Inera Certification Practice Statement for

SITHS PKI

Version 0.9
Revision date 2024-01-19

DRAFT

Copyright © Inera AB

No part of this document may be reproduced, modified or distributed in any form or by any means, in whole or in part, or stored in a database or retrieval system, without prior written permission of Inera.

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.

Revision History

Version	Author	Comment	Effective Date
0.5	Niclas Abramsson, Inera AB	Document created	2023-12-08
0.6	Niclas Abramsson, Inera AB	Commented draft	2024-01-05
0.9	Stéphane Kunegel, Inera AB	Final draft for review	2024-01-19

Contents

1 INTRODUCTION 11
1.1 Overview 11
1.2 Document name and identification 11
1.3 PKI participants 11
1.3.1 Certification authorities 11
1.3.2 Registration authorities 12
1.3.3 Subscribers 12
1.3.4 Relying parties 12
1.3.5 Other participants 13
1.4 Certificate usage 13
1.4.1 Appropriate certificate uses 13
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 14
1.5.4 CPS approval procedures 14
1.6 Definitions and acronyms 14
2 PUBLICATION AND REPOSITORY RESPONSIBILITIES 14
2.1 Repositories 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 16
3.1.6 Recognition, authentication, and role of trademarks 16
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 17
3.2.5 Validation of authority 17
3.2.6 Criteria for interoperation 17
3.3 Identification and authentication for re-key requests 17
3.4 Identification and authentication for revocation request 18
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 19
4.2.1 Performing identification and authentication functions 19
4.2.2 Approval or rejection of certificate applications 19
4.2.3 Time to process certificate applications 19
4.3 Certificate issuance 19
4.3.1 CA actions during certificate issuance 19
4.3.2 Notification to subscriber by the CA of issuance of certificate 19
4.4 Certificate acceptance 19
4.4.1 Conduct constituting certificate acceptance 19
4.4.2 Publication of the certificate by the CA 20
4.4.3 Notification of certificate issuance by the CA to other entities 20
4.5 Key pair and certificate usage 20
4.5.1 Subscriber private key and certificate usage 20
4.5.2 Relying party public key and certificate usage 20
4.6 Certificate renewal 20
4.7 Certificate re-key 20
4.8 Certificate modification 20
4.9 Certificate revocation and suspension 20
4.9.1 Circumstances for revocation 20
4.9.2 Who can request revocation 21
4.9.3 Procedure for revocation request 21
4.9.4 Revocation request grace period 21
4.9.5 Time within which CA must process the revocation request 22
4.9.6 Revocation checking requirement for relying parties 22
4.9.7 CRL issuance frequency 22

4.9.8 Maximum latency for CRLs 22
4.9.9 On-line revocation/status checking availability 22
4.9.10 On-line revocation checking requirements 23
4.9.11 Other forms of revocation advertisements available 23
4.9.12 Special requirements re key compromise 23
4.9.13 Circumstances for suspension 23
4.9.14 Who can request suspension 23
4.9.15 Procedure for suspension request 23
4.9.16 Limits on suspension period 23
4.10 Certificate status services 23
4.10.1 Operational characteristics 23
4.10.2 Service availability 23
4.10.3 Optional features 23
4.11 End of subscription 23
4.12 Key escrow and recovery 24
5 FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS 24
5.1 Physical controls 24
5.1.1 Site location and construction 24
5.1.2 Physical access 25
5.1.3 Power and air conditioning 27
5.1.4 Water exposures 27
5.1.5 Fire prevention and protection 28
5.1.6 Media storage 28
5.1.7 Waste disposal 28
5.1.8 Off-site backup 28
5.2 Procedural controls 28
5.2.1 Trusted roles 28
5.2.2 Number of persons required per task 29
5.2.3 Identification and authentication for each role 30
5.2.4 Roles requiring separation of duties 31
5.3 Personnel controls 31
5.3.1 Qualifications, experience, and clearance requirements 31
5.3.2 Background check procedures 31
5.3.3 Training requirements 32
5.3.4 Retraining frequency and requirements 32

5.3.5 Job rotation frequency and sequence 32
5.3.6 Sanctions for unauthorized actions 32
5.3.7 Independent contractor requirements 32
5.3.8 Documentation supplied to personnel 33
5.4 Audit logging procedures 33
5.4.1 Types of events recorded 33
5.4.2 Frequency of processing log 34
5.4.3 Retention period for audit log 34
5.4.4 Protection of audit log 34
5.4.5 Audit log backup procedures 34
5.4.6 Audit collection system (internal vs. external) 34
5.4.7 Notification to event-causing subject 34
5.4.8 Vulnerability assessments 35
5.5 Records archival 35
5.5.1 Types of records archived 35
5.5.2 Retention period for archive 35
5.5.3 Protection of archive 35
5.5.4 Archive backup procedures 36
5.5.5 Requirements for time-stamping of records 36
5.5.6 Archive collection system (internal or external) 36
5.5.7 Procedures to obtain and verify archive information 36
5.6 Key changeover 36
5.6.1 Self-Signed CA 36
5.6.2 CA Hierarchies 36
5.7 Compromise and disaster recovery 37
5.7.1 Incident and compromise handling procedures 37
5.7.2 Computing resources, software, and/or data are corrupted 37
5.7.3 Entity private key compromise procedures 37
5.7.4 Business continuity capabilities after a disaster 38
5.8 CA or RA termination 38
6 TECHNICAL SECURITY CONTROLS 39
6.1 Key pair generation and installation 39
6.1.1 Key pair generation 39
6.1.2 Private key delivery to subscriber 39
6.1.3 Public key delivery to certificate issuer 40

6.1.4 CA public key delivery to relying parties 40
6.1.5 Key sizes 40
6.1.6 Public key parameters generation and quality checking 40
6.1.7 Key usage purposes (as per X.509 v3 key usage field) 40
6.2 Private Key Protection and Cryptographic Module Engineering Controls 40
6.2.1 Cryptographic module standards and controls 41
6.2.2 Private key (n out of m) multi-person control 41
6.2.3 Private key escrow 41
6.2.4 Private key backup 41
6.2.5 Private key archival 41
6.2.6 Private key transfer into or from a cryptographic module 41
6.2.7 Private key storage on cryptographic module 42
6.2.8 Method of activating private key 42
6.2.9 Method of deactivating private key 42
6.2.10 Method of destroying private key 42
6.2.11 Cryptographic Module Rating 43
6.3 Other aspects of key pair management 43
6.3.1 Public key archival 43
6.3.2 Certificate operational periods and key pair usage periods 43
6.4 Activation data 43
6.4.1 Activation data generation and installation 43
6.4.2 Activation data protection 44
6.4.3 Other aspects of activation data 44
6.5 Computer security controls 44
6.5.1 Specific computer security technical requirements 44
6.5.2 Computer security rating 44
6.6 Life cycle technical controls 44
6.6.1 System development controls 44
6.6.2 Security management controls 44
6.6.3 Life cycle security controls 45
6.7 Network security controls 45
6.8 Time-stamping 45
7 CERTIFICATE, CRL, AND OCSP PROFILES 46
7.1 Certificate profile 46
7.1.1 Version number(s) 46

