has implemented technical and procedural mechanisms that require the participation of multiple trusted individuals to perform sensitive CA cryptographic operations.

TeliaSonera uses "Secret Sharing" to split the activation and recovery data needed to make use of a CA private key into separate parts called "Secret Shares". A threshold number of Secret Shares (n) out of the total number of Secret Shares created and distributed for a particular hardware cryptographic module (m) is required to activate or recover a CA private key stored on the cryptographic module.

6.2.3 Private Key escrow

TeliaSonera does not escrow private keys.

6.2.4 Private Key backup

TeliaSonera creates backup copies of CA's private keys for routine recovery and disaster recovery purposes. Backups are dealt with in accordance with the same access protection rules which apply to the original keys. At least two privileged CA Officers are required to manage CA private key backups.

Backups may be made of the Subscribers' or RA's private confidentially keys. The keys are then copied and stored in encrypted form and protected at a level no lower than stipulated for the primary version of the keys.

Offline CA keys are stored as offline key backups. When an offline CA key is activated it is temporarily restored to the online CA system and then removed from the online CA system again.

6.2.5 Private Key archival

No Subscriber, RA or CA private keys will be archived by TeliaSonera.

6.2.6 Private Key transfer into or from a cryptographic module

TeliaSonera generates CA key pairs on the hardware cryptographic modules in which the keys will be used. Where CA key pairs are transferred to another hardware cryptographic module for clustering reasons such key pairs are transported between modules in encrypted form using private networks dedicated for TeliaSonera CA.

In addition, TeliaSonera makes encrypted copies of CA key pairs for routine recovery and disaster recovery purposes.

6.2.7 Private Key storage on cryptographic module

CA private digital signature key storage is kept in a secure cryptographic hardware module rated to at least FIPS 140-2 Level 3.

Subscriber keys protected by smart cards will be generated and stored locally in the smart card and will never be exposed outside the smart card.

6.2.8 Method of activating private key

The activation of the private key of the CA is included in the procedure described in paragraph 6.1.1. At least one person serving in a trusted role of the CA and authenticated with a two factor authentication method is required for the re-activation. The key remains active in the CA system for a single process until it is deactivated.

Essential information exchange between a RA and the CA is encrypted. All CA and RA operators are authenticated in CA or RA system in accordance with section 5.2.3 and transactions affecting the use of a CA's private issuer keys are authenticated by the CA system based on a digital signature. Activation of the private key of the TeliaSonera RA requires the use of activation data as described in section 6.4.

TeliaSonera strongly recommends that Subscribers and Registration Officers in Customers store their private keys in encrypted form and protect their private keys through the use of a hardware token and/or strong passphrase. The use of two factor authentication mechanisms (e.g., token and passphrase or biometric and token) is encouraged.

6.2.9 Method of deactivating private key

The CA private issuer key is deactivated, for example, by closing the application using it, restarting or removing the cryptographic module.

6.2.10 Method of destroying private key

For operational keys which are stored on the issuer system's hard disk or other media in encrypted form, the following applies:

a. If the equipment is to be used further in the same protected environment, erasing is carried out in such a way that these keys cannot be recovered atleast without physical access to the media. Old or broken CA key storage media may be temporarily stored in the protected CA environment.

b. If the media that has contained CA key material will permanently leave the protected CA environment, it will be destroyed. Reliable de-magnetizer or physical destruction is used when destroying the media.

The Subscriber private confidentiality keys that are stored by the CA for backup purposes are securely destroyed at the end of service. Customer is responsible to destroy or otherwise prevent misusage of expired or deserted subscriber private keys in their possession.

6.2.11 Cryptographic Module Rating

All CA digital signature key generation, CA digital signature key storage and certificate signing operations are performed in a secure cryptographic hardware module rated to at least FIPS 140-2 Level 3.

6.3 Other aspects of key pair management

No private keys or other confidential information within the CA may leave its prescribed protected environment. When servicing and in other similar situations where the prescribed protection methods cannot be maintained, all storage media containing sensitive information or sensitive private issuer keys are removed or destroyed. Encrypted keys may temporarily transfer outside the protected environments for backup and clustering purposes like described in 6.2.6.

6.3.1 Public key archival

TeliaSonera retain archives of all verification public keys for the period of at least ten years after the expiration of the last Subscriber certificate that has been issued by the CA.

6.3.2 Certificate operational periods and key pair usage periods

Private Root CA keys are used for a maximum of twenty five (25) years in order to issue subordinate CA certificates.

