Telia hardware based e-legitimation

Certificate Policy and Certification Practice Statement

Revision Date: 31th March 2021

Version: 1.2

Published by: Telia Sverige AB

Table of Contents

Table of Contents ..... **III**
Revision History ..... **VIII**
Certification Practice Statement Summary **9**
1 INTRODUCTIONS **10**
1.1 Overview 10
1.2 Document name and identification 10
1.3 PKI participants 11
1.3.1 Certification authorities (CA) 11
1.3.2 Registration authorities (RA) 11
1.3.3 Subscribers 11
1.3.4 Relying parties 12
1.3.5 Other participants 12
1.4 Certificate usage 12
1.4.1 Appropriate certificate uses 12
1.4.2 Prohibited certificate uses 13
1.5 Policy administration 13
1.5.1 Organization administering the document 13
1.5.2 Contact person 13
1.5.3 Person determining CPS suitability for the policy 13
1.5.4 CPS approval procedures 13
1.6 Definitions and acronyms 13
2 PUBLICATION AND REPOSITORY RESPONSIBILITIES **14**
2.1 Repositories 14
2.1.1 CPS Repository 14
2.1.2 Revocation information Repository 14
2.2 Publication of certification information 14
2.3 Time or frequency of publication 14
2.4 Access controls on repositories 14
3 IDENTIFICATION AND AUTHENTICATION **15**
3.1 Naming 15
3.1.1 Types of names 15
3.1.2 Need for names to be meaningful 15
3.1.3 Anonymity or pseudonymity of subscribers 15
3.1.4 Rules for interpreting various name forms 15
3.1.5 Uniqueness of names 15
3.1.6 Recognition, authentication, and role of trademarks 15
3.2 Initial identity validation 16
3.2.1 Method to prove possession of private key 16
3.2.2 Authentication of organization identity 16
3.2.3 Authentication of individual identity 16
3.2.4 Non-verified subscriber information 16
3.2.5 Validation of authority 17
3.2.6 Criteria for interoperation 17
3.3 Identification and authentication for re-key requests 17
3.3.1 Identification and authentication for routine re-key 17
3.3.2 Identification and authentication for re-key after revocation 17
3.4 Identification and authentication for revocation request 17
4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS **18**
4.1 Certificate Application 18
4.1.1 Who can submit a certificate application 18
4.1.2 Enrollment process and responsibilities 18
4.2 Certificate application processing 18
4.2.1 Performing identification and authentication functions 18
4.2.2 Approval or rejection of certificate applications 20

4.2.3 Time to process certificate applications 20
4.3 Certificate issuance 20
4.3.1 CA actions during certificate issuance 20
4.3.2 Notification to subscriber by the CA of issuance of certificate 21
4.4 Certificate acceptance 21
4.4.1 Conduct constituting certificate acceptance 21
4.4.2 Publication of the certificate by the CA 21
4.4.3 Notification of certificate issuance by the CA to other entities 21
4.5 Key pair and certificate usage 21
4.5.1 Subscriber private key and certificate usage 21
4.5.2 Relying party public key and certificate usage 21
4.6 Certificate renewal 22
4.6.1 Circumstance for certificate renewal 22
4.6.2 Who may request renewal 22
4.6.3 Processing certificate renewal requests 22
4.6.4 Notification of new certificate issuance to subscriber 22
4.6.5 Conduct constituting acceptance of a renewal certificate 22
4.6.6 Publication of the renewal certificate by the CA 22
4.6.7 Notification of certificate issuance by the CA to other entities 22
4.7 Certificate re-key 22
4.7.1 Circumstance for certificate re-key 22
4.7.2 Who may request certification of a new public key 22
4.7.3 Processing certificate re-keying requests 22
4.7.4 Notification of new certificate issuance to subscriber 22
4.7.5 Conduct constituting acceptance of a re-keyed certificate 22
4.7.6 Publication of the re-keyed certificate by the CA 23
4.7.7 Notification of certificate issuance by the CA to other entities 23
4.8 Certificate modification 23
4.8.1 Circumstance for certificate modification 23
4.8.2 Who may request certificate modification 23
4.8.3 Processing certificate modification requests 23
4.8.4 Notification of new certificate issuance to subscriber 23
4.8.5 Conduct constituting acceptance of modified certificate 23
4.8.6 Publication of the modified certificate by the CA 23
4.8.7 Notification of certificate issuance by the CA to other entities 23
4.9 Certificate revocation and suspension 23
4.9.1 Circumstances for revocation 23
4.9.2 Who can request revocation 23
4.9.3 Procedure for revocation request 24
4.9.4 Revocation request grace period 24
4.9.5 Time within which CA must process the revocation request 24
4.9.6 Revocation checking requirement for relying parties 24
4.9.7 CRL issuance frequency 24
4.9.8 Maximum latency for CRL's 24
4.9.9 On-line revocation/status checking availability 24
4.9.10 On-line revocation checking requirements 24
4.9.11 Other forms of revocation advertisements available 24
4.9.12 Special requirements re-key compromise 24
4.9.13 Circumstances for suspension 24
4.9.14 Who can request suspension 24
4.9.15 Procedure for suspension request 24
4.9.16 Limits on suspension period 24
4.10 Certificate status services 25
4.10.1 Operational characteristics 25
4.10.2 Service availability 25
4.10.3 Optional features 25
4.11 End of subscription 25
4.12 Key escrow and recovery 25
4.12.1 Key escrow and recovery policy and practices 25

4.12.2 Session key encapsulation and recovery policy and practices 25
5 FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS 26
5.1 Physical controls 26
5.1.1 Site location and construction 26
5.1.2 Physical access 26
5.1.3 Power and air conditioning 29
5.1.4 Water exposures 29
5.1.5 Fire prevention and protection 29
5.1.6 Media storage 30
5.1.7 Waste disposal 30
5.1.8 Off-site backup 30
5.2 Procedural controls 30
5.2.1 Trusted roles 30
5.2.2 Number of persons required per task 32
5.2.3 Identification and authentication for each role 32
5.2.4 Roles requiring separation of duties 33
5.3 Personnel controls 33
5.3.1 Qualifications, experience, and clearance requirements 33
5.3.2 Background check procedures 33
5.3.3 Training requirements 34
5.3.4 Retraining frequency and requirements 34
5.3.5 Job rotation frequency and sequence 34
5.3.6 Sanctions for unauthorized actions 34
5.3.7 Independent contractor requirements 34
5.3.8 Documentation supplied to personnel 35
5.4 Audit logging procedures 35
5.4.1 Types of events recorded 35
5.4.2 Frequency of processing log 36
5.4.3 Retention period for audit log 36
5.4.4 Protection of audit log 36
5.4.5 Audit log backup procedures 36
5.4.6 Audit collection system (internal vs. external) 36
5.4.7 Notification to event-causing subject 36
5.4.8 Vulnerability assessments 36
5.5 Records archival 37
5.5.1 Types of records archived 37
5.5.2 Retention period for archive 37
5.5.3 Protection of archive 37
5.5.4 Archive backup procedures 38
5.5.5 Requirements for time-stamping of records 38
5.5.6 Archive collection system (internal or external) 38
5.5.7 Procedures to obtain and verify archive information 38
5.6 Key changeover 38
5.6.1 Self-Signed CA 38
5.6.2 CA Hierarchies 39
5.7 Compromise and disaster recovery 39
5.7.1 Incident and compromise handling procedures 39
5.7.2 Computing resources, software, and/or data are corrupted 39
5.7.3 Entity private key compromise procedures 39
5.7.4 Business continuity capabilities after a disaster 40
5.8 CA or RA termination 40
6 TECHNICAL SECURITY CONTROLS 41
6.1.1 Key pair generation 41
6.1.2 Private Key delivery to subscriber 41
6.1.3 Public key delivery to certificate issuer 42
6.1.4 CA public key delivery to relying parties 42
6.1.5 Key sizes 42
6.1.6 Public key parameters generation and quality checking 42
6.1.7 Key usage purposes (as per X.509 v3 key usage field) 42

6.2 Private Key Protection and Cryptographic Module Engineering Controls 42
6.2.1 Cryptographic module standards and controls 43
6.2.2 Private Key (n out of m) multi-person control 43
6.2.3 Private Key escrow 43
6.2.4 Private Key backup 43
6.2.5 Private Key archival 43
6.2.6 Private Key transfer into or from a cryptographic module 43
6.2.7 Private Key storage on cryptographic module 44
6.2.8 Method of activating private key 44
6.2.9 Method of deactivating private key 44
6.2.10 Method of destroying private key 44
6.2.11 Cryptographic Module Rating 44
6.3 Other aspects of key pair management 44
6.3.1 Public key archival 45
6.3.2 Certificate operational periods and key pair usage periods 45
6.4 Activation data 45
6.4.1 Activation data generation and installation 45
6.4.2 Activation data protection 45
6.4.3 Other aspects of activation data 45
6.5 Computer security controls 45
6.5.1 Specific computer security technical requirements 45
6.5.2 Computer security rating 46
6.6 Life cycle technical controls 46
6.6.1 System development controls 46
6.6.2 6.6.2 Security management controls 46
6.6.3 Life cycle security controls 46
6.7 Network security controls 47
6.8 Time-stamping 47
7 CERTIFICATE AND OCSP PROFILES 48
7.1 Certificate profile 48
7.1.1 Version number(s) 48
7.1.2 Certificate extensions 48
7.1.3 Algorithm object identifiers 49
7.1.4 Name forms 49
7.1.5 Name constraints 49
7.1.6 Certificate policy object identifier 50
7.1.7 Usage of Policy Constraints extension 50
7.1.8 Policy qualifiers syntax and semantics 50
7.1.9 Processing semantics for the critical Certificate Policies extension 50
7.2 CRL profile 50
7.2.1 Version number(s) 50
7.2.2 CRL and CRL entry extensions 50
7.3 OCSP profile 50
7.3.1 Version number(s) 50
7.3.2 OCSP extensions 50
8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS 51
8.1 Frequency or circumstances of assessment 51
8.2 Identity/qualifications of assessor 51
8.3 Assessor's relationship to assessed entity 51
8.4 Topics covered by assessment 51
8.5 Actions taken as a result of deficiency 51
8.6 Communication of results 52
9 OTHER BUSINESS AND LEGAL MATTERS 53
9.1 Fees 53
9.1.1 Certificate issuance or renewal fees 53
9.1.2 Certificate access fees 53
9.1.3 Revocation or status information access fees 53
9.1.4 Fees for other services 53