7.1.2 Certificate extensions 46
7.1.3 Algorithm object identifiers 46
7.1.4 Name forms 46
7.1.5 Name constraints 46
7.1.6 Certificate policy object identifier 46
7.1.7 Usage of Policy Constraints extension 46
7.1.8 Policy qualifiers syntax and semantics 46
7.1.9 Processing semantics for the critical Certificate Policies extension 46
7.2 CRL profile 46
7.2.1 Version number(s) 47
7.2.2 CRL and CRL entry extensions 47
7.3 OCSP profile 48
7.3.1 Version number(s) 48
7.3.2 OCSP extensions 48
8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS 49
8.1 Frequency or circumstances of assessment 49
8.2 Identity/qualifications of assessor 49
8.3 Assessor's relationship to assessed entity 49
8.4 Topics covered by assessment 49
8.5 Actions taken as a result of deficiency 49
8.6 Communication of results 49
9 OTHER BUSINESS AND LEGAL MATTERS 49
9.1 Fees 49
9.1.1 Certificate issuance or renewal fees 49
9.1.2 Certificate access fees 49
9.1.3 Revocation or status information access fees 49
9.1.4 Fees for other services 49
9.1.5 Refund policy 49
9.2 Financial responsibility 50
9.2.1 Insurance coverage 50
9.2.2 Other assets 50
9.2.3 Insurance or warranty coverage for end-entities 50
9.3 Confidentiality of business information 50
9.3.1 Scope of confidential information 50
9.3.2 Information not within the scope of confidential information 50

9.3.3 Responsibility to protect confidential information 50
9.4 Privacy of personal information 50
9.4.1 Privacy plan 50
9.4.2 Information treated as private 51
9.4.3 Information not deemed private 51
9.4.4 Responsibility to protect private information 51
9.4.5 Notice and consent to use private information 51
9.4.6 Disclosure pursuant to judicial or administrative process 51
9.4.7 Other information disclosure circumstances 51
9.5 Intellectual property rights 51
9.6 Representations and warranties 51
9.6.1 CA representations and warranties 51
9.6.2 RA representations and warranties 52
9.6.3 Subscriber representations and warranties 52
9.6.4 Relying party representations and warranties 53
9.6.5 Representations and warranties of other participants 53
9.7 Disclaimers of warranties 53
9.8 Limitations of liability 53
9.9 Indemnities 53
9.10 Term and termination 54
9.10.1 Term 54
9.10.2 Termination 54
9.10.3 Effect of termination and survival 54
9.11 Individual notices and communications with participants 54
9.12 Amendments 54
9.12.1 Procedure for amendment 54
9.12.2 Notification mechanism and period 54
9.12.3 Circumstances under which OID must be changed 55
9.13 Dispute resolution provisions 55
9.14 Governing law 55
9.15 Compliance with applicable law 55
9.16 Miscellaneous provisions 55
9.16.1 Entire agreement 55
9.16.2 Assignment 55
9.16.3 Severability 55

9.16.4 Enforcement (attorneys' fees and waiver of rights) 55
9.16.5 Force Majeure 55
9.17 Other provisions 55
Appendix A. Acronyms 56
Appendix B. Definitions 57

1 INTRODUCTION

1.1 Overview

The purpose of this CPS is to describe the procedures the CA uses when issuing certificates, and that all Registration Authorities, Subscribers, Subjects, and Relying Parties shall follow in connection with these certificates. This document defines the Certification Practice Statement for the following CAs:

- SITHS e-id Root CA v2
    - SITHS e-id Person ID 3 CA v1
    - SITHS e-id Person HSA-id 3 CA v1
    - SITHS e-id Person ID 2 CA v1
    - SITHS e-id Person HSA-id 2 CA v1
    - SITHS e-id Function CA v1
    - SITHS e-id Person ID Mobile CA v1
- SITHS e-id Card Identifier CA v1

This CPS describes the procedures and routines, which apply when completing a certificate for individuals, organizations, functions and devices and for revoking and revocation checking of such certificates. This CPS lay out how Inera AB conform to SITHS Certificate Policy (CP).

This CPS generally conforms to the Internet Engineering Task Force (IETF):

- RFC 3647 for Certificate Policy and Certification Practices Statement.
- RFC 2119 Key words for use in RFCs to Indicate Requirement Levels.

1.2 Document name and identification

This CPS is titled “Inera Certification Practice Statement for SITHS PKI” with OID 1.2.752.74.8.4

1.3 PKI participants

1.3.1 Certification authorities

The term Certification Authority (CA) is an all-embracing term that refers to all entities authorized to issue public key certificates within SITHS. The CA term encompasses two subcategories of issuers:

- Root Certification Authorities. The SITHS Root CA acts as root for all subordinate CAs that are part of the SITHS CA hierarchy. A Root CA within SITHS only issues subordinate CA certificates.
- Subordinate issuing Certification Authorities. The set of SITHS Subordinate Issuing CAs issue end entity certificates based on the approved certificate profiles governed by the SITHS Policy Authority.

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

- Guarantee that all information within issued certificates is correct and verified in accordance with SITHS CP.
- Issue certificates according to Certificate Profiles approved by the SITHS Policy Authority.
- Provide information for repositories in accordance with section 2.1.
- Conduct audits in accordance with SITHS CP.
- Conduct subject identification in accordance with chapter 2.

- Provide subscribers and trusting parties, that use issued certificates, with appropriate information as dictated by SITHS CP and in accordance with applicable laws and regulations.
- Revoke certificates and issue revocation lists in accordance with chapter 4.

This CPS is approved by the SITHS Policy Authority.

Inera AB will make sure to maintain sufficient resources in the form of monetary means and insurances to be able to fulfil its duties according to SITHS CP.

1.3.2 Registration authorities

A Registration Authority is an entity that performs identification and authentication of certificate applicants for end-entity certificates, initiates or passes along revocation requests for end-entity certificates. Inera AB and SITHS member organizations may act as RAs for certificates they issue.

Each RA must operate in accordance with the SITHS Trust Framework and the terms in the SITHS Membership Agreement.

1.3.3 Subscribers

Subscribers under SITHS include all end entities of certificates issued by a SITHS CA. A subscriber is the entity named as the end entity subscriber of a certificate. End entity subscribers may be individuals or, infrastructure components such as firewalls, routers, trusted servers or other devices.

In most cases certificates are issued directly to individuals or entities for their own use. However, there commonly exist other situations where the party requiring a certificate is different from the subject to whom the credential applies.

For example, an organization may require certificates for a specific website. In such situations the entity subscribing for the issuance of certificates is different from the entity, which is the subject of the certificate (generally, the holder of the credential). Two different terms are used in this CPS to distinguish between these two roles: "subscriber", is the entity which contracts with a SITHS member organization for the issuance of credentials and "subject", is the entity to which the credential is bound. The subscriber bears ultimate responsibility for the use of the credential, but the subject is the individual that is authenticated when the credential is presented.

When “subject‟ is used, it is to indicate a distinction from the subscriber. When “subscriber” is used it may mean just the subscriber as a distinct entity but may also use the term to embrace the two. The context of its use in this CPS will invoke the correct understanding.

CAs are technically also subscribers of certificates within SITHS, either as a Root CA issuing a self-signed certificate to itself, or as a Subordinate Issuing CA issued a certificate by a superior CA. References to end entities and subscribers in this CPS, however, apply only to end entity subscribers.

1.3.4 Relying parties

A Relying Party is an individual or entity that acts in reliance of a certificate and/or a digital signature issued under SITHS. A relying party may or may not also be a subscriber within SITHS.

Relying parties are responsible for implementing controls regarding validity and revocation status of used certificates.

1.3.5 Other participants

1.3.5.1 Processing centers

Inera AB act as a Processing Center within SITHS which means Inera AB has established secure facility housing, among other things, CA systems, including the cryptographic modules holding the private keys used for the issuance of Certificates and perform all certificate lifecycle services of issuing, managing, revoking, and renewing certificates.

1.3.5.2 Subcontractors

Inera may use subcontractors to host the Processing Center within SITHS and for manufacturing tokens like Smart Cards or other tokens holding the private key of the subscriber.

1.3.5.3 Compliance Auditors

Inera will accept third party audit performed by SITHS Policy Authority appointed compliance auditors.