Private CA keys are used for a maximum of twenty five (25) years in order to issue Subscriber certificates and revocation lists. CA certificates are given a maximum validity period to cover the time from generation up to and including the point when associated private keys cease to be used for signing of Subscriber certificates and revocation lists.

Cross certificates between different generations of CA keys are given a maximum validity period of five years plus an overlap time of maximum six months (the time before changing the key when the new key and the cross certificate for the old key are available for updating).

Subscriber certificates issued in accordance with this CPS are issued both for new keys and for existing keys which have been certified previously in connection with the keys being generated on smart cards.

Subscriber certificates are given a maximum period of validity of five years.

Subscriber certificates for existing keys on smart cards are given a maximum period of validity which is equal to the expiry date of the original certificate, but no more than five years. Certificates used by TeliaSonera staff for operating the CA and RA systems and internal system certificates are given a maximum validity period of five years.

6.4 Activation data

6.4.1 Activation data generation and installation

Activation data (Secret Shares) used to protect TeliaSonera CA and Customers CA private keys is generated in accordance with the requirements of section 6.2.2.

TeliaSonera CA and RA operators are either using smart cards with the private keys protected by PINs or have the private keys stored on a hard disk. If the keys are stored on a hard disk the CA and RA operators are required to select strong passwords to protect the private keys.

TeliaSonera's password selection guidelines require that passwords:

- be generated by the user;
- have at least eight characters;
- have at least one alphabetic and one numeric character;

- have at least one lower-case letter;
- not contain many occurrences of the same character;
- not be the same as the operator's profile name; and
- not contain a long substring of the user's profile name.

TeliaSonera strongly recommends that Subscribers and Registration Officers in Customers choose passwords that meet the same requirements. TeliaSonera also recommends the use of two factor authentication mechanisms (e.g., token and pass phrase or biometric and token) for private key activation.

6.4.2 Activation data protection

All activation data will be protected from unauthorized use by a combination of cryptographic and physical access control mechanisms.

Activation data (Secret Shares) used to protect TeliaSonera CA and Customers CA private keys is stored in secure locations where at least two trusted individuals are required to access them.TeliaSonera CA and RA operators are required to store their Administrator private keys on smart cards or in encrypted form using password protection and their browser's "high security" option. TeliaSonera CA and RA operators are required and Subscribers and Registration Officers in Customers are strongly recommended to protect the activation data for their private keys against loss, disclosure, modification, or unauthorized use.

6.4.3 Other aspects of activation data

No stipulation.

6.5 Computer security controls

6.5.1 Specific computer security technical requirements

The entire CA system is built in such a way that individual roles as per section 5.2 can be separated.

The access control systems used is built in such a way that every operator is identified at an individual level and authenticated in accordance with the section 5.2.3.

The above shall apply regardless of whether an operator acts directly within the CAs central premises or whether the operator is in an external RA function.

6.5.2 Computer security rating

The CA software used by TeliaSonera is Common Criteria EAL4+ certified.

6.6 Life cycle technical controls

6.6.1 System development controls

Two-phase testing is used in the development of the CA and RA production systems. 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 similar to the production system. The 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.

6.6.2 Security management controls

The CA follows the policies defined by TeliaSonera'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 8.

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.

Operational documentation has been drawn up which documents in detail how roles and authorization are applied and maintained.

6.6.3 Life cycle security controls

No stipulation.

6.7 Network security controls

Firewalls have been implemented which strictly limit all types of information exchange which have been defined as forbidden. Only the type of information exchange which is strictly necessary for the CA service is permitted.

Essential information exchange between the RA and the CA is encrypted and transactions affecting the use of the CA's private issuer keys are individually signed. All communication ports in the CA system which are not needed are deactivated and associated software routines which are not used are blocked.

6.8 Time-stamping

No stipulation.

7 CERTIFICATE, CRL, AND OCSP PROFILES

7.1 Certificate profile

All stipulations regarding Certificate profile, except for section 7.1.1 Version number(s), will be specified in each CPS referring to this Production CPS.

7.1.1 Version number(s)

All issued subscriber certificates are X.509 Version 3 certificates, in accordance with the PKIX Certificate and CRL Profile. CA administration certificates may be X.509 Version 1 certificates.

7.2 CRL profile

All stipulations regarding CRL profile, except for section 7.2.1 Version number(s), will be specified in each CPS referring to this Production CPS.

7.2.1 Version number(s)

All issued CRLs are X.509 version 2 CRLs in accordance with the RFC 5280 “Internet X.509 Public Key Infrastructure Certificate and CRL Profile” dated May 2008.

7.3 OCSP profile

All stipulations regarding OCSP profile, except for section 7.3.1 Version number(s), will be specified in each CPS referring to this Production CPS.