9.1.5 Refund policy 53
9.2 Financial responsibility 53
9.2.1 Insurance coverage 53
9.2.2 Other assets 53
9.2.3 Insurance or warranty coverage for end-entities 53
9.3 Confidentiality of business information 53
9.3.1 Scope of confidential information 53
9.3.2 Information not within the scope of confidential information 54
9.3.3 Responsibility to protect confidential information 54
9.4 Privacy of personal information 54
9.4.1 Privacy plan 54
9.4.2 Information treated as private 54
9.4.3 Information not deemed private 55
9.4.4 Responsibility to protect private information 55
9.4.5 Notice and consent to use private information 55
9.4.6 Disclosure pursuant to judicial or administrative process 55
9.4.7 Other information disclosure circumstances 55
9.5 Intellectual property rights 55
9.6 Representations and warranties 55
9.6.1 CA representations and warranties 55
9.6.2 RA representations and warranties 56
9.6.3 Subscriber representations and warranties 56
9.6.4 Relying party representations and warranties 56
9.6.5 Representations and warranties of other participants 56
9.7 Disclaimers of warranties 57
9.8 Limitations of liability 57
9.9 Indemnities 57
9.10 Term and termination 57
9.10.1 Term 57
9.10.2 Termination 57
9.10.3 Effect of termination and survival 57
9.11 Individual notices and communications with participants 57
9.12 Amendments 57
9.12.1 Procedure for amendment 57
9.12.2 Notification mechanism and period 58
9.12.3 Circumstances under which OID must be changed 58
9.13 Dispute resolution provisions 58
9.14 Governing law 58
9.15 Compliance with applicable law 58
9.16 Miscellaneous provisions 58
9.16.1 Entire agreement 58
9.16.2 Assignment 59
9.16.3 Severability 59
9.16.4 Enforcement (attorneys' fees and waiver of rights) 59
9.16.5 Force Majeure 59
9.17 Other provisions 59
Acronyms and Definitions 60
Acronyms 60
Definitions 61
References 67

Revision History

Version	Version date	Change	Author
1.0	2009-06-08	First version of the new CPS for Telia hardware based e-legitimation. Major update compared to earlier Swedish version (rev A) of the CPS: - a new CPS OID is being used, - changed to English as language, - uses structure according to RFC 3647, - points to TeliaSonera Production CPS for common issues which are the same for all Telia eID services, - allows for children from 13 years of age to receive Telia e-legitimation, - allows for foreign passports to be used as identification documents.	Telia CPS Management Team
1.1	2018-10-24	- Changed Company name - Removed ETSI as Certificate Policy - Other minor changes	Telia CPS Management Team
1.11	2018-12-21	- Change OCSP RFC reference - Other minor changes	Telia CPS Management Team
1.12	2020-01-21	- Corrected OID reference	Telia CPS Management Team
1.2	2020-03-01	Removed reference to Telia Production CPS and added relevant information to this CPS	Telia CPS Management Team

Certification Practice Statement Summary

This document defines the Certificate Policies and Certification Practice Statement for the issuing of 'Telia hardware based e-legitimation' certificates. Telia hardware based e-legitimation CA's will sign and issue certificates to individuals with Swedish personnummer (Swedish social security number) whom are residents in Sweden. The private keys connected to these certificates will be stored in hardware based devices, mainly EID cards (Electronical Identification Cards).

Telia hardware based e-legitimation is a part of the 'Telia eID Services'.

This document is intended for users, relying parties, customers and organizations that are interested in the Telia e-legitimation certificate Services and what obligations Telia has and what processes Telia uses as issuer of those certificates.

The Telia hardware based e-legitimation CPS generally conforms to the structure in Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices 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 certificates 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 INTRODUCTIONS

1.1 *Overview*

This document defines the Certification Practice Statement for the issuing of 'Telia hardware based e-legitimation' certificates (here on referred to as 'Telia e-legitimation').

This CPS is also a Certifcate Policy for Telia hardware based e-legitimation certificates.

The CPS describes the business processes valid when issuing certificates for individuals and it also applies for the revocation and revocation check of above mentioned certificates.

The CPS contains all relevant processes and descriptions that should make it possible for relying parties and other parties to form an opinion about the security level of the issued certificates.
In addition to the CPS there are a number of Telia internal documents which in detail describes all routines and processes involved in all parts of the issuing process, for example technical descriptions of the CA and RA systems, plans of physical production sites, different types of security routines and so on. Those documents are not publically available.

The CPS also contains the responsibilities and warranties of Telia at the time of certificate issuance and commitments to customers and relying parties.

Telia is responsible for this particular practice statement (CPS) and all processes and commitments indicated in this document. Parts of the service may be performed by a subcontractor or other parties. If this is the case, Telia will always be held as the ultimate responsible in accordance with this CPS.

Telia e-legitimation can be issued to Swedish residents of 13 years and older with a Swedish personnummer (social security number).
Telia acts as a Trusted Third Party and Telia e-legitimation is to be used when interacting with different Swedish authorities, public administration, and private service providers.

The CPS follows RFC3647 "Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework" in structure and content.

Telia's CPS for Telia e-legitimation is decided and approved by the Telia CPS Management Team (CPSMT). The CPSMT is also responsible for making sure that the CPS fulfills all requirements mentioned in the certificate policy and is continuously checking that the issuance of Telia e-legitimation is done in compliance with this CPS.
If there is a need to update this CPS, the work shall be initiated by someone from the CPSMT, and before the update takes effect the CPSMT will make an approval decision. Also see section 9.12.

This CPS has been published to:
https://repository.trust.telia.com.

Telia CPS Management Team approved this CPS 15th March 2021.

1.2 *Document name and identification*

The routines and roles resulting from this CPS apply only in connection with certificates referring to the Telia hardware based e-legitimation CPS.

The CPS name of this CPS is {SE-TELIA-ELEG-CPS6} and the object identifier is {1.2.752.35.1.4}:

```
ISO (1) ISO member body (2) SE (752) Telia Sverige AB (35)
Telia e-legitimation (1) Telia hardware based e-legitimation Certificate
Policy and Certification Practice Statement (4).
```

The Telia document number of this CPS is 4/011 01-AZDA 102 213.

1.3 *PKI participants*

Telia will only issue Telia e-legitimation certificates to Swedish residents with a Swedish personnummer (Swedish social security number).

All of the participating organizations shall undertake what's stated in this CPS.

This CPS applies to Telia, RAs and other subcontractors contracted by Telia, subscribers, relying parties and auditors.

1.3.1 Certification authorities (CA)

Telia manages the Telia eID Services. In the Telia eID Services CAs are created for Telia services and other organizations that are customers to Telia.

Telia eID Services is responsible for managing the certificate life cycle of Telia e-legitimation CAs and end entity certificates signed by those CAs. This will include:

- Creating and signing of certificates binding subscribers, and CA and RA personnel with their public encryption keys; and
- Provide certificate status through OCSP responders or;
- Provide certificate status through RP-API

1.3.2 Registration authorities (RA)

RAs operating under this CPS are responsible for all duties assigned to it by Telia and this CPS.

Telia is responsible for all RAs used when issuing Telia e-legitimation even in the case that Telia is using subcontractors or customers as RAs. The RAs receive applications for Telia e-legitimation and processes the necessary checks for each application before a Telia e-legitimation is issued.

All RAs are contractually bound to follow Telia's regulations regarding the issuance of Telia e-legitimation and the RAs routines and processes are audited by Telia before the RAs are approved as RAs for Telia e-legitimation.

All individuals at RAs are authenticated by certificates when performing their duties on behalf of Telia.

Administrators whom act within the framework of an RA have been educated to gain necessary skills to verify and approve the certificate applications and/or to hand out the Telia e-legitimation to the subscriber when issued.

The RA functions are geographically segregated from the issuing system.

Telia e-legitimation is mainly issued for one of three different product types of EID cards. Typical RAs for the product types are:

a) "Telia e-legitimation EID cards for individuals": Telia or a Swedish government;
b) "Telia e-legitimation Company cards": Public and private organizations; and
c) "Telia e-legitimation SIS-approved Employee/Company cards": Public and private organizations with a valid license from Det Norske Veritas for issuing of identification cards according to Swedish standard SS 61 43 14:2004/T1:2005 "Identifieringskort - Identitetskort av typ ID-1" (Identity cards – Identification cards of type ID-1) and the regulation SBC 151-U "Särskilda Bestämmelser för certifiering av överenstämmelse med standard SS 61 43 14" (Special Regulations for certification of compliance with standard SS 61 43 14).

Telia's regulations regarding the issuance of Telia e-legitimation is called "Telias policy för utfärdande av ID-kort med e-legitimation" for product type a) and "Telias policy för utfärdande av företagskort med e-legitimation" for product type b) and c).

1.3.3 Subscribers

A subscriber has to be a Swedish resident with a Swedish personnummer who is at least 13 years old. In order to apply for a Telia e-legitimation, individuals under the age of 18 years need to have all guardians' approval.

All subscribers must sign an approval contract of Telia's conditions for the use of Telia e-legitimation.

Certificates may also be issued to OCSP responders at Telia or at an organization appointed by Telia to be able to handle OCSP requests.

As mentioned in section 1.3.2 Telia e-legitimation is mainly issued for three different product types of EID cards.

"Telia e-legitimation SIS approved Employee/Company cards" are valid identification cards and obey to the requirements stated in SS 61 43 14:2004/T1:2005 and the regulation SBC 151-U. Such EID cards are

only issued to employees or other personnel contractual connected to organizations with a valid license to issue such EID cards.

The subscriber is responsible for leaving correct application information and for protecting and storing his/her own private key in an acceptable manner. The subscriber is always the owner of Telia e-legitimation regardless of the hardware protecting the private keys.
Each application for Telia e-legitimation results in two certificates, one Confidentiality certificate to be used when authenticating and/or encrypting, and one Digital Signature certificate to be used for signing. The two certificates of Telia e-legitimation are handled as one unit, for example regarding revocation where both certificates are revoked in case of an approved revocation request.

1.3.4 Relying parties

A Relying Party may be either an RA organization connected to Telia e-legitimation CAs or any other organization, person, application or device where there is a valid agreement with Telia for the use of Telia Relying Party services.

1.3.5 Other participants

No stipulation.

1.4 *Certificate usage*

Telia e-legitimation is issued to individuals and is amongst others meant for use with services at governments, other organizations within the public sector, business agencies and private service providers where electronically proof of the subscriber's identity and electronic signatures are needed.

The relying party is responsible for deciding whether the issuing processes mentioned in this CPS have an adequate security level for the application where the certificates are to be used.

The subscriber of Telia e-legitimation and the relying parties are legally bound through a contractual agreement with Telia.

1.4.1 Appropriate certificate uses

Telia e-legitimation may be used by individuals to communicate electronically in a safe and secure way with Swedish authorities and companies in the capacity as individual or as representative for a legal person. To secure the communication between an organization and an individual, one or many key usages are required for authentication, signing and encryption.

An approved application of Telia e-legitimation will generate two certificates for the subscriber to use. The Digital Signature certificate and its corresponding private key shall only be used for digital signatures. The Confidentiality certificate and its corresponding private key shall be used for authentication/ identification and encryption purposes.

Information about each certificate's appropriate key usage is indicated in the key usage extension of the certificate. When using the certificates and their corresponding private keys, consideration must be taken to the certificate's usage area.