1.4 Certificate usage

1.4.1 Appropriate certificate uses

Individual Certificates are normally used by individuals to sign and encrypt information, to authenticate to applications (client authentication) and to authenticate and encrypt communication (such as SSL/TLS). An individual certificate may however be used for other purposes, provided that a relying party is able to reasonably rely on that certificate and the usage is not otherwise prohibited by law, by SITHS CP, by this CPS under which the certificate has been issued and any agreements with subscribers.

1.4.2 Prohibited certificate uses

Certificates shall be used only to the extent the use is consistent with applicable law. SITHS certificates are not designed, intended, or authorized for use as control equipment in hazardous circumstances or for uses requiring fail-safe performance such as the operation of systems, where failure could lead directly to death, personal injury, or severe environmental damage. CA certificates shall not be used for any functions except CA functions. In addition, end entity subscriber certificates shall not be used as CA certificates.

1.5 Policy administration

1.5.1 Organization administering the document

Inera AB
118 20 Stockholm

Phone: +46 (0) 771 25 10 10 (touch-tone 2)

1.5.2 Contact person

Inera AB
Email: info@inera.se
Phone: +46 (0) 771 25 10 10
Internet: http://www.inera.se
Revocation Service: +46 (0) 771 25 10 10 (touch-tone 2)

Inera AB
Identifieringstjänst SITHS
Inera AB, Box 17703, 118 93 Stockholm, Sweden
Email: sithspolicyauthority@inera.se

1.5.3 Person determining CPS suitability for the policy

The SITHS Policy Authority determines the suitability and applicability of this CPS.

1.5.4 CPS approval procedures

Approval of this CPS and subsequent amendments shall be made by the SITHS Policy Authority. Amendments shall either be in the form of a document containing an amended form of the CPS or an update notice. Amended versions or updates shall be linked to the repository defined in section 2.1.1.

1.6 Definitions and acronyms

See Appendix A. for a table of acronyms and Appendix B. for definitions.

2 PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 Repositories

A full text version of this CPS is published at https://www.inera.se/siths/repository.

2.2 Publication of certification information

Inera AB will make the following information available:

a) This CPS.
b) Certificate Revocation Lists of revoked certificates and information of revoked certificates via OCSP.
c) Self-signed CA-certificates, intermediate CA-certificates and cross-certified certificates for cross-certified CAs are distributed to SITHS Policy Authority who is responsible for making them publicly available.

The CRLs will contain information of all revoked certificates for each CA at the time of publication. Each CRL will only hold information of which the CRL is intended to give notification.

Inera will provide CA-certificates as long as they can be used for verification purposes.

2.3 Time or frequency of publication

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

This CPS is reviewed at least every 12 months.

2.4 Access controls on repositories

This CPS and CA-certificates are publicly available.

CRLs are available at CRL Distribution Points specified in chapter 7.

Revocation information via OCSP is available for signed and unsigned requests.

3 IDENTIFICATION AND AUTHENTICATION

3.1 Naming

3.1.1 Types of names

SITHS CA's shall issue certificates with a non-null subject Distinguished Name (DN) that complies with ITU X.500 standards.

Every subscriber identity is registered along with a set of attributes. Identities and attributes are verified by involved RAs.

For SITHS function certificates additional rulesets for each RA are applied and verified by validation specialists based on the rules determined by the SITHS Policy Authority.

The composition of names for different types of certificates are defined in the certificate profiles.

3.1.2 Need for names to be meaningful.

Distinguished Named in SITHS are ensured to be unique by means of a unique identifier. The unique identifier is contained within the Subject Serial number and serves as the general identification attribute for the end entity subscriber. For SITHS the unique identifiers are defined as follows:

- For individuals – A Swedish personal identity number, coordination number and/or an HSA-id.
- For functions – An HSA-id

The country attribute specifies the scope of other attributes contained within a certificate. This means that all attributes must be defined and be interpretable within each country.

Locality is defined as follows:

- For functions – the municipality where the Board of Directors of the organization that owns the domain-name has its seat.
- For individuals – one of the following
    - the county of the third party or the accountable issuer organization
    - locality is not used for all private companies

Organization is defined as follows:

- For functions – the name of the organization that owns the domain name
- For individuals – the organization name of the third party or the accountable issuer

Subscriber is defined according to 1.3.3.

Email addresses can only be expressed as SMTP-addresses (IETF RFC 2822 or IETF RFC 5322).

3.1.3 Anonymity or pseudonymity of subscribers

SITHS subscribers are not permitted to use pseudonyms (names other than a subscriber's true name).

3.1.4 Rules for interpreting various name forms.

Distinguished Names in Certificates are formed and interpreted using X.500 standards and ASN.1 syntax.

3.1.5 Uniqueness of names

The names of subscribers within SITHS shall be unique as stated in section 3.1.2. This applies to all certificate profiles. Inera verifies that the subscriber information is accurate by relying on an official business register maintained by an applicable government agency and also information in the HSA-directory.

3.1.6 Recognition, authentication, and role of trademarks

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

Inera AB does not check the right of the Customer Organization to use the names it gives in its certificate applications except for the Organization Name as stated in section 3.2.2, nor does the CA participate in any name claim dispute resolution procedure concerning brand names, domain names, trademarks, or service names. In the event of a name claim dispute, Inera AB reserves the right to reject a certificate order, or to revoke an already issued certificate.

3.2 Initial identity validation

3.2.1 Method to prove possession of private key

The certificate applicant must demonstrate that it rightfully holds the private key corresponding to the public key to be listed in the certificate. The SITHS CA shall verify that the certificate applicant possesses the Private Key corresponding to the Public Key. How this is done varies depending on the used SITHS issuance routine.

3.2.2 Authentication of organization identity

Inera AB verifies the organization name, legal name, business identity code and other relevant organization information of a new Customer Organization from an official business register maintained by an applicable government agency and/or information in the HSA-directory.

The Customer Organization makes an agreement with Inera to act as a Registration Officer within the Customer Organization and to register Inera certificates for the individuals or client devices related to the organization. The Customer Registration Officer is restricted to register certificates only within their own Organizations (O). Before enabling the service, the CA verifies the organization identity as described in the section 3.2.2.

3.2.3 Authentication of individual identity

The Customer Registration Officer is responsible for authenticating the Subject data according to SITHS Policy Framework. Subject authentication is typically based on previously recorded personal information in the HSA-directory.

Identity control is performed according to any of below procedures:

a. The subscriber shows an approved and valid ID.
b. The subscriber is identified and signs the order with a valid digital identity.

Identity check according to a) is normally performed by a connected RA of the Inera organization where the RA undertakes to practice the identification check in accordance with SITHS Policy Framework.

In the case the identity check also involves issuance of the hardware protected Inera e-legitimation, the requirements in the CPS for Inera Hardware based e-legitimation and SBC151 (regulations for issuing of SIS-approved ID-cards) is pursued.

3.2.4 Non-verified subscriber information

No stipulation.

3.2.5 Validation of authority

Inera is responsible for the administration interface which acts as a certificate issuing system. All identities issued according to this CPS are issued by administration interface or via an API provided by Inera.

Acceptable identities for authentication to the administration interface are identities issued by CAs within SITHS.