7.3.1 Version number(s)

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

8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS

8.1 Frequency or circumstances of assessment

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

8.2 Identity/qualifications of assessor

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

8.3 Assessor's relationship to assessed entity

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

8.4 Topics covered by assessment

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

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

b. CA environmental controls.

8.5 Actions taken as a result of deficiency

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

a) The Compliance Auditor may note the deficiency as part of the report;

b) The Compliance Auditor may meet with TeliaSonera and determine if the deficiency can be remedied and an action plan should be developed and steps taken to remedy the deficiency. Such steps could be to change applied procedures and/or updating this CPS;

c) The Compliance Auditor may report the deficiency and if the TeliaSonera CA Service deems the deficiency to have risk to the operation of the TeliaSonera or Customers CAs, the TeliaSonera CA Service operator may revoke the CA's certificate.

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

8.6 Communication of results

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

9 OTHER BUSINESS AND LEGAL MATTERS

9.1 Fees

Fees are defined in applicable Customer agreement unless otherwise specified in a CPS referring to this Production CPS.

9.2 Financial responsibility

9.2.1 Insurance coverage

TeliaSonera and all CAs residing in the TeliaSonera production environment will maintain adequate levels of insurance necessary to support its business practices.

9.2.2 Other assets

No stipulation.

9.2.3 Insurance or warranty coverage for end-entities

No stipulation.

9.3 Confidentiality of business information

9.3.1 Scope of confidential information

Information which is not excluded in section 9.3.2 is treated as confidential by the CA in relation to the Customer and/or keyholder and will not be disclosed without the consent of the Customer and/or key holder.

TeliaSonera will disclose confidential information where this is required by law or by a decision of a court or public authority. Private keys linked to issued certificates cannot be disclosed when these are not stored by TeliaSonera.

9.3.2 Information not within the scope of confidential information

The following information is not deemed to be confidential in the relation between the CA and the Customer and/or keyholder:

a) This CPS and each CPS referring to this Production CPS
b) Information in issued certificates including public keys (but not private keys)
c) Revocation lists and OCSP responses
d) General key holder terms and conditions

Exceptions may apply to key holder information if this is stated in a specific agreement with the key holder's organisation.

9.3.3 Responsibility to protect confidential information

All confidential information will be physically and/or logically protected by CA from unauthorized viewing, modification or deletion.

Storage media used by the CA system is protected from environmental threats such as temperature, humidity and magnetism and that also applies to backup and archive media.

Confidentiality keys will in some cases be backed up by TeliaSonera, and in those cases the keys will be protected in accordance with Section 6, and will not be disclosed without prior consent of the Subscriber or a duly authorized representative of the issuing CA.

9.4 Privacy of personal information

TeliaSonera processes personal data in accordance with applicable national legislation (Swedish or Finnish) and any agreement with Customer and/or keyholder.

9.5 Intellectual property rights

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

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

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

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

9.6 Representations and warranties

9.6.1 CA representations and warranties

TeliaSonera will operate in accordance with this CPS and each CPS referring to this Production CPS, when issuing and managing certificates provided to CAs, RAs, sub-CAs and Subscribers. TeliaSonera will require that all the RAs operating on its behalf will comply with the relevant provisions of this CPS and applicable CPS referring to this Production CPS concerning the operations of the RAs. TeliaSonera will take commercially reasonable measures to make Subscribers and Relying Parties aware of their respective rights and obligations with respect to the operation and management of any keys, certificates or End-Entity hardware and software used in connection with the PKI. Subscribers will be notified as to procedures for dealing with suspected key compromise and service cancellation.

When a CA publishes or delivers a certificate, it declares that it has issued a certificate to a Subscriber and that the information stated in the certificate was verified in accordance with the applicable CPS.

CA personnel associated with PKI roles will be individually accountable for actions they perform. "Individually accountable" means that there shall be evidence that attributes an action to the person performing the action.

All CA personnel are authenticated when performing any actions in the CA applications. The audit logs are the main tool to control any misuse of the CA personnel's authorities. For the processes authenticating the CA personnel see section 5 of this CPS.

9.6.2 RA representations and warranties

The CA bears overall responsibility for the issued certificates. Registration responsibilities of the CA's overall responsibility can, however, be transferred through an agreement between the CA and a Relying Party, to the Relying Party, when the last-mentioned party acts also as Registration Authority. A Customer can, through an agreement, take responsibility for a separately defined part of the CA's responsibilities related to registration.