Certificates issued in accordance with this CPS identify the following types of usage for the certified key pairs and the key usages are according to stipulations in section 6.1.7:

a) Electronical signatures for use in non-repudiation services;
b) Identification and authentication; and
c) Confidentiality encryption.

It is beyond Telia's control to prevent private keys from being used for unwanted purposes or for purposes against the subscriber's intentions. All subscribers are requested to use the private keys only in trustworthy and reliable equipment and applications and not to use the private digital signature key to sign data that haven't been reviewed and approved by the subscriber.

Customers that are RAs for Telia e-legitimation or relying parties may use the information in Telia e-legitimation to have the public keys of the certificates resigned in secondary subscriber certificates issued by another CA. The value of the key usage extension must remain the same for the corresponding primary and secondary certificates or be further restricted regarding the key usage for the secondary Confidentiality certificate.

1.4.2 Prohibited certificate uses

It is not recommended to use the Confidentiality certificates for encryption of files. This recommendation is done since there are no backups of the private keys connected to the certificates.

1.5 *Policy administration*

1.5.1 Organization administering the document

Telia CPS Management Team (CPSMT) is the responsible authority for reviewing and approving changes to the Telia hardware based e-legitimation CPS. Written and signed comments on proposed changes shall be directed to the Telia contact as described in Section 1.5.2. Decisions with respect to the proposed changes are at the sole discretion of CPSMT.

CPSMT consists of three regular members appointed by Telia eID Services and optional members that may be called for when necessary to decide issues outside the competence of the regular members. At least two of the regular members have to agree upon a decision for a change to be valid and introduced in the CPS.

1.5.2 Contact person

Any questions relating to this CPS should be sent in writing to:

Telia Sverige AB
PKI
Box 5275
402 25 Göteborg
Sweden

Telephone: 020 32 32 62, international +46 771 32 32 62
E-mail: kundtjanst-eid@teliacompany.com
Web: www.telia.se

1.5.3 Person determining CPS suitability for the policy

CPSMT is the administrative entity for determining this Certification Practice Statement (CPS)

1.5.4 CPS approval procedures

CPSMT will review any modifications, additions or deletions done to this CPS, and determine if modifications, additions or deletions are acceptable and do not jeopardize operations or the security of the issuance of Telia e-legitimation.

1.6 *Definitions and acronyms*

A list of definitions and acronyms is 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 and CA certificates issued according to this CPS are published at the Telia eID Services Repository web site (https://repository.trust.telia.com). The web site is normally available at all times.

Any reviews or suggestions for changes of this CPS will also be announced at the web site mentioned above.

2.1.2 Revocation information Repository

OCSP requests shall be made to http://ocsp.trust.telia.com. OCSP requests need to be signed, i.e. a relying party who wants to validate certificates by OCSP needs to make an agreement with Telia regarding the Relying Party services and receive a valid Relying Party certificate.

2.2 *Publication of certification information*

Telia will make the following information available.

a) This CPS;
b) Issued CA certificates; and
c) Revocation information via OCSP responders to Telia customers with valid Telia Relying Party agreements.

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

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*

The Relying Party service (OCSP) is available all days of the week, 24 hours a day, except when there is planned maintenance or other factors beyond Telia's control. In case of interruptions in the services Telia will promptly begin work to restore the services to normal functionality.

Revocation information of issued subscriber certificates will be updated promptly or at least within one hour from an accepted certificate revocation request.

2.4 *Access controls on repositories*

This CPS and issued CA certificates are publicly available at https://repository.trust.telia.com.

Relying Party services (OCSP) are only available through an agreement with Telia and the use of a valid Relying Party certificate. The service is available at http://ocsp.trust.telia.com.

3 IDENTIFICATION AND AUTHENTICATION

3.1 *Naming*

3.1.1 Types of names

The subscriber is registered with identity, name and contact information. This will be done by Telia or an RA appointed by Telia. The subscriber's personnummer is used to establish an unambiguous identity of the subscriber.

The subscriber's personnummer is used to verify the subscriber's names and home address against the official Swedish Population Address Register (SPAR) or other equivalent register approved by Telia.

The Telia e-legitimation certificates will include subject distinguished names in accordance with the X.500 series of standards. The certificate subject name attributes and encoding will be according to section 7.1.5.

The following subscriber information is included in the Telia e-legitimation certificates:

Information	Demand on content
Given Name	All of the subscriber's given names spelled according to the register. Pseudonyms are not allowed.
Surname	All of the subscriber's surnames spelled according to the register. Pseudonyms are not allowed.
Common name	A combination of the subscriber's commonly used given name and all surnames of the subscriber. The subscribers commonly used given name is according to the register. If information regarding this is missing in the register the information is taken from the subscriber's application under the condition that the given name stated in the application is one of the given names registered in the register. Otherwise the first given name in the register is used.
Country	'SE', Sweden, the country where the subscriber is resident at the time of the certificate application.
Personnummer	Valid Swedish social security number – 12 digits in the form 'YYYYMMDDNNNC'. Used to establish an unambiguous identity of the subscriber.

The subscriber's home address according to SPAR, or other equivalent register approved by Telia, is used to send the activation data to the subscriber.

3.1.2 Need for names to be meaningful

The Telia e-legitimation certificates will contain the legal name of the subscriber and the subscriber's personnummer which uniquely identifies the subscriber.

3.1.3 Anonymity or pseudonymity of subscribers

Not applicable.

3.1.4 Rules for interpreting various name forms

No stipulation.

3.1.5 Uniqueness of names

The subject distinguished name will contain a unique sequence of naming attributes ensuring a unique reference to each subscriber.

For subscribers receiving Telia e-legitimation the subject distinguished name of the certificates will contain the subscriber's personnummer (social security number) which uniquely identifies the subscriber.

3.1.6 Recognition, authentication, and role of trademarks

Not applicable.

3.2 *Initial identity validation*

3.2.1 Method to prove possession of private key

The subscriber's private keys are generated in the chip of the EID card or the hardware device by the card manufacturer appointed by Telia. The key generation is done in the same production process where initialization and personalization of the card or device takes place.

Signed PKCS#10 or CRS (Certificate Request Syntax) are made by the RA at the card manufacturer site and are sent to Telias systems. The systems of Telia validate the signature of the RA making the request and validate the signature of the requests. The RAs private keys are stored on a smart card or other hardware device and all certificate requests can be traced to the individual responsible for the request.

The certificates are then issued by the CA system and returned to the card manufacturer to be stored in the corresponding card or device. The personalized card or device is then distributed in a secure way to the subscriber.

3.2.2 Authentication of organization identity

Not applicable.

Only information concerning individuals are certified in Telia e-legitimation certificates.

3.2.3 Authentication of individual identity

To become a subscriber of Telia e-legitimation, an application is filed either by an individual applicant or an organization authorized on behalf of the applicant. Background checks will be made by Telia or RAs appointed by Telia. Telia and/or RAs will keep a record of the type of identification document used, and the document's id, for the authentication of the individual for at least ten years after the expiration date of the issued Telia e-legitimation.

Depending on which product type the applicant is applying for, identification and authentication will be done in line with one of the three process types described in section 4.2 with subsections.

In all cases Telia or an RA appointed by Telia will compare the identity of the applicant, or another person certifying the identity of the applicant, with a valid identification document. This is done either as a part of the application process or at the time the subscriber receives the EID card or hardware device. Valid identification documents are:

a) SIS-approved Employee card, Company card or Identification card;
b) Skatteverkets identity card;
c) Swedish driving license;
d) Swedish EU passport;
e) Swedish National identity card;
f) EIDs issued in Sweden with the Swedish EID trust mark (Svensk e-legitimation) administered by Myndigheten för Digital Förvaltning (Agency for Digital Government). The EIDs must be at the assurance level of 3 or 4.

Telia, or the card manufacturer appointed by Telia, always authenticate the information given by the applicant or by an organization authorized to act on behalf of the applicant. Before the Telia e-legitimation certificates are issued, the information of the application is checked against the Swedish national register SPAR or other register approved by Telia.

The authenticated information is the subscriber's personal information and home address according to 3.1.1.

3.2.4 Non-verified subscriber information

Not applicable.

3.2.5 Validation of authority

Applications for a Telia e-legitimation will only be made by individuals.
Telia or an RA, on behalf of Telia, will validate that the following have been verified:

- The identity of the individual making the application; and
- In case the subscriber is under aged, i.e. less than 18 years old, permission has been received signed by all guardians.

3.2.6 Criteria for interoperation

Not applicable.

Cross certification will not be a service for CAs conformant with this CPS.

3.3 *Identification and authentication for re-key requests*

3.3.1 Identification and authentication for routine re-key

Routine re-key is not supported.

No special routine exists for renewal of Telia e-legitimation. Renewal of keys and certificates are ordered and delivered in the same way as new certificates meaning, a new validation of the subscriber is done and new hardware with new subscriber private keys are delivered.

3.3.2 Identification and authentication for re-key after revocation

See section 3.3.1 above.

3.4 *Identification and authentication for revocation request*

A request for revocation will be done in one of the following manners:

- The subscriber makes a phone call to Telia service desk to revoke the certificates;
- The subscriber uses a self administration GUI to revoke the certificates of Telia e-legitimation.
- The request must be digitally signed by the Digital Signature private key of the Telia e-legitimation;
- Telia or an RA appointed by Telia will, if there is a suspicion of a compromised Telia e-legitimation; revoke the certificates on behalf of the subscriber; or
- Telia or an RA will revoke the certificates if requested by a representative of the Employer. This is only applicable in the case that a Telia e-legitimation of a subscriber is issued for a Company card/hardware device or a SIS-approved Employee/Company card which has been issued by the Employer or another organization with which the subscriber has a business relation.

When a request for revocation is requested over the phone, the person who calls has to give necessary information in order for Telia to be able to revoke the certificates.

All Telia or RA personnel approved to make revocations have been supplied with an individual RA administrator card. The RA administrator is authenticated to the revocation application by using the private keys of the RA administrator card.

When making a revocation request as above, Telia's systems will check that the revocation request is valid and that the person requesting the revocation is authorized to do so. If both these criteria are met, the certificate in question is revoked.
The revocation information in the OCSP service is updated no later than one hour after that the Telia e-legitimation certificates have been revoked.

Telia will keep records of all revocation requests. The records will hold information of the identity of the requesting person, the identity of the administrator revoking the certificates and the time the revocation was done. The records are included in the audit logs of the RA systems at Telia's production facilities. For further information regarding the records see section 5.4 and 5.5.

The service desk of Telia eID Services is responsible for receiving revocation requests for Telia e-legitimation at all times. The customer has to give information making it possible for the service desk to identify the correct e-legitimation. The service desk is available to receive revocation requests 24 hours a day, all days of the year.

4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 *Certificate Application*

4.1.1 Who can submit a certificate application

The certificate application is done either by the applicant or by an organization authorized to act on behalf of the applicant. The certificate application is processed via an administrator at an RA appointed by Telia or sent directly to Telia.