Identities issued by these CAs are accepted to order SITHS identities:

- SITHS e-id Person HSA-id 3 CA v1
  SHA1{a7610e355018165c171cf14324779af8763d479f}
- SITHS e-id Person ID 3 CA v1
  SHA1{ad9c170a7a5b4d1e67166492281e68eff6eb8f08}
- SITHS e-iD Person ID Mobile CA v1
  SHA1{eb7d3fc447f3c109b62684a5040ff6d91fe6c54d}

Identities issued by these CAs are accepted within the SITHS user pages:

- SITHS e-id Person HSA-id 3 CA v1
  SHA1{a7610e355018165c171cf14324779af8763d479f}
- SITHS e-id Person HSA-id 2 CA v1
  SHA1{7f91bd5a9fd24d752930c7b80dfd40330568c9b5}
- SITHS e-id Person ID 3 CA v1
  SHA1{ad9c170a7a5b4d1e67166492281e68eff6eb8f08}
- SITHS e-id Person ID 2 CA v1
  SHA1{94556fd9785b9223270e9d94841d08b33f3f440e}
- Telia Card Identifier CA v2
  SHA1{6ea83100aac94520aca78b287e24f1d8eeed095c}
- Telia Card Identifier CA v3
  SHA1{9888857392a154b69170e8e5382b898d0e2f6fab}
- SITHS eID Card Identifier CA v1
  SHA1{5ba34673a1272abaa22c2f94b7575e666d493125}
- SITHS e-iD Person ID Mobile CA v1
  SHA1{eb7d3fc447f3c109b62684a5040ff6d91fe6c54d}

Functions within the user pages may be limited depending on both the issuer of the person certificate and the assurance level of the person certificate.

3.2.6 Criteria for interoperation

Not applicable.

3.3 Identification and authentication for re-key requests

Not applicable.

3.4 Identification and authentication for revocation request

End entity certificates:

A revocation request for an end entity certificate shall be submitted in any of below three ways:

a. The subscriber's registration authority performs a revocation via the administration interface. The request is signed with a digital signature (according to 3.2.5).
b. The Subject performs a revocation in the self-administration interface. The request is signed with a digital signature (according to 3.2.5).
c. The Subject, Subscriber, or Registration Officer in a Customer Organization shall submit a request for certificate revocation to the Revocation Service by telephone. Revocation by Customer Organization shall only be executed when a) and b) cannot be used as revocation methods.

The Subject or the Subscriber can activate customer's self-service revocation. The Subject can submit the revocation request to Inera directly or via the Revocation Officer of the Customer Organization. In the latter case the Revocation Officer is responsible for the verification of the authenticity of the request.

If there is a risk of abuse of the private key associated with a certificate, the certificate is revoked in accordance with the request even if above identity validation requirements cannot be met. Information about the order of the revocation shall be logged. The method for identification and authentication for every revocation request shall be logged by the CA, along with eventual reasons for simplified identification and authentication.

CA issuing certificates:

Revocation is performed on request/behalf of SITHS Policy Authority.

4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 Certificate Application

4.1.1 Who can submit a certificate application

Certificate application may or can be performed by:

- Person who is the subject of the certificate and who is an employee of, or has a professional relation with, an organization within the issuance domain
- Id-administrators or authorized applicants within an issuance domain
- Persons within the SITHS Policy Authority

4.1.2 Enrollment process and responsibilities

4.1.2.1 End entity certificates

A certificate enrollment must undertake this process:

a. The Registration Officer in RA Organization will complete a digital application. The digital application is signed with a digital signature. When signing the application, the terms and conditions stated in section 9.6.2 are accepted by the Registration Officer. In the process the subscriber will state all relevant personal information according to section 3.1.1.
b. The keyholder/subscriber is identified according to section 3.2.

c. The digital application form is archived according to section 5.5.

4.1.2.2 CA and RA certificates

The representative of the CA enrolls RA system or Administration interface certificates. A digital request for the issuance of a RA system certificates needs to be approved by a trusted role. The installation of the new RA system certificates requires dual control.

The enrollment of certificates for Registration Officer in RA oOganization undertakes the same process as in section 4.1.2.1.

4.2 Certificate application processing

4.2.1 Performing identification and authentication functions

Identification and authentication of Subject and Subscriber information is performed according to section 3.2.

4.2.2 Approval or rejection of certificate applications

Inera will approve certificate application if it meets the requirements of validation and identification and if the application is digitally signed by an RA or by a representative of an RA. All other certificate applications will be rejected.

4.2.3 Time to process certificate applications

Under normal circumstances Inera will process a certificate application immediately.

4.3 Certificate issuance

4.3.1 CA actions during certificate issuance

CA actions during certificate issuance:

Issuing a certificate is Inera's acceptance of a certificate application from an RA or a representative of an RA.

The issuance of a certificate means that Inera accepts the subscriber application and the subscriber information that the subscriber has declared.

The digital registration by RAs is conducted in a system and in an environment that is secured from integrity flaws and follows routines that prevent faulty mixtures of keys and subscriber information.

Certificates are generated when an authorized representative for a CA or RA or other authorized representative for RA has ascertained that all application and control routines have been fulfilled.

Every certificate application from an authorized representative for a CA or RA or other authorized representative for RA can be traced back to the individual that signed the certificate application.

4.3.2 Notification to subscriber by the CA of issuance of certificate

Issued certificates are downloaded to the subscribers token (Smart Card or Mobile device), published to the HSA-directory and also accessible to the subscriber via SITHS user pages.

In some cases certificates are also sent via e-mail to the subscriber.

4.4 Certificate acceptance

4.4.1 Conduct constituting certificate acceptance

The following conduct constitutes certificate acceptance:

For functions:

- Signing a receipt for a SITHS certificate for functions constitutes the subscribers acceptance of the certificate.

For individuals:

- Signing a receipt for a SITHS certificate for persons constitutes the subscribers acceptance of the certificate.

4.4.2 Publication of the certificate by the CA

Certificates are published to the HSA directory. Certificates are published to the relevant attribute (i.e. userCertificate) of the object representing the certificate subject in the directory.

4.4.3 Notification of certificate issuance by the CA to other entities

Notification is sent to the RA if Inera fails to publish the certificate to HSA.

4.5 Key pair and certificate usage

4.5.1 Subscriber private key and certificate usage

Use of the private key corresponding to the public key in the certificate shall only be permitted once the subscriber has agreed to the subscriber agreement and accepted the certificate. The certificate shall only be used in accordance with:

- The SITHS subscriber agreement.
- The relevant CP.
- The terms of this CPS.

Certificate use must be consistent with the Key Usage field extensions included in the certificate. Subscribers shall protect their private keys from unauthorized use and shall discontinue use of the private key following expiration or revocation of the certificate.

4.5.2 Relying party public key and certificate usage

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

a) Verify the certificate is appropriate for the intended use;
b) Check the validity of the certificate, i.e. verify the validity dates and the validity of the certificate and issuance signatures; and
c) Verify from a valid Certificate Revocation List (CRL) or other certificate status service provided by the CA (i.e OCSP service) the certificate has not been revoked or suspended. If certificate status cannot be verified due to system failure or similar, the certificates should not be accepted.

4.6 Certificate renewal

No stipulation.

4.7 Certificate re-key

No stipulation.

4.8 Certificate modification

No stipulation.

4.9 Certificate revocation and suspension

4.9.1 Circumstances for revocation

Function for suspension of a certificate is not available.

A certificate must be revoked under the following conditions:

a) Upon suspected or known compromise of the private key.
b) Upon suspected or known compromise of the media holding the private key.
c) Subject or subscriber information is known to be invalid or re-verification fails.
d) When there is an essential error in the certificate.

A certificate may be revoked under the following conditions:

a) When any information in the certificate changes.
b) Upon termination of a Subject.
c) When a Subject no longer needs access to secured organizational resources.
d) When the certificate is redundant (for example, a duplicate certificate has been issued).
e) Customer's certificate contract with Inera has ended.
f) Any other reason that makes the certificate obsolete or threats related keys.

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

4.9.2 Who can request revocation

A revocation request may be made by the Registration Officer in the RA Organization, the Subject, SITHS Policy Authority and Authorized Inera revocation staff.

4.9.3 Procedure for revocation request

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

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

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

4.9.4 Revocation request grace period

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

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

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

4.9.5 Time within which CA must process the revocation request

Revoked certificates are published in the latest revocation list within one hour after a certificate is marked for revocation. The decision to revoke a certificate is normally made in relation to receiving the revocation request. In doubtful situations the decision can however be postponed until sufficient confirmation is given, there is no maximum time for such confirmations.