TeliaSonera will require that all Registration Officers comply with all the relevant provisions of this CPS and applicable CPS referring to this Production CPS. TeliaSonera will make available registration policies and Customer responsibility descriptions to Customers acting as RA and will require them to comply with the registration policies and Customer responsibility descriptions through a certification service agreement. The registration policies and Customer responsibility descriptions contain all relevant information pertaining the rights and obligations of the Registration Officers, Subscribers and Relying Parties.

The Registration Officer is responsible for the identification and authentication of Subscribers following section 3.1 and section 4.1. of the applicable CPS referring to this Production CPS. The Registration Officer is also responsible for revoking certificates in accordance with the CPS.

Registration Officers are individually accountable for actions performed on behalf of a CA. Individually accountability means that there must be evidence that attributes an action to the person performing the action (audit logs). Records of all actions carried out in performance of RA duties shall identify the individual who performed the particular duty. When an RA submits Subscriber information to a CA, it

will certify to that CA that it has authenticated the identity of that Subscriber and that the Subscriber is authorized to submit a certificate request in accordance with the CPS.

Submission of the certificate request to the CA will be performed in a secure manner as described in the applicable CPS.

All Registration Officers are authenticated when performing any actions in the RA applications. The audit logs are the main tool to control any misuse of the RA personnel's authorities. For the processes authenticating the RA personnel see section 5 of this CPS.

9.6.3 Subscriber representations and warranties

TeliaSonera will require that Subscribers comply with all the relevant provisions of this CPS and applicable CPS referring to this Production CPS. Subscribers are required to protect their private keys, associated pass phrase(s) and tokens, as applicable, and to take all reasonable measures to prevent their loss, disclosure, modification, or unauthorized use.

Any Subscriber information shall be complete, validated and accurate with full disclosure of all required information in connection with a certificate or a query to a CA.

The Subscriber shall only use the keys and certificates for the purposes identified in applicable CPS and in any applicable agreement(s).

When a Subscriber suspects a private key compromise, the Subscriber shall notify the issuing Certification Authority in the manner specified in applicable CPS. When any other entity suspects private key compromise, they should notify the issuing CA.

TeliaSonera is not a trustee, agent, fiduciary, or other representative of the Subscriber and the relationship between TeliaSonera and the Subscriber is not that of an agent and a principal. TeliaSonera makes no representation to the contrary, either implicitly, explicitly, by appearance or otherwise. The Subscriber does not have any authority to bind TeliaSonera by contract, agreement or otherwise, to any obligation.

9.6.4 Relying party representations and warranties

TeliaSonera will require that Relying Parties comply with all the relevant provisions of this CPS and applicable CPS referring to this Production CPS.

Prior to accepting a Subscriber's certificate, a relying party is responsible to:

a) Verify that the certificate is appropriate for the intended use;
b) Check the validity of the certificate, i.e. verify the validity dates and the validity of the certificate and issuance signatures; and
c) Check the status of the certificate against the appropriate and current CRL or OCSP Responder in accordance with the requirements stated in this CPS. As part of this verification process the digital signature of the CRL or OCSP Responder should also be validated. If certificate status can't be received due to system failure or similar, the certificates shall not be accepted.

It is also up to the relying party to study this CPS and applicable CPS referring to this Production CPS to decide whether the security level of the issuance process is appropriate for the actual application where to be used.

TeliaSonera will provide certificate status information identifying the access point to the CRL or on-line certificate status server in every certificate TeliaSonera issues in accordance with the CPS referring to this Production CPS.

9.6.5 Representations and warranties of other participants

No stipulation.

9.7 Disclaimers of warranties

TeliaSonera assumes no liability except as stated in the relevant Customer contracts pertaining to certificate issuance and management.

9.8 Limitations of liability

TeliaSonera assumes no liability except as stated in the relevant Customer contracts pertaining to certificate issuance and management.

9.9 Indemnities

If a claim for damages will be presented against the CA based on the matters listed below, the Customer 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. The Customer shall compensate the CA for any damage caused by:

- 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 section 9.6.3.
- the Customer's failure as a Relying Party to verify the validity of the certificate according to section 9.6.4,
- the Customer's otherwise non-justified trust on the certificate as Relying Party, in consideration of the circumstances.

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

9.10 Term and termination

9.10.1 Term

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

9.10.2 Termination

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

9.10.3 Effect of termination and survival

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

9.11 Individual notices and communications with participants

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

9.12 Amendments

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

9.12.1 Procedure for amendment

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

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

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

TeliaSonera CA Policy Management Team decides which measures are taken in relation to the comments received. If comments received necessitate changes to the original change proposal which

were not covered by the original notification, these changes may come into force no earlier than 15 days after publication of a new modified notification.