The RA or Telia administrator sends the certificate application to the card manufacturer appointed by Telia. The administrator signs the certificate applications digitally with the private key of their RA administration cards.

All subscriber information will be validated against valid registers at the reception of the certificate request.

4.1.2 Enrollment process and responsibilities

The subscriber is bound through a Subscriber Agreement with Telia. The customer accepts the terms and conditions of the agreement either at the time of registration or upon certificate acceptance.

The enrollment process depends on the type of EID card or hardware device protecting the private keys associated with the Telia e-legitimation. There are three different processes described in section 4.2 with subsections.

4.2 *Certificate application processing*

The application and delivery processes for Telia e-legitimation certificates are dependent on the type of EID card or hardware device ordered, which will protect the private keys associated with the Telia e-legitimation. There are three different processes, as described below in section 4.2.1, performed by Telia or an RA appointed by Telia.

4.2.1 Performing identification and authentication functions

Telia or an RA appointed by Telia will always identify the applicant and authenticate the certificate application. How identification and authentication is done will depend on the product type used to protect the private keys associated with the Telia e-legitimation. The different processes are stated in the subsections below.

The management of electronical registration at Telia, or an RA appointed by Telia, takes place in an environment suitable protection level regarding integrity and routines are used to prevent confusion regarding identity information and possible photos and signatures belonging to the applications.

When all steps of the identification and authentication process has been finished the administrator at Telia or the RA will digitally sign and send the certificate application to the card manufacturer. Every administrator has an own RA administrator card and all signed certificate applications can be traced to the administrator who signed the application.

When the card manufacturer receives the certificate application the process of certificate issuance process according to section 4.3 will be carried out.

Telia has two regulations regarding the issuance of Telia e-legitimation that are used as requirements to be fulfilled by Telia and the appointed RAs. The processes and routines used by Telia and appointed RAs will be reviewed by Telia before the first certificate applications can be performed by the appointed RA. The two policy documents are:

a) “Telias policy för utfärdande av ID-kort med e-legitimation” (Telia’s policy for issuing of identification cards with e-legitimation); and
b) “Telias policy för utfärdande av företagskort med e-legitimation” (Telia’s policy for issuing of company cards with e-legitimation).

The two policy documents include the RA obligations from the CPS and other demands on the RA processes and routines.

4.2.1.1 Identification cards issued for individuals by an RA other than Telia

The business processes used by the RA will comply with the regulation “Telias policy för utfärdande av ID-kort med e-legitimation”.

The following process steps are at least used when approving an application for an identification card with Telia e-legitimation, issued by the approved RA:

a) An application for the identification card is done by the applicant in person at the RAs premises and identifies him/herself according to “Telias policy för utfärdande av ID-kort med e-legitimation”. If the applicant does not have a valid identification document a person certificating the identity of the applicant may be used in accordance with “Telias policy för utfärdande av ID-kort med e-legitimation”;
b) An applicant who has an age of less than 18 years need to be accompanied by one of his/her guardians and needs to bring a document with all guardians’ approval to apply for an identification card.
c) The RA administrator verifies the identification information given in the application and verifies the identification information, based on personnummer, given in the application with the corresponding information in the SPAR register or equivalent register approved by Telia. If the name information in the application differs from the SPAR information the application is rejected, see section 4.2.2;
d) A photo is taken of the applicant and the applicant’s signature is scanned;
e) The RA administrator fills in an electronical order of an identification card with the identification information according to the register used, and including the photo and signature of the applicant. The order is signed by the RA with the private key on the RA administrator’s card and sent to the card manufacturer. The RA administrator needs to be authorized to order the product; otherwise the order will be rejected. The application form is archived;
f) The production steps according to section 4.3.1 are done at the card manufacturer’s premises;
g) The finalized identification cards are sent via registered mail to the RA premises where the application of the identification card was made;
h) The activation codes are sent to the applicant’s home address;
i) The applicant receives a notification from the RA to show up in person at the RA premises where the application was made to receive the identification card;
j) The applicant goes to the RA premises and the applicant identifies him/herself according to “Telias policy för utfärdande av ID-kort med e-legitimation”;
k) The administrator informs the applicant of the Subscriber Agreement for Telia e-legitimation, if not done earlier according to the RA’s processes. The applicant accepts the Subscriber Agreement and the delivery of the identification card by signing a card receipt. The RA administrator signs the receipt as well, hands out the product to the applicant, and keeps the receipt for archiving.

4.2.1.2 Company EID cards and hardware devices

The business processes used by the RA organization will comply with the regulation “Telias policy för utfärdande företagskort med e-legitimation”.

Company cards are issued by customers of Telia to their employees or other individuals connected to their businesses. The customer acts as an RA for the issuing of the corresponding Telia e-legitimation.

The following process steps are at least used when approving an application for a product, with Telia e-legitimation, issued by the approved RA:

a) An application for the product is done by the applicant or by another authorized person according to the organization’s processes and sends the application to an authorized RA administrator.
b) The RA administrator verifies the identification information given in the application and authenticates the authority of the person who has signed the application;
c) The applicant comes in person to the RA administrator and identifies him/herself according to “Telias policy för utfärdande av företagskort med e-legitimation”. If the applicant does not have a valid identification document a person certificating the identity of the applicant may be used in accordance with “Telias policy för utfärdande av företagskort med e-legitimation”;
d) A photo is taken of the applicant and the applicant’s signature is scanned if applicable;
e) The RA administrator fills in an electronical product order with the identification information. The order is signed by the RA with the private key on the RA administrator’s card and sent to the card manufacturer. The RA administrator needs to be authorized to order the product; otherwise the order will be rejected. The application form is archived;
f) The card manufacturer verifies the identification information, based on personnummer, stated in the application with the corresponding information in the SPAR register or other equivalent register approved by Telia. If the name information in the application differs from the SPAR information the application is rejected, see section 4.2.2;

g) The production steps according to section 4.3.1 are done at the card manufacturer's premises.
h) The finalized product is sent via registered mail to the Telia RA administrator who made the order of the product;
i) The activation codes are sent to the applicant's home address;
j) The applicant receives a notification from the organization to show up in person at the RA administrator to receive the Company card or device;
k) The applicant goes to the RA administrator and the applicant identifies him/herself according to "Telias policy för utfärdande företagskort med e-legitimation". If the applicant does not have a valid identification document a person certificating the identity of the applicant may be used in accordance with "Telias policy för utfärdande företagskort med e-legitimation".
l) The administrator informs the applicant of the Subscriber Agreement for Telia e-legitimation, if not done earlier according to the organization's processes. The applicant accepts the Subscriber Agreement and the delivery of the product by signing a receipt. The RA administrator signs the receipt as well, hands out the product to the applicant, and keeps the receipt for archiving.

The steps c) and d) above are only applicable if a photo is needed for the card product which has been applied for. In other cases all of the identification procedure of c) will take place during step k).

4.2.2 Approval or rejection of certificate applications

Telia or an RA appointed by Telia will approve a certificate application if it meets the requirements of validation and identification. All other certificate applications will be rejected.

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

The name information given in a certificate application will be validated against the SPAR register or an equivalent register approved by Telia. If the name information given in the application differs from the information in the register the certificate application will be rejected and the applicant will be informed about the reason. Minor spelling differences are accepted and the spelling of the subscriber's names according to the register will be used in the certificates subject distinguished name.

4.2.3 Time to process certificate applications

The processing time of a Telia e-legitimation application will differ depending on the steps taken in the validation plan. This depends among other things on the hardware used to protect the private keys.

The processing times will be stated in the RA agreements or other applicable agreements.

4.3 *Certificate issuance*

4.3.1 CA actions during certificate issuance

Telia approves applications for Telia e-legitimation by issuing a Telia e-legitimation for the applicant.

The required information registration for certificates and belonging EID cards and hardware devices are performed in a system, with very high protection level regarding integrity and confidentiality, at the site of the card manufacturer appointed by Telia. The registration routine assures that no personal information, and possible attached photos and signatures, are to be confused or mapped wrongly.

The production process for issuing Telia e-legitimation certificates with belonging private keys on EID cards, or other hardware devices, consist at least of the following activities:

a) Authentication of the digital signature done by the RA submitting the certificate request;
b) Control of the RA's authority to apply for the ordered product where the private keys associated with the Telia e-legitimation will be secured;
c) Validation of the applicants personal information against the SPAR register or other equivalent register approved by Telia;
d) Key generation on cards or devices;
e) Creation of activation data, i.e. PINs and PUK;
f) Visual personalization of cards and devices;
g) Electronical personalization of cards and devices;
h) Certificate requests and storage of certificates on cards and devices;
i) Distribution of cards and devices to the RAs making the orders or to the home address of the applicant by registered mail; and
j) Distribution of activation data i.e. letters with PINs and PUK. The envelopes are tamper proof and the content of the letters is impossible to view from 'outside'.

Due to the segregation of duties principle, no individual has the necessary rights to perform all the steps mentioned above. In order to enable traceability, the issuance process is documented and logged electronically. Each performed step in the issuance process is signed by a responsible administrator at the card manufacturer site.

The certificates are created in Telia's CA system when the system receives a signed certificate request from the authorized RA at the card manufacturer. The private keys for the RA are stored on an RA administrator card. Each certificate request can be traced to an individual responsible for the request.

4.3.2 Notification to subscriber by the CA of issuance of certificate

When the certificates have been issued, together with the corresponding EID card or hardware device protecting the private keys, the subscriber will be notified by the RA.

Notification will normally be done via mail but may also be done via e-mail or telephone.
The way this will be done is dependent on the agreement between Telia and the RA.

4.4 *Certificate acceptance*

4.4.1 Conduct constituting certificate acceptance

The subscriber accepts to comply with his/her obligations concerning Telia e-legitimation by accepting the delivery of the EID card or hardware device, with the Telia e-legitimation and corresponding private keys, and by signing the acceptance of the Subscriber Agreement for Telia e-legitimation.

4.4.2 Publication of the certificate by the CA

Telia will not publish subscriber certificates to a public available repository if not agreed upon with a customer to Telia.

Publication will be done to internal directories or databases at the Telia production sites or at a customer organizations site.

Telia will publish all CA certificates at the Telia eID Services Repository web site.

4.4.3 Notification of certificate issuance by the CA to other entities

No stipulation.

4.5 *Key pair and certificate usage*

4.5.1 Subscriber private key and certificate usage

The subscriber shall only use certificates and their associated key pairs for the purposes identified in this CPS and in applicable agreements with Telia.

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.

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)); or
c) Verification of digital signatures in connection with non-repudiation services (Key Usage Non-Repudiation (1)).

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

Alternative c) may not apply in combination with alternative a) or alternative b). If area of application c) (Non-Repudiation) is given in a certificate, this means that the certificate and its associated keys may only be used for non-repudiation services and is called Digital Signature certificate in this document.