4.9.6 Revocation checking requirement for relying parties

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

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

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

4.9.7 CRL issuance frequency

CRLs for end entity certificates

- A new CRL is published at least every hour.
- The nextUpdate of the CRLs is set to seventy-two (72) hours.

CRLs for CA issuing certificates

- A new CRL is published at least every eighteen (18) months.
- The nextUpdate of the CRL is set to eighteen (18) months.
- If an issuing CA-certificate is revoked a new CRL will be published within a reasonable time.

4.9.8 Maximum latency for CRLs

Under normal circumstances the newly created CRL will be available in the repository within fifteen (15) minutes.

4.9.9 On-line revocation/status checking availability

Inera provides on-line revocation status checking via the OCSP protocol.

In general, the OCSP service is a 24/7 service. Availability of the service is provided in the agreement with Inera AB.

Validity time of an OCSP response is seventy-two (72) hours.

OCSP status is normally updated instantly upon a revocation request. Status information from the CA is pushed out to the OCSP-responder(s).

Status for Root CA/Offline CA will not be instantly available due to manual procedures. Status will be available within reasonable time a CA is revoked.

4.9.10 On-line revocation checking requirements

OCSP requests may be unsigned or signed.

All responses will be signed by a private key corresponding to a public key certified by the CA to which the OCSP request is made.

A request must be validated according to section 4.9.6.

4.9.11 Other forms of revocation advertisements available

Not applicable.

4.9.12 Special requirements re key compromise

Inera will use economically reasonable efforts to notify potential relying parties if Inera discovers, or has reason to believe, that there has been a compromise of the private key of one of the issuing CAs.

4.9.13 Circumstances for suspension

Certificate suspension is not allowed within SITHS.

4.9.14 Who can request suspension

See 4.9.13.

4.9.15 Procedure for suspension request

See 4.9.13.

4.9.16 Limits on suspension period

See 4.9.13.

4.10 Certificate status services

4.10.1 Operational characteristics

The OCSP-service will answer to signed and unsigned requests.

URLs to CRLs and the OCSP-responders are specified within each certificate.

4.10.2 Service availability

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

SLA is stated in the agreement with Inera AB.

4.10.3 Optional features

Inera does not provide online status information for expired certificates.

4.11 End of subscription

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

A subscriber may end a subscription for a SITHS certificate by:

- Allowing his/her/its certificate to expire.
- Revoking his/her/its certificate before certificate expiration without replacing the certificate.

4.12 Key escrow and recovery

Private keys are not escrowed.

5 FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

5.1 Physical controls

5.1.1 Site location and construction

Ineras CA and Processing center operations are conducted within Inera´s subcontractors premises in Sweden. All Inera CA and Processing center 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. The physical protection of which corresponds at least with the requirements for “Skyddsklass 3” defined in the regulation on priority rating, redundancy, power supply and physical protection of communications networks and services issued by MSB (Myndigheten för samhällsskydd och beredskap). Within these server rooms, key components are locked in separate, freestanding security cabinets.

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

5.1.1.2 RA Site location and construction

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

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

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

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

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

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

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

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 Nogui Teknik AB Operational Documentation. The security procedures are described in separate documentations belonging to the Inera AB 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 are 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 Data Center Physical access

Nogui Teknik AB 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 cage. The security cage has been placed in a data centre 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 data center"	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 or an authorized visit request.
Physical Security Tier 2 "common areas"	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/visitor badge. Physical access to tier two is automatically logged.

Tier	Description	Access Control Mechanisms
Physical Security Tier 3 "CA Security area"	CA Security Area is the security cage. The security cage provides access separation from the common areas of the data centre.	Access to CA Security Area requires the usage of an individual access card . 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 Tier 4 "CA Security Cabinet "	The CA Security Cabinet is where the CA systems and other critical devices are placed and where sensitive CA operations occur. Tier four is the only tier where local maintenance access to servers is possible.	The tier four data center requires dual control. Access to HSMs is restricted in accordance with Inera AB´s segregation of duties requirements. The opening and closing of cabinets or containers in this tier are logged for audit purposes. All access is video monitored. A notification is generated to the CA Security Board members. CA Security Board member will always check, grant and document each access to tier 4. Unescorted access is not given to person without clearance for Tier 4.

5.1.2.2 Remote administration room Physical access

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

Tier	Description	Access Control Mechanisms
Physical Security Tier 1	Physical security tier one refers to the outermost physical security barrier for the facility.	Access to this tier requires the use of a proximity card employee badge. Physical access to tier one is automatically logged.
Physical Security Tier 2	Tier two includes common areas including restrooms and common hallways.	Tier two enforces individual access control for entering the common areas of the facility through the use of a proximity card employee badge. Physical access to tier two is automatically logged. Visitors must always be escorted.

Tier	Description	Access Control Mechanisms
Physical Security Tier 3	Tier three is the first tier at which sensitive central CA and RA components are stored.	Tier three enforces individual access control using two-factor authentication including proximity card and PIN code. Dual control is enforced to enter or exit Tier three. Dual control is enforced to activate or deactivate Tier three alarm. Offline keying material like RA-system key backups and secret shares are protected using safes. Access to keying material is restricted in accordance with Inera AB´s segregation of duties requirements. Unescorted personnel are not allowed into a tier three secured area. Physical access to tier three is automatically logged and video monitored.
Physical Security Tiers 4	Tier four is the tier at which especially sensitive RA and CA operations that require remote administration capabilities occur.	Tier four enforces individual access control using two-factor authentication including biometrics or proximity card employee badge and PIN code. Dual control is enforced to enter or exit Tier four. Dual control is enforced to activate or deactivate Tier four alarm. Access to keying material is restricted in accordance with Inera AB´s segregation of duties requirements. Unescorted personnel are not allowed into a tier four secured area. Physical access to tier four is automatically logged and video monitored.

5.1.3 Power and air conditioning

Nogui Teknik AB´s 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

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

5.1.5 Fire prevention and protection

Nogui Teknik AB has taken reasonable precautions to prevent and extinguish fires or other damaging exposure to flame or smoke. Nogui Teknik AB´s fire prevention and protection measures have been designed to comply with local fire safety regulations .

5.1.6 Media storage

All media containing production software and data, audit, archive, or backup information is stored within the Nogui Teknik AB 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 Nogui Teknik AB´s normal waste disposal requirements.

5.1.8 Off-site backup

Nogui Teknik AB 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

Inera is responsible for all procedures defined in this section. This includes production and logistics of the entire administrative process.

Critical CA and RA operations are 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 operations personnel;
- security personnel;
- system administration personnel;
- designated engineering personnel; and
- executives that are designated to manage infrastructural trustworthiness.

Inera 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 fulfil 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
- personalizing 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 Inera 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.

5.2.2 Number of persons required per task

Iver 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 two Trusted Persons that works in conjunction. Either person work physically together or the other Trusted Person is involved via following security controls:

- 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.
- Critical files and directories are monitored by checksum tests so they are not modified during operational access. Security supervisors get alarm if modifications are done.
- Access controls and other security measures take care that no one person can alone install software that can access CA keys. Either person can install or person can access keys.

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

The Trusted roles in section 5.2.1 are fulfilled by at least one person each maintaining the segregation of duties based on job responsibilities.

Initiation of a CA and generation of CA keys requires the presence of at least two persons that hold the ISSO or CAA roles and at least one auditor that is approved by the SITHS Policy Authority.

5.2.3 Identification and authentication for each role

For all personnel chosen to become Trusted Persons, verification of identity is performed by Inera respective Iver HR, or appointed security function, by checking of a well-recognized form of identification (e.g., passport, driver license or other nationally accepted identification card). Identity is further confirmed through the background checking procedures described in section 5.3.1.