9.12.2 Notification mechanism and period

See 9.12.1

9.12.3 Circumstances under which OID must be changed

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

9.13 Dispute resolution provisions

If a dispute relating to this CPS or CPS referring to this CPS is not successfully resolved by negotiations, it shall be settled by arbitration in accordance with the Reconciliation and Arbitration Rules of the International Chamber of Commerce (ICC). The Stockholm or Helsinki Chamber of Commerce shall administer the reconciliation in accordance with the ICC's rules, and the venue for arbitration shall be Stockholm or Helsinki. The proceedings shall be held in Swedish or Finnish unless the parties agree to hold them in English.

9.14 Governing law

Swedish or Finnish law shall apply to the interpretation of this CPS or CPS referring to this CPS depending where the related Customer agreement has been made, if not otherwise agreed.

9.15 Compliance with applicable law

TeliaSonera will, in relation to the CA Service, comply with applicable national, state, local and foreign laws, rules, regulations, ordinances, decrees and orders including but not limited to restrictions on exporting or importing software, hardware or technical information.

9.16 Miscellaneous provisions

9.16.1 Entire agreement

No stipulation.

9.16.2 Assignment

No stipulation.

9.16.3 Severability

No stipulation.

9.16.4 Enforcement (attorneys' fees and waiver of rights)

No stipulation.

9.16.5 Force Majeure

TeliaSonera shall not be held responsible for any delay or failure in performance of its obligations hereunder to the extent such delay or failure is caused by fire, flood, strike, civil, governmental or military authority, acts of terrorism or war, sabotage, or other similar causes beyond its reasonable control and without the fault or negligence of TeliaSonera or its subcontractors.

9.17 Other provisions

No stipulation.

Acronyms

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

DEFINITIONS

Access control:

The granting or denial of use or entry.

Activation Data:

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

Administrator:

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

Administrator Certificate:

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

Agent:

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

Application Server:

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

Authentication:

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

Authorization:

The granting of permissions of use.

Authorised representative:

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

Asymmetric encryption algorithm:

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

Base certificate:

See primary certificate.

Business process:

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

CA certificate:

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

CA key:

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

Certificate:

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

Certificate extensions:

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

Certificate level:

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

Certification Authority (CA):

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

Certification Chain:

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

Certificate Policy:

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

Certification Practice Statement (CPS):

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

Certificate Revocation List (CRL):

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

Confidential:

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

Confidentiality:

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

Cross Certification:

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

Cryptographic Module:

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

Decryption:

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

Distinguished Encoding Rules (DER):

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

Digital Signature:

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

Directory Service:

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

Distinguished Name (DN):

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

Dual Control:

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

EID card:

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

Electronic identity check:

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

Electronic signature:

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

Encryption:

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

E-mail Certificates:

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

Entity:

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

FIPS 140-2:

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

FIPS 180-1:

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

Integrity:

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

ISO 11568-5:

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

Key:

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

Key holder:

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

Key Pair:

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

Log:

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

MD5:

A Message Digest Algorithm.

Non-repudiation:

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

Non-repudiation services:

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

Object Identifier:

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

Operator:

Employee of a CA.

Out of band process:

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

PKCS #1:

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

PKCS #7:

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

PKCS #10:

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

PKIX:

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

PKI personnel:

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

Policy:

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

Primary certificate:

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

PrintableString:

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

Private Key:

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

Public Key Infrastructure:

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

Public:

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

Public Key:

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

RA policy:

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

Registration Authority (RA):

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

Re-key:

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

Relative Distinguished Name (RDN):

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

Relying Party:

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

Repository:

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

Revocation:

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

RSA:

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

Secondary certificate:

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

Sensitive:

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

Signature Verification Certificate:

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

Split Knowledge

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

SSL Client Certificate:

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

SSL Server Certificate:

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

Storage module:

In this document relates to cryptographic module.

Subject:

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

Subscriber:

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

Surveillance Camera:

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

Symmetric encryption:

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

Threat:

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

Token:

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

Trusted Third Party (TTP):

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

Trusting party:

A recipient of a certificate which trusts this certificate on authentication, verification of digital signatures and/or encryption of information. See also Relying Party.

Unambiguous identity:

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

URI :

Universal Resource Indicator - an address on the Internet.

UTF8String:

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

Verification:

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

Vettor:

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

Vulnerability:

Weaknesses in a safeguard or the absence of a safeguard.

Written:

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

X.500:

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

X501 PrintableString:

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

X.509:

ITU standard that describes the basic format for digital certificates.