Subscribers have to accept the Subscriber Agreement of Telia e-legitimation before receiving the EID card or hardware device with the private keys corresponding to the subscribers Telia e-legitimation.

For more information regarding appropriate subscriber key usage see section 1.4.1.

4.5.2 Relying party public key and certificate usage

Prior to accepting a Telia e-legitimation, 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 OCSP Responder in accordance with the requirements stated in this CPS. As part of this verification process the digital signature of the OCSP response should also be validated. If certificate status can't be received due to system failure or similar, the certificates shall not be accepted.

Telia will provide certificate status information identifying the access point to the OCSP responders in every certificate issued by Telia in accordance with this CPS.

All relying parties OCSP requests must be signed by a valid Relying Party certificate.
All OCSP responses will be signed by a private key corresponding to a public key certified by the CA for which the OCSP request is made. A separate key pair will be used for the responses of each CA.

4.6 *Certificate renewal*

Certificate renewal is not supported by Telia for any certificates issued according to this CPS.

To receive a new Telia e-legitimation the subscriber has to make a new application.

4.6.1 Circumstance for certificate renewal

Not applicable.

4.6.2 Who may request renewal

Not applicable.

4.6.3 Processing certificate renewal requests

Not applicable.

4.6.4 Notification of new certificate issuance to subscriber

Not applicable.

4.6.5 Conduct constituting acceptance of a renewal certificate

Not applicable.

4.6.6 Publication of the renewal certificate by the CA

Not applicable.

4.6.7 Notification of certificate issuance by the CA to other entities

Not applicable.

4.7 *Certificate re-key*

4.7.1 Circumstance for certificate re-key

No special routine exists for re-key of Telia e-legitimation certificates. Renewal of certificates and keys are ordered and delivered in the same way as the original Telia e-legitimation meaning, a new application for Telia e-legitimation has to be filed by the subscriber and hardware with new keys and certificates are delivered as well as new activation codes.

4.7.2 Who may request certification of a new public key

Re-key of CA's may be ordered by approved employees of the Telia eID services according to Telia routines.

4.7.3 Processing certificate re-keying requests

Not applicable.

4.7.4 Notification of new certificate issuance to subscriber

Not applicable.

4.7.5 Conduct constituting acceptance of a re-keyed certificate

Not applicable.

4.7.6 Publication of the re-keyed certificate by the CA

Not applicable.

4.7.7 Notification of certificate issuance by the CA to other entities

Not applicable.

4.8 *Certificate modification*

Certificate modification is not supported by Telia.

4.8.1 Circumstance for certificate modification

Not applicable.

4.8.2 Who may request certificate modification

Not applicable.

4.8.3 Processing certificate modification requests

Not applicable.

4.8.4 Notification of new certificate issuance to subscriber

Not applicable.

4.8.5 Conduct constituting acceptance of modified certificate

Not applicable.

4.8.6 Publication of the modified certificate by the CA

Not applicable.

4.8.7 Notification of certificate issuance by the CA to other entities

Not applicable.

4.9 *Certificate revocation and suspension*

Telia provides a revocation service available 24 hours/day. The revocation information can only be obtained through the Relying Party service. No other forms of revocation information are publically available. Telia does not provide temporary revocation (suspension) of certificates.

4.9.1 Circumstances for revocation

A Telia e-legitimation will be revoked:

a) When any subscriber information certified by the Telia e-legitimation changes;
b) Upon suspected or known compromise of the private key(s);
c) Upon suspected or known compromise of the card or device holding the private keys;
d) Upon suspected or known compromise of the activation codes used in connection with the private keys;
e) Upon termination of a subscriber; or
f) When a subscriber of a Company card or a SIS-approved Employee/Company card no longer is an employee or otherwise connected to the organization that issued the EID card.

Telia or an RA appointed by Telia in its discretion will revoke a certificate when an entity fails to comply with obligations set out in this CPS, any applicable agreement or applicable law.
Telia reserves the right to revoke a Telia e-legitimation at any time if Telia suspects that conditions may lead to a compromise of a subscriber's keys or certificates.

4.9.2 Who can request revocation

The revocation of a Telia e-legitimation may be requested by:

a) A subscriber whose name the Telia e-legitimation are issued under;
b) Personnel of an RA associated with Telia;
c) Personnel at the Subscriber's Employer, or another organization with which the subscriber has a business relation, if Telia e-legitimation is a part of a Company card or a SIS-approved Employee/Company card issued by that organization; or

d) Personnel at Telia.

4.9.3 Procedure for revocation request

Revocation requests are done according to section 3.4.

4.9.4 Revocation request grace period

On suspicion of a certificate being compromised or a certificate in any other way no longer is relevant for usage, the Telia e-legitimation subscriber must immediately make a revocation request for the Telia e-legitimation to Telia or any other RA appointed for the relevant service.

4.9.5 Time within which CA must process the revocation request

The process of handling an approved revocation request will take maximum 1 hour.

4.9.6 Revocation checking requirement for relying parties

Prior to accepting a Telia e-legitimation, a relying party is responsible to check the status of the certificate against the appropriate OCSP Responder in accordance with the requirements stated in this CPS. As part of this verification process the digital signature of the 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.

Telia will provide certificate status information identifying the access point to the OCSP responders in every Telia e-legitimation certificate issued by Telia.

4.9.7 CRL issuance frequency

CRL's are not publically available.

4.9.8 Maximum latency for CRL's

Not applicable.

4.9.9 On-line revocation/status checking availability

Telia provides on-line revocation status checking via the OCSP protocol.
The service is only accessible provided that the relying party has an agreement with Telia.
Availability of the service will be provided in the agreement.

4.9.10 On-line revocation checking requirements

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

4.9.11 Other forms of revocation advertisements available

Not applicable.

4.9.12 Special requirements re-key compromise

Not applicable.

4.9.13 Circumstances for suspension

Telia does not support suspension of certificates.

4.9.14 Who can request suspension

Not applicable.

4.9.15 Procedure for suspension request

Not applicable.

4.9.16 Limits on suspension period

Not applicable.

4.10 *Certificate status services*

4.10.1 Operational characteristics

The address to the OCSP responders is:

- Domain Name: ocsp.trust.telia.com
- Port number: 80

4.10.2 Service availability

The Relying Party services are usually available 24/7 all days of the year except for planned maintenance.

SLAs are not a part of this CPS. SLAs are agreed upon within the Relying party agreements or other customer agreements.

4.10.3 Optional features

Not applicable.

4.11 *End of subscription*

The termination of a subscription as a result of the subscriber no longer requiring the service, compromise of the private keys or activation codes, or termination of employment (voluntary or imposed, and only applicable in the case if the Telia e-legitimation is used for Company cards/hardware devices and SIS-approved Employee/Company cards according to section 1.3.2 b) and c)) will result in the immediate revocation of the certificate and updating of revocation information in the Relying Party services.

4.12 *Key escrow and recovery*

4.12.1 Key escrow and recovery policy and practices

Neither CA Private Signing Keys nor Subscribers private keys will be escrowed.

4.12.2 Session key encapsulation and recovery policy and practices

Not applicable.

5 FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

5.1 *Physical controls*

5.1.1 Site location and construction

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

All Telia 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 (54B/2014) 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.
b. Identifying key holders and ownership of the correct private key on electronic application. d. Electronic registration of key holders.
c. e. Revocation service for revoking certificates.
d. 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 Telia Operational Documentation. The security procedures are described in separate documentations belonging to the Telia 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

Telia 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. At least one of the security vaults 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 facility"	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 "Facility hallways"	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 common areas.	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 centre 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 authorisation 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 Telia'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 Telia RA systems are protected by four tiers of physical security, with access to the lower tier required before gaining access to the higher tier. 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 Telia 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 centre and the offline tier four key storage room.	The tier four data centre enforces individual access control through the use of two factor authentication. Authorisations for unescorted access to tier four are not given to any individuals. Physical access to tier four is automatically logged and video monitored. Offline keying material like RA-system key backups and secret shares are protected through the use of safes. Access to keying material is restricted in accordance with Telia's segregation of duties requirements. The opening and closing of the safes is logged for audit purposes.

5.1.3 Power and air conditioning

Telia 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

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

5.1.5 Fire prevention and protection

Telia has taken reasonable precautions to prevent and extinguish fires or other damaging exposure to flame or smoke. Telia'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 centres.

5.1.6 Media storage

All media containing production software and data, audit, archive, or backup information is stored within the Telia 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 Telia's normal waste disposal requirements.

5.1.8 Off-site backup

Telia 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*

Telia 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 enrolment 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.

Telia 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 Telia 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. Registration Officers also create new Customer accounts, privileges and values to enable Telia's self-service software for Customers.

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

5.2.2 Number of persons required per task

Telia 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 persons 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. If alarm is caused by a security supervisor only another security supervisor can inspect and accept the alarm.
- 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. If alarm is caused by a security supervisor only another security supervisor can inspect and accept the alarm
- Segregation of duties separates the role to install new CA and RA software from the role to activate CA and RA keys and vice versa. CAA role may have both rights but there are several compensating processes such as regular log comparison and configuration check and login alarm to verify that there doesn’t exist any non-controlled processes or certificates.

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

Telia 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

Telia 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 Telia 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 Telia personnel and to affiliate or partner company personnel if Telia 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, Telia 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 unfavourable 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

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

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

- Basic PKI concepts,
- Job responsibilities,
- Telia 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

Telia 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

Not applicable.

5.3.6 Sanctions for unauthorized actions

All employees and external resources working for Telia 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 Telia 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 Telia 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 Telia's secure facilities only to the extent that they are escorted and directly supervised by Trusted Persons.

5.3.8 Documentation supplied to personnel

Telia personnel involved in the operation of Telia 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

Telia 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; and
  - Cryptographic device lifecycle management events.
- CA, RA, Subscriber and system certificate life cycle management events, including:
  - Certificate requests, renewal, and re-key requests, and revocation;
  - All verification activities stipulated in these Requirements and the CA's Certification Practice Statement;
  - Date, time, phone number used, persons spoken to, and end results of verification telephone calls;
  - Acceptance and rejection of certificate requests;
  - Issuance of Certificates; and
  - Generation of Certificate Revocation Lists and OCSP entries.
- Security-related events including:
  - Successful and unsuccessful PKI system access attempts;
  - PKI and security system actions performed;
  - Security profile changes;
  - System crashes, hardware failures, and other anomalies;
  - Firewall and router activities; and
  - Entries to and exits from the CA facility.

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.

Telia 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 organisation and individual identity and authority

The following information concerning revocation requests is recorded at the Telia'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 unauthorized 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 continuously analyzed 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.

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

5.4.3 Retention period for audit log

Audit logs in accordance with section 5.4.1 are retained for at least seven years or longer if required by law for audit and compliance purposes.

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. Logging servers are protected from normal CA operators.