Iver 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

Inera 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 in the 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 Inera personnel and to affiliate or partner company personnel if Inera AB 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, Inera AB conducts background checks. The actual background checks conducted depend on the local law and other circumstances. In Sweden the following background checks are conducted for persons in Trusted Roles:

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

In Finland, the background checks include:

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

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

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

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

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

5.3.3 Training requirements

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

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

- Basic PKI concepts,
- Job responsibilities,
- Inera AB 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

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

5.3.5 Job rotation frequency and sequence

No stipulation.

5.3.6 Sanctions for unauthorized actions

Management will together with human resources and security personnel determine the appropriate sanctions in relation to the type, magnitude, and frequency of the unauthorized action. Such sanctions may include measures from a written warning to termination of employment and when applicable, legal action.

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 Inera 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 Inera's secure facilities only to the extent that they are escorted and directly supervised by Trusted Persons.

5.3.8 Documentation supplied to personnel

Inera AB personnel involved in the operation of Inera AB 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

Inera 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; and
- Kind of entry.

Inera 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; and
- Method used to validate organization and individual identity and authority.

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

Inera also reviews its audit logs for suspicious or unusual activity in response to alerts generated based on irregularities and incidents within Inera 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. Important audit logging is distributed to multiple logs like CA backend logs, CA frontend logs, server logs, firewall logs, CA alarms. All but alarms are transferred to several CA logging servers.

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 Inera personnel.

5.4.7 Notification to event-causing subject

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

5.4.8 Vulnerability assessments

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

5.5 Records archival

Inera 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 Inera compliance with this CPS and other audits.
i. Applicable terms and conditions and contracts (in all versions applied).
j. All CP and CPS versions published by the CA.

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

5.5.2 Retention period for archive

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

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.

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 Inera.

In the event that changes in procedures for access to archived material have been caused by Inera ceasing its operations, information on procedures for continued access to archived material shall be supplied by Inera 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)

No stipulation.

5.5.7 Procedures to obtain and verify archive information

Inera 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

Inera 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 cease to be used for issuing of new certificates.

5.6.1 Self-Signed CA

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

a. a new CA key pair is created,
b. a new self-signed certificate is issued for the new public CA key,
c. a cross certificate is issued where the new public CA key is signed using the old private CA key,
d. the certificates in accordance with b) to c) is published in the relevant directory,
e. new Subscriber certificates are signed with the new private CA key,
f. 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

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

5.7.1 Incident and compromise handling procedures

Inera 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 Inera has implemented disaster recovery plans.

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

Inera undertakes, on suspicion that Inera 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 Inera has a relationship that the CA's private key has been compromised and how new CA certificates can be obtained.
d. In the event Inera has cross certified the compromised CA key with another operational CA key, revoke any such cross certificates.

Subscriber key holders will be informed 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 Inera's influence. Through Inera'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

Inera 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.

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

Inera maintains offsite backup of important CA information for CAs issued at the Inera'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 it is necessary for an issuer CA to cease operation, Inera makes economically 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, Inera and, in the case of a Customer CA, the applicable Customer, will develop a termination plan to minimize disruption to Customers, Subscribers, and Relying Parties. Such termination plans may address the following, as applicable:

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

6 TECHNICAL SECURITY CONTROLS

6.1 Key pair generation and installation

6.1.1 Key pair generation

6.1.1.1 Specific requirements for CA 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. "SITHS e-ID Root CA v2"). They are activated only when needed. Two privileged CA Officers are required to temporarily activate an offline key.

The key ceremony of CA keys is always witnessed by an independent party and/or videotaped for examination.

6.1.1.2 Specific requirements for private Subscriber keys

Generation of subscriber private keys for functions are beyond the control of Inera.

Generation of subscriber private keys for persons must either be:

- For dedicated hardware devices such as SITHS cards:
  - Generated in the chip of a secure cryptographic module. These cryptographic modules shall be certified to at least NIST FIPS 140-2 level 2 or Common Criteria EAL5+ and use a random number generation according to NIST SP800-90A.
  - Or generated within the boundaries of an external HSM and then securely injected into the secure cryptographic module according to EN 419211-3 and thereafter immediately removed from the external HSM. The HSM shall have been certified to at least NIST FIPS 140-2 level 3 or CEN EN 419221-5 and use a random number generation according to NIST SP800-90A
- For certificates issued from SITHS e-id Person ID Mobile CA v1 private keys are generated and stored within the hardware based secure storage that is part of the mobile device itself.

6.1.2 Private key delivery to subscriber

SITHS cards and other cryptographic hardware devices are distributed via mail or registered mail to the subscriber directly. They are sent to the subscriber's home address according to the Swedish SPAR register or equivalent register approved by Inera. Subscribers with protected personal data have their mail forwarded via the Swedish government service "Förmedlingsuppdrag" (mail forwarding).

The device is sent locked to the subscriber who needs to activate it in the presence of an RA. The activation data required to unlock the device can be computed by the administration interface in the presence of an RA. The device can only be unlock and new activation data selected by the subscriber 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 Inera 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 hardware device.

6.1.3 Public key delivery to certificate issuer

Subscribers and RAs submit their public key to Inera AB 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).

When CA, RA, or end-user Subscriber key pairs are generated by Inera AB, this requirement is not applicable.

6.1.4 CA public key delivery to relying parties

CA public keys are delivered as certificates to Inera, responsible of publishing them on agreed addresses, specified in the AIA of the issued certificates, and/or any other place Inera finds suitable.

6.1.5 Key sizes

The CAs' issuer keys are generated as RSA keys with a minimum length of bits 4096 bits.

The Subscribers' and operators' RSA keys are generated with a minimum length of RSA 2048 bits or ECC 256 bits.

6.1.6 Public key parameters generation and quality checking

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

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

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

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

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

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

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

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

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

6.2 Private Key Protection and Cryptographic Module Engineering Controls

Inera AB has implemented a combination of physical, logical, and procedural controls to ensure the security of Inera AB and Customers CA private keys. Logical and procedural controls are described here in section 6.2. Physical access controls are described in section 5.1.2. Subscribers are required

by contract to take necessary precautions to prevent the loss, disclosure, modification, or unauthorized use of private keys.

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

6.2.1 Cryptographic module standards and controls

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

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

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

a. Hardware protected private keys which are created and stored in smart cards or equivalent chip-based hardware rated at a minimum FIPS 140-2 level 2 or Common Criteria EAL4.

b. Or, for mobile devices, stored within a hardware based secure storage that is part of the storage device itself.

End entities private keys for functions should be stored, used and protected in a fashion that prevents key compromise, unauthorized access and use. These keys are the key holder (and the key holder's organization) sole responsibility.

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

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

Inera AB uses quorum authentication where a minimum number of key or secret holders (a quorum, n out of m) is needed to authenticate a specific role and perform sensitive CA operations.

6.2.3 Private key escrow

Inera does not escrow private keys.

6.2.4 Private key backup

Inera 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

Inera will not archive subscriber Private Keys.

6.2.6 Private key transfer into or from a cryptographic module

Inera 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 Inera CA.

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

Inera AB 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 that are stored on the issuer system's hard disk or other media in encrypted form, the following applies:

a. If the equipment is to be used further in the same protected environment, erasing is carried out in such a way that these keys cannot be recovered at least without physical access to the media. Old or broken CA key storage media may be temporarily stored in the protected CA environment.
b. If the media that has contained CA key material will permanently leave the protected CA environment, it will be destroyed. Reliable de-magnetizer or physical destruction is used when destroying the media.

The Subscriber private confidentiality keys that are stored by the CA for backup purposes are securely destroyed at the end of service. Customer is responsible for destroying or otherwise preventing misuse 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.

All subscriber cryptographic module specifications are agreed upon with SITHS Policy Authority.

6.3 Other aspects of key pair management

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

6.3.1 Public key archival

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

6.3.2 Certificate operational periods and key pair usage periods

Private Root CA keys are used for a maximum of thirty-one (31) years in order to issue subordinate CA certificates.

Private CA keys are used for a maximum of thirty-one (31) years in order to issue Subscriber certificates and revocation lists. CA certificates are given a maximum validity period to cover the time from generation up to and including the point when associated private keys cease to be used for signing of Subscriber certificates and revocation lists.

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

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

Maximum period of validity for Subscriber certificates will be according to SITHS Certificate profiles.

6.4 Activation data

6.4.1 Activation data generation and installation

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

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

Inera AB´s password selection guidelines require that passwords:

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

- not contain many occurrences of the same character;
- not be the same as the operator's profile name; and
- not contain a long substring of the user's profile name.

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

6.4.2 Activation data protection

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

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

6.4.3 Other aspects of activation data

No stipulation.

6.5 Computer security controls

6.5.1 Specific computer security technical requirements

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

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

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

6.5.2 Computer security rating

The CA software used by Inera AB 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 QA system that is similar to the production system. The acceptance test is performed in the QA system before the changes are taken into production.

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

6.6.2 Security management controls

The CA follows the policies defined by Inera AB´s Security Unit in security management. Furthermore, the CA follows the Security Policy, Certificate Policy, and Certification Practice

Statement defined by it in all of its operations. The auditing of the operation is 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 Inera for the CA service. The reporting of abnormal events and of detected or suspected weaknesses in security is carried out according to the procedures defined in Inera's Incident Management procedures.

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

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

6.6.3 Life cycle security controls

No stipulation.

6.7 Network security controls

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

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

6.8 Time-stamping

No stipulation.

7 CERTIFICATE, CRL, AND OCSP PROFILES

7.1 Certificate profile

All certificates issued are subject to the certificate profiles that are in use for SITHS PKI. The SITHS Policy Authority maintains these certificate profiles. SITHS certificate profiles are available at: https://www.inera.se/siths/repository

If or when SITHS certificate profiles change Inera will, upon request from the SITHS Policy Authority, implement the new certificate profiles to applicable systems. The proceedings will be agreed upon with SITHS Policy Authority.

7.1.1 Version number(s)

See SITHS certificate profiles.

7.1.2 Certificate extensions

See SITHS certificate profiles.

7.1.3 Algorithm object identifiers

See SITHS certificate profiles.

7.1.4 Name forms

See SITHS certificate profiles.

7.1.5 Name constraints

See SITHS certificate profiles.

7.1.6 Certificate policy object identifier

See SITHS certificate profiles.

7.1.7 Usage of Policy Constraints extension

See SITHS certificate profiles.

7.1.8 Policy qualifiers syntax and semantics

See SITHS certificate profiles.

7.1.9 Processing semantics for the critical Certificate Policies extension

See SITHS certificate profiles.

7.2 CRL profile

CRLs conform to RFC 5280.

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

CRL basic fields are listed in the table below:

Field name	Field description and contents
Version	This field states which of the CRL versions defined in the X.509 standard the CRL conforms to. The CRLs conform to the version 2.
Signature algorithm	The CRLs are signed by using the same algorithm as is used for signing of the certificates. The algorithm used is sha256RSA* or sha512RSA*.

Issuer	This field states the name of the Issuer of the CRL. The CRL issuer name is always the same as the Issuer name (the CA's name) in the certificates listed on the CRL.
This Update	Date and time of CRL issuance.
Next update	Date and time by which the next CRL shall be issued. The next CRL may be issued at any time after the issuing of the previous CRL, however, it shall be issued before the time stated in the "Next update" field. The time difference between "This update" and "Next update" is defined in section 4.9.7.
Revoked certificates	This field states the serial numbers of revoked certificates, and for each revoked certificate the date and time of revocation and the reason for revocation.

*Functional certificate CRLs

7.2.1 Version number(s)

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

7.2.2 CRL and CRL entry extensions

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

In general, following CRL extensions may be used:

Extension	Extension description and contents
Authority key identifier	The identifier of the public key of the CRL Issuer is given in this field. The identifier can be used to identify the public key that corresponds to the private key used for the signing of the CRL. Within Inera AB PKI the SHA-1 hash algorithm is used to calculate the identifier.
CRL number	The CRL number is a number that indicates the position of the CRL in the sequence of issued CRLs. The numbering starts with 1, and it increase monotonically by one for each issued CRL. Based on the CRL number users are able to determine if a certain CRL replaces another CRL.
Reason Code of the CRL Entry	The reason for revocation can be one of the following: KeyCompromise, CACompromise, AffiliationChanged, Superseded, CessationOfOperation, CertificateHold
Invalidity date	The invalidity date provides the date, on which it is known or suspected that the private key was compromised or that the certificate otherwise became invalid. This date may be earlier than the revocation date in the CRL entry, which is the date at which the CA processed the revocation.

7.3 OCSP profile

7.3.1 Version number(s)

OCSP specification as defined by RFC6960 (X.509 Internet Public Key Infrastructure Online Certificate Status Protocol) is implemented for the OCSP responders.

Inera OCSP-servers have lightweight mode according to RFC5019 implemented. Responders will answer “unauthorized” to all request on expired or unknown certificates.

7.3.2 OCSP extensions

OCSP Nonce extension should be used in requests.

8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS

8.1 Frequency or circumstances of assessment

An independent, qualified third party will perform an annual Compliance Audit according to year plan.

8.2 Identity/qualifications of assessor

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

8.3 Assessor's relationship to assessed entity

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

8.4 Topics covered by assessment

The purpose of the Compliance Audit is to verify that Inera AB and all involved subcontractors comply with the requirements of this CPS.

8.5 Actions taken as a result of deficiency

The audited entity and the SITHS Policy Authority shall, in good faith, use economically reasonable efforts to agree on a corrective action plan for correcting the problems causing the exceptions or deficiencies and to implement the plan.

8.6 Communication of results

Inera AB does not communicate any results regarding the Compliance Audit to anyone but the SITHS Policy Authority.

9 OTHER BUSINESS AND LEGAL MATTERS

9.1 Fees

Fees are defined in applicable Customer agreement for the SITHS service. For more information see http://www.inera.se.

9.1.1 Certificate issuance or renewal fees

According to 9.1

9.1.2 Certificate access fees

According to 9.1

9.1.3 Revocation or status information access fees

According to 9.1

9.1.4 Fees for other services

According to 9.1

9.1.5 Refund policy

According to 9.1

9.2 Financial responsibility

9.2.1 Insurance coverage

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

9.2.2 Other assets

No stipulation.

9.2.3 Insurance or warranty coverage for end-entities

No stipulation.

9.3 Confidentiality of business information

9.3.1 Scope of confidential information

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

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

9.3.2 Information not within the scope of confidential information

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

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

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

9.3.3 Responsibility to protect confidential information

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

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

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

9.4 Privacy of personal information

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

9.4.1 Privacy plan

Please refer to chapter 9.4.

9.4.2 Information treated as private

Please refer to chapter 9.4.

9.4.3 Information not deemed private

Please refer to chapter 9.4.

9.4.4 Responsibility to protect private information

Please refer to chapter 9.4.

9.4.5 Notice and consent to use private information

Please refer to chapter 9.4.

9.4.6 Disclosure pursuant to judicial or administrative process

Please refer to chapter 9.4.

9.4.7 Other information disclosure circumstances

Please refer to chapter 9.4.

9.5 Intellectual property rights

No part of this CPS (other than in accordance with the exceptions detailed below) may be reproduced, published in a database system or transmitted in any form (electronic, mechanical, photocopied, recorded or similar) without written permission from Inera 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 Inera AB in accordance with section 1.5.2.

The allocation of intellectual property rights among SITHS participants other than subscribers and relying parties shall be governed by the applicable agreements between such SITHS participants.