5.4.5 Audit log backup procedures

Audit logs are transferred online to at least two logging servers. Back-up copies of the system audit logs are made regularly according to defined schedules using offline storage media. 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 Telia 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, organisation, 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*

Telia 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 Telia 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

Telia CA will retain all documentation relating to certificate requests and the verification thereof, and all certificates and revocation thereof, for at least seven years, or longer if required by law, after any certificate based on that documentation ceases to be valid.

5.5.3 Protection of archive

The archives are stored also 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 Telia.

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

5.5.4 Archive backup procedures

Information to be archived is collected continuously from the places of origin and transferred to several online archives. Online archives are backed up regularly to offline archives.

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)

Telia is using internal archive systems and servers to collect archived information.

5.5.7 Procedures to obtain and verify archive information

Telia 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*

Telia 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. 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 c) 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*

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

5.7.1 Incident and compromise handling procedures

Telia 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 Telia has implemented disaster recovery plans.

Detailed instructions are provided in the Telia 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 Telia Security staff and Telia's incident handling procedures are initiated. Such procedures require appropriate escalation, incident investigation, and incident response. If necessary, Telia'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 Telia CA private key, Customer CA private key or the Telia infrastructure, Telia's Key Compromise Response procedures are followed. Detailed instructions are provided in the Telia Operation Procedures.

Telia undertakes, on suspicion that Telia 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 Telia 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 Telia 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 Telia's influence. Through Telia'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

Telia 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. Telia 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 canters located in different cities.

Telia maintains offsite backup of important CA information for CAs issued at the Telia'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 Telia CA or a Customers CA to cease operation, Telia 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, Telia 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

6.1.1 Key pair generation

6.1.1.1 Specific requirements for the CA's issuer keys

The CA's issuer keys are generated in FIPS 140-2 level 3 validated cryptographic 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. "Telia Root CA v1"). They are activated only when needed. Two privileged CA Officers are required to temporarily activate an offline key. The key ceremony of Webtrust audited CA keys is always witnessed by an independent party and/or videotaped for examination

6.1.1.2 Specific requirements for Subscriber private keys

The subscriber's private keys are stored on EID cards or other hardware devices. Key generation is carried out in batches before the certification of the keys takes place. Key generation takes place locally in the card's and devices chip, and the private keys never leave the chip.

Before key generation and initialization:

Non-initialized cards and devices are controlled and registered at the delivery from the hardware manufacturer and are kept in a vault with the delivery batches intact. The access to the vault with the non-initialized cards and devices is restricted in such a way that two persons need to be present when managing the cards.

The generation of private keys and personalization of eID Cards and hardware devices are done in batches and the batches are used in the order they have been initialized. Every step in the process is documented both electronically and on a printed report that follows the batch through all production steps.

After key generation and initialization:

Initialized but not personalized batches of cards and devices, and remaining cards and devices from partly used batches, are kept in the same vaults as the non-initialized cards and devices and managed under dual control.

After personalization:

Personalized cards and devices are always kept separated from non-personalized cards and devices.

There exist process descriptions regarding possible discrepancies at production failures, failures in the delivery processes and at the event of lost or defective cards and devices.

6.1.2 Private Key delivery to subscriber

EID cards and other hardware devices are distributed via registered mail, using a commercial delivery service and tamper evident packaging, usually to the RA where the application of Telia e-legitimation were made but may also be sent directly to the subscriber's home address depending of the service used. If the hardware device is sent directly to the subscriber his/her home address is verified against the Swedish SPAR register or equivalent register approved by Telia.

The activation data required to activate the device is communicated to the subscriber using an out of band process where the activation data is sent to the subscriber's home address according to the Swedish SPAR register or equivalent register approved by Telia.

Hardware devices not packed and sent the same day as they are personalized (due to lack of time) are locked into a vault until being sent the next working day.

The production systems don't allow the envelopes with activation data to be printed until two days after the hardware devices have been sent to the RA or subscriber. This prevents hardware devices and activation data from being present at the same time and place, neither at the hardware device manufacturer nor in the mail service being used.

The hardware devices are only handed out to the subscriber personally after the subscriber has been identified according to 3.2.3. This is stated in the notifying letter and in the RA routines according to the Telia issuer regulations.

The reception of the hardware device is signed by the subscriber. The signed receipt is kept for ten years after the expiration date of the Telia e-legitimation.

6.1.3 Public key delivery to certificate issuer

Subscribers and RAs submit their public key to Telia 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 Telia, this requirement is not applicable.

6.1.4 CA public key delivery to relying parties

Telia makes the CA certificates for Telia CAs and for Customer CAs, if the Customers so agrees, available to Subscribers and Relying Parties through the Telia CA Service repository https://cps.trust.telia.com or through the Telia CA Service LDAP directory.

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

Telia 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 4096 bits.

The subscribers' and operators' RSA keys are generated with a minimum length of 1024 bits.

1024 bit keys are still allowed due to known technical limitations of third party devices. Please note that this is subject to change in future revisions of this CPS when a minimum length of 2048 bits will be required for the subscribers' and operators' keys.

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 subscriber certificates contain information which defines suitable areas of application for the certificate and its associated keys. For more information regarding the subscriber key usage see section 4.5.1.

6.2 *Private Key Protection and Cryptographic Module Engineering Controls*

The subscriber's private keys are created and stored in the chip of EID cards or other hardware devices. The keys will be generated and protected in a cryptographic module rated to at least FIPS 140-2 Level 2. The protection profile, such as information structure and information access rights, of a card or device needs to be approved by Telia before it is allowed to issue a Telia e-legitimation to such a device.

The subscriber is required to protect its private key from disclosure according to the requirements as defined by Telia in the Subscriber Agreement for Telia e-legitimation.

Telia e-legitimation may be issued for a hardware device post production, i.e. the certificates are not issued at the initial personalization of the hardware device. This is allowed in the case that Telia definitely can verify that the subscriber's private keys, corresponding to the public keys certified, are protected in a hardware device that at least has the protection profile and has been created and handled according to the stipulations in this CPS. The subscribers agreements used must at least correspond to the demands stipulated in the Subscriber Agreements of Telia e-legitimation.

It is also a necessity that the primary certificates, issued for the subscriber keys of the hardware device, have been issued in a way and with content that the subscriber's identity can be uniquely verified via personnummer.

6.2.1 Cryptographic module standards and controls

Hardware protected private keys are created and stored in EID cards or other hardware devices. The keys will be generated and protected in a cryptographic module rated to at least FIPS 140-2 Level 2 regarding hardware and card OS.

The hardware devices used for the protection of the subscribers' private keys have the following characteristics:

Standards used	ISO 7816 in applicable parts.
Information structure (Electronic personalization)	Profile based on the Swedish standard SS 61 43 32 and file structure according to PKCS#15 or ISO 7816-15.

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

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

Telia 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

Telia does not escrow private keys.

6.2.4 Private Key backup

Telia 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 offline CA system.

6.2.5 Private Key archival

RA or CA private keys will be archived by Telia for disaster recovery purposes. Subscriber private keys may be archived by Telia if that is agreed with the customer and necessary to implement key restore.

6.2.6 Private Key transfer into or from a cryptographic module

Telia 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 Telia CA.

In addition, Telia 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 Telia RA requires the use of activation data as described in section 6.4.

Telia 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:

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 at least without physical access to the media. Old or broken CA key storage media may be temporarily stored in the protected CA environment.

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*

Initialization, personalization and generation of private keys for hardware devices takes place in a well protected area. Access to the area is granted individually and at least two persons have to be present in the area at all times. All access to the area is logged.

The certificate enrollment process for Telia's customers is done in systems separated from other production.

The production logs for production of the hardware devices includes information of all orders from RAs and are connected to personal data of the subscriber and chip-ID, card serial number and certificate serial numbers that have been generated in the production processes.

Routines are established to verify that visual information on the hardware device are corresponding to the information in the Telia e-legitimation connected to the private keys protected by the hardware device.

6.3.1 Public key archival

Telia retain archives of all verification public keys for the period of at least seven 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 twenty five years.

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 Telia 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

All subscribers' private keys are protected by PINs of at least six digits and a PUK of eight digits.

The subscribers' PUKs are stored encrypted at Telia, or a card manufacturer appointed by Telia, and can, if agreed in applicable agreements, be distributed to the subscriber's home address by registered mail after a separate request from the subscriber.

6.4.2 Activation data protection

The activation data required to use the private keys on the hardware device is communicated to the subscriber using an out of band process. The activation data is sent to the subscriber's home address according to the Swedish SPAR register or equivalent register approved by Telia.

Telia e-legitimation may not be used by any other person than the subscriber. If the subscriber suspects that another person may have knowldege of the activation data, the subscriber shall immediately make a revocation request for the Telia e-legitimation.

6.4.3 Other aspects of activation data

Not applicable.

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 Telia 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 6.6.2 Security management controls

The CA follows the policies defined by Telia'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 authorisation are applied and maintained.

6.6.3 Life cycle security controls

Telia has prevented developers to access production systems. Versions and releases are separated from each other using software management tools designed to this purpose. Each update to production is approved and documented.

6.7 *Network security controls*

Firewalls have been implemented to restrict access to the Telia CA equipment. Only specified traffic allowed through network boundary controls such as protocols and ports required by Telia CA's operations.

Essential information exchange between the RA and Telia 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.

Telia CA services are secured by two-factor authentication through VPN to protect data and systems from unauthorized personnel. Suspicious login attempts or activities will be monitored and alerted by the IDS.

6.8 *Time-stamping*

The system time on Telia CA computers is updated using the Network Time Protocol (NTP) to synchronize system clocks. The used Telia NTP servers are using time where quality is on level Stratum-2.

7 CERTIFICATE AND OCSP PROFILES

7.1 *Certificate profile*

7.1.1 Version number(s)

All issued certificates are X.509 Version 3 certificates, in accordance with RFC 5280 “Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile” and as specified in this section. The content of the certificates follows the Swedish standard SS 61 43 31 “Identification Cards – Electronic ID Certificate”, the certificate profile for SIS-approved identification cards.

7.1.2 Certificate extensions

The following certificate extensions will be used in accordance with RFC 5280 and SS 61 43 31. The extensions are mandatory except for Authority Key Identifier which is optional in self-signed CA certificates.

Standard Certificate Extensions for CA certificates

Extension	**Critical**	**Value/Comments**
Authority Key Identifier	non-critical	SHA-1 (hash of Issuing CA’s public key)
Basic Constraints	critical	Subject Type=’CA’ Path Length depending on the depth of the Issuer chain. If the CA is a self-signed CA the Basic Constraints is set to ‘0’.
Subject Key Identifier	non-critical	SHA-1 (hash of Issued CA’s public key)
Key Usage	non-critical	The keyUsage is set to ‘keyCertSign’ and ‘cRLSign’.