9.6 Representations and warranties

9.6.1 CA representations and warranties

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

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

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

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

9.6.2 RA representations and warranties

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

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

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

Registration Officers are individually accountable for actions performed on behalf of a CA. Individually accountability means that there must be evidence that attributes an action to the person performing the action (audit logs). Records of all actions carried out in performance of RA duties shall identify the individual who performed the particular duty. When an RA submits Subscriber information to a CA, it will certify to that CA that it has authenticated the identity of that Subscriber and that the Subscriber is authorized to submit a certificate request in accordance with the CPS.

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

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

9.6.3 Subscriber representations and warranties

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

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

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

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

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

9.6.4 Relying party representations and warranties

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

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

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

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

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

9.6.5 Representations and warranties of other participants

No stipulation.

9.7 Disclaimers of warranties

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

9.8 Limitations of liability

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

9.9 Indemnities

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

- the Subject's failure to protect his private key or prevent it from being lost, disclosed or compromised,
- the failure to submit a certificate revocation request to the Revocation Service under the conditions that require notification to the CA, as stated in section 9.6.3.

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

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

9.10 Term and termination

9.10.1 Term

This CPS remains in force until notice of the opposite is communicated by Inera AB on its web site in the Inera AB CA Service Repository, specified in section 2.1.1

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 Inera's web site in the Inera AB CA Service Repository, specified in section 2.1.1, upon termination outlining the provisions that may survive termination of the document and remain in force.

9.11 Individual notices and communications with participants

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

9.12 Amendments

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

9.12.1 Procedure for amendment

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

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

Inera will post the notification at the CPS publishing point at https://www.inera.se/siths/repository. Changes affecting the terms of an agreement shall be notified in writing to the address given in the contact information of the signatory of the agreement.

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

9.12.2 Notification mechanism and period

See 9.12.1

9.12.3 Circumstances under which OID must be changed

If Inera determines that a new Object Identifier (OID) is required, Inera will assign a new OID and required amendments will be made.

9.13 Dispute resolution provisions

If a dispute relating to this CPS or CPS referring to this CPS is not successfully resolved by negotiations, it shall be settled by arbitration in accordance with the Reconciliation and Arbitration Rules of the International Chamber of Commerce (ICC). The Stockholm 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 to hold them in English.

9.14 Governing law

Swedish law shall apply to the interpretation of this CPS or CPS referring to this CPS, if not otherwise agreed.

9.15 Compliance with applicable law

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

9.16 Miscellaneous provisions

9.16.1 Entire agreement

No stipulation.

9.16.2 Assignment

No stipulation.

9.16.3 Severability

No stipulation.

9.16.4 Enforcement (attorneys' fees and waiver of rights)

No stipulation.

9.16.5 Force Majeure

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

9.17 Other provisions

No stipulation.

Appendix A. Acronyms

CA	Certification Authority
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
DER	Distinguished Encoding Rules
DN	Distinguished Name
DSA	Digital Signature Algorithm
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
SHA	Secure Hash Algorithm
TLS	Transport Layer Security
TTP	Trusted Third Party
UPS	Uninterruptible Power Supply
URI	Uniform Resource Identifier
URL	Uniform Resource Locator

Appendix B. Definitions

Access control:

The granting or denial of use or entry.

Activation Data:

Activation data, in the context of certificate enrolment, 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 enrolment 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.

Application Server:

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

Authentication:

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

Authorization:

The granting of permissions of use.

Authorised representative:

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

Asymmetric encryption algorithm:

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

Base certificate:

See primary certificate.

Business process:

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

CA certificate:

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

CA key:

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

Certificate:

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

Certificate Applicant:

An individual or organization that requests the issuance of a Certificate by a CA.

Certificate Application:

A request from a certificate Applicant (or authorized representative) to a CA for the issuance of a certificate.

Certification Authority (CA):

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

Certification Chain:

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

Certificate Extensions:

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

Certificate Level:

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

Certificate Policy (CP):

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

Certification Practice Statement (CPS):

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

Certificate Revocation List (CRL):

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

Confidential:

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

Confidentiality:

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

Cross Certification:

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

Cryptographic Module:

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

Decryption:

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

Distinguished Encoding Rules (DER):

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

Digital Signature:

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

Directory Service:

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

Distinguished Name (DN):

Every entry in a X.500 or LDAP directory has a Distinguished Name, or DN. It is a unique entry identifier 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.

Electronic signature:

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

Encryption:

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

E-mail Certificates:

Certificates utilized for encrypting and verifying digital signatures.

Entity:

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

FIPS 140-2:

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

FIPS 180-1:

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

Intellectual Property Rights:

Rights under one or more of the following: any copyright, patent, trade secret, trademark, and any other intellectual property rights.

Integrity:

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

ISO 11568-5:

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

Key:

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

Key holder:

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

Key Generation Ceremony:

A procedure whereby a CA or RA key pair is generated, its private key is transferred into a cryptographic module, its private key is backed up, and/or its public key is certified**.**

Key Pair:

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

Log:

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

MD5:

A Message Digest Algorithm.

Non-repudiation:

An attribute of a communication that provides protection against a party to a communication falsely denying its origin, denying that it was submitted, or denying its delivery. Denial of origin includes the denial that a communication originated from the same source as a sequence of one or more prior messages, even if the identity associated with the sender is unknown.

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.

Non-verified Subscriber Information

Information submitted by a certificate applicant to a CA or RA, and included within a certificate, that has not been confirmed by the CA or RA and for which the applicable CA and RA provide no assurances other than that the information was submitted by the certificate applicant.

Object Identifier:

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

Offline CA:

CAs that are maintained offline for security reasons in order to protect them from possible attacks by intruders by way of the network.

Online CA:

CAs that sign end entity subscriber certificates are maintained online so as to provide continuous signing services.

Online Certificate Status Protocol (OCSP):

A protocol for providing relying parties with real-time certificate status information.

Operator:

Employee of a CA.

Out of band process:

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

Operational Period:

The period starting with the date and time a certificate is issued (or on a later date and time certain if stated in the certificate) and ending with the date and time on which the certificate expires or is earlier revoked.

PKCS #12:

Public-Key Cryptography Standard #12, developed by RSA Security Inc., which defines a secure means for the transfer of private keys.

PKIX:

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

PKI personnel:

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

Policy:

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

Primary certificate:

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

PrintableString:

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

Private Key:

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

Processing Center:

An organization that creates a secure facility housing, among other things, the cryptographic modules used for the issuance of certificates.

Public Key Infrastructure (PKI):

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

Public:

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

Public Key:

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

RA policy:

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

Registration Authority (RA):

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

Re-key:

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

Relative Distinguished Name (RDN):

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

Relying Party:

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

Relying Party Agreement:

An agreement used by a CA setting forth the terms and conditions under which an individual or organization acts as a relying party.

Repository:

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

Revocation:

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

RSA:

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

Secondary certificate:

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

Sensitive:

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

Signature Verification Certificate:

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

Split Knowledge

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

SSL Client Certificate:

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

SSL Server Certificate:

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

Storage module:

In this document relates to cryptographic module.

Subject:

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

Subscriber:

Entity subscribing with a Certification Authority on behalf of one or more Subjects. The Subject may be a Subscriber acting on its own behalf.

Surveillance Camera:

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

Symmetric encryption:

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

Threat:

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

Token:

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

Trusted Third Party (TTP):

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

Trusting party:

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

Unambiguous identity:

An identity comprising a set of attributes which relate unambiguously to a specific person. The unambiguous connection between the identity and the person may be 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 that universal /foreign characters are supported.

Verification*:*

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

Vettor:

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

Vulnerability:

Weaknesses in a safeguard or the absence of a safeguard.

Written:

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

X.500:

ITU standard of a directory service.

X501 PrintableString:

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

X.509:

ITU standard that describes the basic format for digital certificates.