Standard Certificate Extensions for Subscriber certificates

Extension	**Critical**	**Value/Comments**
Authority Information Access	non-critical	‘http://ocsp.trust.telia.com’
Authority Key Identifier	non-critical	SHA-1 (hash of Issuing CA’s public key)
Certificate Policies	non-critical	PolicyIdentifier=’1.2.752.35.1.4’ Policy Qualifier Id=CPS Qualifier: ‘https://repository.trust.telia.com’
Subject Key Identifier	non-critical	SHA-1 (hash of Subject’s public key)
Key Usage	critical	Telia e-legitimation consists of two certificates with different key usage. The keyUsage is set to the following in the certificates: - ‘nonRepudiation’ - ‘digitalSignature’ and ‘keyEncipherment’

Private Certificate Extension for Subscriber certificates

A private extension is used to indicate the card serial number of the EID card or hardware device where the subscriber’s private keys are protected. The SEIS Card Number extension contains the ISO 7812 serial number of a card or device in a printable string.
The object identifier of the SEIS Card Number extension is {1.2.752.34.2.1}.

Extension	**Critical**	**Value/Comments**
SEIS Card Number (1.2.752.34.2.1)	non-critical	Card serial number. Private extension according to SS 61 43 31.

Standard Certificate Extensions for OCSP signer certificates

Extension	Critical	Value/Comments
Authority Key Identifier	non-critical	SHA-1 (hash of Issuing CA's public key)
Extended Key Usage	non-critical	'OCSPSigning'
Subject Key Identifier	non-critical	SHA-1 (hash of Subject's public key)
Key Usage	critical	'digitalSignature'

Private Certificate Extension for OCSP signer certificates

The private extension ocsp-nocheck is used for the OCSP signer certificates according to RFC6960 "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol".

Extension	Critical	Value/Comments
id-pkix-ocsp-nocheck (1.3.6.1.5.5.7.48.1.5)	non-critical	Private extension according to RFC6960.

7.1.3 Algorithm object identifiers

The RSA algorithm is used in combination with the SHA-1 hash algorithm for signing and verification of the certificates. The following object identifier is used in the certificates signature algorithm field: Sha1withRSAEncryption OBJECT IDENTIFIER ::== iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 5; {1.2.840.113549.1.1.5}.

7.1.4 Name forms

Every DN will be in the form of an X.501 DirectoryString.

7.1.5 Name constraints

Subject and Issuer DNs comply with PKIX standards and are present in all certificates.
The name fields used are Issuer Distinguished Name and Subject Distinguished Name.
All attributes are mandatory except for organizational Unit which is optional.

Attributes used in Issuer Distinguished Name

Attribute	Encoding	Value
country (C)	PrintableString	'SE'
organization (O)	UTF8String	'TeliaSonera Sverige AB'
organizational unit (OU)	UTF8String	
common name (CN)	UTF8String	Name of CA

Attributes used in Subject Distinguished Name

Attribute	Encoding	Value
country (C)	PrintableString	'SE'
given name (G)	UTF8String	All given names of the subscriber
surname (S)	UTF8String	All surnames of the subscriber
serial number (SN)	PrintableString	Subscriber's Personnummer in the form 'YYYYMMDDNNNC'
common name (CN)	UTF8String	Combination of given name and surname of the subscriber.

Attributes used in Subject Distinguished Name of CA certificates

Attribute	Encoding	Value
country (C)	PrintableString	'SE'
organization (O)	UTF8String	'TeliaSonera Sverige AB'
organizational unit (OU)	UTF8String	
common name (CN)	UTF8String	Name of CA

Attributes used in Subject Distinguished Name of OCSP signer certificates

Attribute	Encoding	Value
country (C)	PrintableString	'SE'
organization (O)	PrintableString	'TeliaSonera Sverige AB'
organizational unit (OU)	PrintableString	OU of issuing CA if present
common name (CN)	PrintableString	CN of issuing CA followed by the word 'OCSP Responder'

7.1.6 Certificate policy object identifier

The certificate policy object identifier will be present in issued certificates and will contain the OID of this CPS according to section 1.2.

7.1.7 Usage of Policy Constraints extension

Not applicable.

7.1.8 Policy qualifiers syntax and semantics

The policy qualifier CPSuri is used in the subscriber certificates. The value of the CPSuri points to Telia eID Services repository web site where this CPS is published.

7.1.9 Processing semantics for the critical Certificate Policies extension

Not applicable.

7.2 *CRL profile*

7.2.1 Version number(s)

Certificate status control is only available via the OCSP responders in Telia Relying Party service.

7.2.2 CRL and CRL entry extensions

Not applicable.

7.3 *OCSP profile*

7.3.1 Version number(s)

Version 1 of the OCSP specification as defined by RFC6960 "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol" is implemented for the OCSP responders.

7.3.2 OCSP extensions

The OCSP Nonce extension should be used in OCSP requests.

8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS

8.1 *Frequency or circumstances of assessment*

Every third year a Compliance Audit will be performed by an independent, qualified third party.

Telia makes periodical audits of the RAs compliancy with this CPS. The RAs are contractually bound to follow the regulations stated in Telia's card issuer policies, see section 1.3.2, where for instance applicable RA obligations from this CPS and other regulations are mentioned.

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. The Compliance Auditor should perform such compliance audits as his/her primary responsibility.

8.3 *Assessor's relationship to assessed entity*

The Compliance Auditor should not have any financial, legal or organizational relationship with the audited party. A person cannot be Compliance Auditor if he/she:

a) Is owner to or joint owner to Telia or another company within the same group;
b) Is a member of the Telia management or the management of any subsidiary, or assists with Telia's bookkeeping or management of means, or Telia's control of them, or managing the issues regarding information security;
c) Is employed by or in other aspects in subordinate or dependant relation to Telia or any other company referred to in a) and b) above;
d) Is married to or co-habiter with or is sibling or close relative to a person that is referred to in a) and b) above; or
e) Is in debt to Telia or any other company referred to in a) to c) above.

8.4 *Topics covered by assessment*

The purpose of the Compliance Audit is to verify that all routines and processes used for issuing of Telia e-legitimation complies to this CP and CPS.
The audit includes the work that is performed by Telia and engaged RAs and subcontractors. The Compliance Audit will cover all requirements that define the operation of a CA and RA under this CPS, for instance:

- The CA production integrity (key and certificate life cycle management);
- CA and RA environmental controls; and
- CA and RA procedures.

8.5 *Actions taken as a result of deficiency*

If deficiencies are discovered, they will be reported to the Telia CPS Management Team (CPSMT). The CPSMT is responsible for acting upon the flaws and faults discovered during the compliance audit.

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. This may result in updated information to and education of CA and RA personnel and/or changes in applied procedures;
b) The Compliance Auditor may meet with Telia and determine if the deficiency can be remedied and an action plan will be developed, and steps taken to remedy the deficiency. Such steps could be to change applied procedures and/or updating this CPS; or
c) The Compliance Auditor may report the deficiency and if the Telia eID Services deems the deficiency to have risk to the operation of a CA, Telia eID Service management may decide to take the CA out of operation.

Should this CPS be updated in such a way that the new CPS is deemed to involve a change of security level a new CPS with a new identity shall be created (see section 1.2).

8.6 *Communication of results*

The Compliance Auditor shall provide the Telia eID Service management and the CPSMT 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 agreements.

9.1.1 Certificate issuance or renewal fees

See section 9.1.

9.1.2 Certificate access fees

See section 9.1.

9.1.3 Revocation or status information access fees

See section 9.1.

9.1.4 Fees for other services

See section 9.1.

9.1.5 Refund policy

See section 9.1.

9.2 *Financial responsibility*

Telia will maintain adequate levels of insurance necessary to support its business practices.

The issuing of Telia e-legitimation in accordance to this CPS does not mean Telia shall be seen as an agent, proxy or as a representative of the subscriber or the relying party.

9.2.1 Insurance coverage

Telia will maintain, at its own expense, insurance necessary to support its business practices.

9.2.2 Other assets

No stipulation.

9.2.3 Insurance or warranty coverage for end-entities

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

9.3 *Confidentiality of business information*

9.3.1 Scope of confidential information

Information which is not excluded in section 9.3.2, or otherwise defined as public in this CPS, shall be treated as confidential and not be disclosed without the consent of the subscriber or other agreement parties involved.

Examples of confidential information are:

a) Personal and corporate information, not appearing in certificates and in public directories, held by Telia or an RA, e.g. registration and revocation information, logged events, correspondence between the subscriber and Telia;
b) All generated private and secret keys;
c) Activation codes; and
d) Audit information

Any request for the disclosure of information shall be signed and delivered in writing to Telia.

Any disclosure of information is subject to the requirements of Swedish privacy laws.
No information regarding the subscribers' private keys are kept by Telia and are therefore impossible to be disclosed even if decided by a court of law.

9.3.2 Information not within the scope of confidential information

The following information is not deemed to be confidential:

a) Issued certificates including public keys;
b) OCSP responses;
c) Subscriber terms and conditions;
d) This CPS;
e) Information that is documented by the receiving party as having been independently developed by it without unauthorized reference to or reliance on the confidential information of the disclosing party;
f) Information that the receiving party lawfully receives free of restriction from a source other than the disclosing party;
g) Information that is or becomes generally available to the public through no wrongful act or omission on the part of the receiving party; and
h) Information that at the time of disclosure to the receiving party was known to the receiving party free of restriction as evidenced by documentation in the receiving party's possession; or
Information that the disclosing party agrees in writing is free of restrictions.

Exceptions may apply to subscriber information if this is stated in a specific agreement between Telia and the subscriber's employer or any other organization from which the subscriber has received a Telia e-legitimation.

In case the RA is a Swedish government some otherwise confidential information, i.e. information regarding the subscriber's application and reception of Telia e-legitimation, may be rated public according to the Swedish Constitution's "principle of public access to official records".

9.3.3 Responsibility to protect confidential information

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

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

Telia will disclose confidential information if a court of law or any other legal authority subject to Swedish law so decides. Private keys linked to issued certificates cannot be supplied since no private key information is stored by Telia or any of Telia's subcontractors.

9.4 *Privacy of personal information*

9.4.1 Privacy plan

Telia will not disclose any personal information as long as the information is not considered public and unless it is required by law.

In general, all information not stated in 9.4.3 is treated as private and will not be disclosed by Telia without the consent of the subscriber or the subscriber's employer (if the Telia e-legitimation has been received as part of a Company card or a SIS-approved Employee/Company card).

Telia will treat all the subscriber information in accordance with the Subscriber Agreement.

9.4.2 Information treated as private

Telia will treat the following information as being private:

a) Registration information;
b) Application and reception forms;
c) Private keys;
d) Activation codes;
e) Correspondence between Telia and the subscriber; and
f) Logged events.

In case the RA is a Swedish government some otherwise private information, i.e. information regarding the subscriber's application and reception of Telia e-legitimation, may be rated public according to the Swedish Constitution's "principle of public access to official records".

No information regarding the subscribers' private keys are kept by Telia and are therefore impossible to be disclosed even if decided by a court of law.

9.4.3 Information not deemed private

Publicly available information such as:

a) Issued certificates including public keys;
b) OCSP revocation information; and
c) Other information normally regarded as being public,

is not considered as being private information.

9.4.4 Responsibility to protect private information

See section 9.3.3.

9.4.5 Notice and consent to use private information

Private personal information will only be utilized without prior consent as per section 9.4.1.

9.4.6 Disclosure pursuant to judicial or administrative process

Private personal information will only be disclosed if required by law as per section 9.4.1.

Any request for the disclosure of private information will be signed by the requester and delivered in writing to Telia or an RA appointed by Telia. Any disclosure of private information is subject to the requirements of Swedish privacy laws and applicable organizational policy.

9.4.7 Other information disclosure circumstances

No stipulation.

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 Swedish Copyright Act, 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 (electronically, mechanically, photocopied, recorded or similar) without written permission from Telia Sverige 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 Telia in accordance with section 1.5.2.

9.6 *Representations and warranties*

A CA will issue and revoke certificates, operate its certification and repository services, and provide certificate status information in accordance with this CPS. Authentication and validation procedures will be implemented as set forth in Section 3 of this CPS.

9.6.1 CA representations and warranties

Telia will operate in accordance with this CPS, when issuing and managing Telia e-legitimation Telia will require that all the RAs operating on its behalf will comply with the relevant provisions of this CPS concerning the operations of the RAs. Telia will take commercially reasonable measure 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 Telia e-legitimation. Subscribers will be notified as to procedures for dealing with suspected key compromise and service cancellation.

When Telia delivers or publishes a Telia e-legitimation, Telia declares that it has issued a Telia e-legitimation to a subscriber and that the information stated in the Telia e-legitimation has been verified in accordance with this CPS.

Telia warrants that the information in the Telia e-legitimation issued by Telia is checked and verified in accordance with the routines that have been stated in this CPS. In the case Telia uses a subcontractor to perform parts of the service, Telia is responsible as if Telia had performed the tasks itself.

Telia's liability is limited to what is stated in the, at each point in time, valid Terms and conditions for Telia e-legitimation.

9.6.2 RA representations and warranties

Telia will require that all RA Administrators comply with the relevant provisions of this CPS.

The RA Administrator is responsible for the identification and authentication of subscribers following section 3.1 and section 4.1.

Telia and RAs will through their RA personnel make available Subscriber Agreements to the subscribers.

RA Administrators are individually accountable for actions performed on behalf of an RA. Individual 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.

All RA personnel are provided with an EID card which gives access 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.

In the case Telia hires a subcontractor to perform parts of the service, Telia is to be held responsible as if Telia itself had performed the tasks.

9.6.3 Subscriber representations and warranties

Telia will require that all subscribers of Telia e-legitimation comply with the relevant provisions of this CPS.

The subscriber is bound through a contract with Telia and will need to accept the Subscriber Agreement when applying for or before receiving Telia e-legitimation.

Subscribers are required to protect their private keys, associated passwords and tokens, as applicable, in accordance with the Subscriber Agreement, and to take all commercially reasonable measures to prevent their loss, disclosure, modification, or unauthorized use.

The subscriber shall only use the keys and certificates for the purposes identified in this CPS and in the Subscriber Agreement.

When a subscriber suspects a private key compromise, the subscriber shall notify Telia in the manner specified in the Subscriber Agreement.

9.6.4 Relying party representations and warranties

Telia will require that relying parties comply with all the relevant provisions of this CPS.

Prior to accepting a Telia e-legitimation, 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 OCSP Responder in accordance with the requirements stated in this CPS. As part of this verification process the digital signature of the 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 to decide whether the security level of the issuance process is appropriate for the actual application where to be used.

Telia will provide certificate status information identifying the access point to the on-line certificate status server in every certificate Telia issues in accordance with section 4.9.6 and 4.9.9.

9.6.5 Representations and warranties of other participants

No stipulation.

9.7 *Disclaimers of warranties*

Telia warrants that the information in the Telia e-legitimation issued by Telia is checked and verified in accordance with the routines that have been stated in this CPS. In the case Telia uses a subcontractor to perform parts of the service, Telia is responsible as if Telia itself had performed the tasks.

Telia's liability is limited to what is stated in the, at each point in time, valid Terms and conditions for Telia e-legitimation.

9.8 *Limitations of liability*

Telia warrants that the information in the Telia e-legitimation issued by Telia is checked and verified in accordance with the routines that have been stated in this CPS. In the case Telia uses a subcontractor to perform parts of the service, Telia is responsible as if Telia itself had performed the tasks.

Telia's liability is limited to what is stated in the, at each point in time, valid Terms and conditions for Telia e-legitimation.

9.9 *Indemnities*

The Subscriber Agreement regulates all questions regarding indemnities. The customer accepts the Subscriber Agreement at the same time as he/she applies for a Telia e-legitimation or before receiving the Telia e-legitimation.

9.10 *Term and termination*

9.10.1 Term

This CPS remains in force until notice of the opposite is communicated by Telia on the Telia eID Service Repository web site (https://repository.trust.telia.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 at the Telia eID Service Repository web site (https://repository.trust.telia.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*

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

9.12 *Amendments*

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

All changes to this CPS shall be consistent with the certificate policy or policies identified in section 1.2.

9.12.1 Procedure for amendment

CPS publication will be done in accordance with Section 2.

An electronic copy of this CPS is to be made available at the Telia eID Services Repository web site (https://repository.trust.telia.com), or by requesting an electronic copy by e-mail to the contact representative as described in Section 1.5.

The CPSMT may provide notice, in writing, of any proposed changes to this CPS, if in the judgment and discretion of CPSMT the changes may have significant impact on the issued certificates, or Telia eID services.

The period of time that affected parties have to conform to the change will be defined in the notification.

9.12.2 Notification mechanism and period

The following changes can be carried out to this CPS without notification:

- Linguistic amendments and rearrangements which do not affect the security level of the described procedures and regulations;
- Changes in contact information; and
- Changes in URI information.

Changes which shall take place with notification:

a) All types of changes can be made to this CPS 45 days after notification; or
b) Minor changes of lesser importance and which affect only a small number of subscribers or relying parties may be made 30 days after notification.

The notification shall contain a statement of proposed changes, the final date for receipt of comments, and the proposed effective date of the changes. CPSMT will post the notification at the Telia eID Services Repository web site (https://repository.trust.telia.com).

In term of changes in accordance with a) comments should be received no later than 35 days after publication of notification.

In term of changes in accordance with b) comments should be received no later than 20 days after publication of notification.

CPSMT 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 30 days after publication of a new modified notification.

9.12.3 Circumstances under which OID must be changed

If a CPS change is determined by CPSMT to warrant the issuance of a new CPS, CPSMT will assign a new Object Identifier (OID) for the new CPS.

9.13 *Dispute resolution provisions*

If a dispute relating to this CPS is not successfully resolved through negotiations the dispute shall be decided in one of the following ways.

Disputes between Telia and a subscriber, i.e. a possessor of a Telia e-legitimation shall be decided according to Swedish law and Swedish court.

A dispute between Telia and any other party than the subscriber, i.e. an RA or relying party, shall be settled by arbitration in accordance with the Reconciliation and Arbitration Rules of the International Chamber of Commerce (ICC). The Stockholm Chamber of Commerce shall administer the reconciliation in accordance with the ICC's rules, and the venue for arbitration shall be Stockholm. The proceedings shall be held in Swedish unless the parties agree on something else.

9.14 *Governing law*

Swedish law shall apply to the interpretation of this CPS, if not otherwise agreed, and in assessing Telia's actions in relation to the issuing of Telia e-legitimation in accordance with this CPS.

9.15 *Compliance with applicable law*

Telia will 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

Telia 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, or other similar causes beyond its reasonable control and without the fault or negligence of Telia or its subcontractors.

9.17 *Other provisions*

No stipulation.

Acronyms and Definitions

Acronyms

CA	Certification Authority
CP	Certificate Policy
CPS	Certification Practice Statement
CPSMT	Telia CPS Management Team
CRL	Certificate Revocation List
DN	Distinguished Name
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
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
SPAR	Swedish Population Address Register
SSL	Secure Sockets Layer
TTP	Trusted Third Party
URI	Uniform Resource Identifier

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.

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.

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.

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.

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.

Distinguished Name (DN):
Every entry in a X.500 or LDAP directory has a Distinguished Name, or DN. It is a unique entry identifier throughout 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 Identification Card in the form of an active card containing certificates and private keys where the visual parts of the card may be used as a visual ID document.

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.

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.

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.

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 organization, an organizational 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.

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

Personnummer:
Swedish social security number. The personnummer consists of the individual's birth date followed by three digits and one check digit.

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.

PKCS#15
Cryptographic Token Information Format Standard from RSA Laboratories.
PKCS #15 establishes a standard that enables users in to use cryptographic tokens to identify themselves to multiple, standards-aware applications, regardless of the application's cryptoki (or other token interface) provider.

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.

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.

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.

Subscriber:
A subscriber is an entity; a person or application server that is a holder of a private key corresponding to a public and has been issued a certificate. In the case of an application server, a person authorized by the organization owning the application server may be referred to as the subscriber. A subscriber is capable of using, and is authorized to use, the private key that corresponds to the public key listed in the certificate.

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.

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 dependent 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 universal character / 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.

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:
Initially a specification of the directory service required to support X.400 e-mail but commonly used by other applications as well.

X.509:
An ISO standard that describes the basic format of digital certificates.

References

RFC 3647
An IETF framework document providing a list of topics that potentially need to be covered in a Certificate policy or a certification practice statement.
Provided by IETF, http://www.ietf.org.

RFC 5280
Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
Provided by IETF, http://www.ietf.org.

RFC 6960
X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP.
Provided by IETF, http://www.ietf.org.

ETSI TS 10145
Policy requirements for certification authorities issuing qualified certificates
Provided by ETSI, http://www.etsi.org.

SBC 151-U
"Särskilda Bestämmelser för certifiering av överenstämmels med standard SS 61 43 14" (Special Regulations for certification of compliance with standard SS 61 43 14)
Provided by Det Norske Veritas, http://www.detnorskeveritas.se.

SS 61 43 14
Identifieringskort - Identitetskort av typ ID-1 (Identity cards – Identification cards of typ ID-1)
Provided by SIS (Swedish Standards Institute), http://www.sis.se.

SS 61 43 31
Identification cards - Electronic ID certificate
Provided by SIS (Swedish Standards Institute), http://www.sis.se.

SS 61 43 32
Identification Cards - Electronic ID Card - Swedish Profile
Provided by SIS (Swedish Standards Institute), http://www.sis.se.

Telia RA policies:
Telias policy för utfärdande av ID-kort med e-legitimation (Telia's policy for issuing of identification cards with e-legitimation)
Provided by Telia, https://repository.trust.telia.com.

Telias policy för utfärdande av företagskort med e-legitimation (Telia's policy for issuing of company cards with e-legitimation)
Provided by Telia, https://repository.trust.telia.com.