SITHS Certificate Policy redline

Version 2.1
Approval Date: 2021-11-11
Effective Date: 2022-01-01

Revision history

Version	Author	Comment	Effective Date
2.0	SITHS Policy Authority	Major update including an adaptation to “Tillitsramverk för Identifieringstjänst SITHS” and the revised audit process for SITHS.	2019-06-01
2.1	SITHS Policy Authority	Removed references to SITHS Autentiseringstjänst. Clarified the rules for Processing centers. Removed references to CA Browser Forum. Clarified rules for separation of duties and Number of persons required per task. Updated key sizes. Added description for Mobile CA Added references to the trust framework for Swedish e-ID	2022-01-01

inera

Table of contents

1 Introduction

1.1 Overview

All special terms and definitions addressed in 1.6 apply from hereon.

"**Inera AB**" manages PKI's that accommodates a large, public, and widely distributed community of user organizations within the public sector of Sweden. These organizations have diverse needs for IT- and information security. Inera AB offer PKI subscriber services to organizations that have signed a SITHS membership agreement with Inera AB. This agreement must make references to this CP and the SITHS trust framework which defines the conditions under which certificates can be issued. This agreement will also regulate the rights and obligations for each part in the contract. This CP and the membership agreement states that all issuance domains must apply for their membership with a declaration of assurance. Each issuance domain and its declaration of assurance are subject to audit by the SITHS Policy Authority.

An **accountable organization** may have sub-contractors that need end-entity certificates from SITHS. Such sub-contractors shall have an agreement with the accountable organization and are referred to as Third party organizations.

A **SITHS issuance domain** is an entity that consists of one accountable organization and any third parties that have a signed contract with them.

Individuals, organizations and functions that use SITHS certificates are referred to as a relying party. Each relying party must rely on a certificate in accordance with the terms set forth in the relying party agreement.

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

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

This CP presents multiple levels of identity assurance and covers the issuance of Certificates for the following purposes:

- Individuals e.g. users – Authentication and signing certificates to smart cards and mobile devices intended to identify physical persons. For person certificates, SITHS will comply with the current version of the trust framework for Swedish eID's.
- Functions – TLS certificates for machines, servers and shared email addresses intended to identify non-human entities. For function certificates, SITHS aims to comply with the current version of the Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates published at http://www.cabforum.org/. Major deviations will be documented by the SITHS Policy Authority.

1.2 Document Name and Identification

This document is the SITHS Certificate Policy (CP). The SITHS Policy Authority, acting as the policy defining authority, has assigned an object identifier for this CP.

The object identifier (OID) for this CP is: 1.2.752.74.8.1

All issued end-entity certificates will contain an object identifier that can be used to indicate the issuance process used and the resulting level of assurance (if applicable).

For persons, issued certificates will have varying levels of identity assurance. Identity assurance levels for a certificate may vary over time and the current mapping between certificate OID's and the matching identity assurance level can be found in the SITHS repository.

For functions, issued certificates does not at present have any stipulations to the level of identity assurance. However, there is still a mapping in the SITHS repository that indicates which issuance routine was used.

1.3 PKI participants

This section describes the entities relevant to the administration and operation of the SITHS PKI.

1.3.1 Certification authority

SITHS may have multiple generations of PKI structures at any given time. Now active CA's will be described in a document in the SITHS repository.

1.3.2 Registration authorities (RA)

Registration Authorities (RA) can refer to either the organization or the person ultimately responsible for certificate issuance within an issuance domain.

- The organization is hence referred to as issuance domain.
- The person is hence referred to as accountable issuer

Individuals assigned to this role shall be appointed by a representative with the appropriate mandate in their organization. An issuance domain may consist of one or many organizations operating within the Swedish Public Sector. All issuance domains must adhere to the SITHS trust framework and the terms in the SITHS membership agreement.

1.3.3 Subscribers

Subscribers under SITHS are those entities that use a certificate. Subscribers may be:

- Persons – e.g. physical persons within an issuance domain
- Functions – e.g. infrastructural components such as firewalls, routers, trusted servers or other devices.

Each receiver of a SITHS certificate must agree to the SITHS terms and conditions.

1.3.4 Relying Parties

Relying parties are individuals, organizations and functions that use SITHS certificates. For example a service that uses the information in a certificate and has to make a decision whether to trust it or not. Each relying party must trust the certificate in accordance with the terms set forth in the relying party agreement.

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

~~Relying parties that are not part of an issuance domain and wish to use SITHS Out-of-band service, hence referred to as SITHS AUTENTISERINGSTJÄNST, must sign an additional agreement explicitly for this purpose.~~

1.3.5 Other Participants

1.3.5.1 Auditors

SITHS will require the services of other security authorities, such as compliance auditors. Such auditors are appointed by the SITHS Policy Authority.

1.3.5.2 Processing centers

Processing centers are entities that are not a CA but participate in the issuance process of certificates. For example smart card manufacturing facilities and portal applications used for requesting certificate issuance from the CA.

1.4 Certificate usage

1.4.1 Appropriate certificate uses

Certificates issued under this CP may be used for the purposes designated in the key usage and extended key usage fields found in the certificate.

1.4.2 Prohibited certificate uses

Certificates do not attest to the good behavior of the certificate Subjects and Subscribers. They shall not be taken to guarantee that the Subject is trustworthy, honest, reputable in its business dealings, compliant with any laws, or safe to do business with.

Certificates issued under this CP may not be used by any Subscribers in relation to any of the following:

- where prohibited by any laws, be they national, European or international.
- where the usage does not correspond the Key Usage and/or the Extended Key Usage stated in the certificate
- certificates issued to functions shall not be used to identify persons and vice versa.

There are no provisions within this CP for cross-certification or other forms of recognition or usage of certificates issued under this CP by or with certificates issued by other governments, other Certificate Authorities as or under any other PKIs.

1.5 Policy administration

1.5.1 Organization Administering the Document

Inera AB with the mandate of the SITHS Policy Authority is responsible for administering this CP.

1.5.2 Contact Person

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 shall determine the suitability of the SITHS CPS.

1.5.4 CP Approval Procedures

Each formal release of this CP requires approval by the SITHS Policy Authority.

With each formal approval, a new effective date shall be set. On this effective date, all previous versions shall thereby become redundant if no further specification is given.

Inera AB shall preserve records of all past versions of this CP.

1.6 Definitions and acronyms

Unless alternative definitions, meanings or interpretations are assigned ~~in the following parts of this sub-clause, the definitions in CABF and~~ RFC 3647 apply. ~~Should there be any conflict between terms defined in both these documents, CABF shall take precedence~~

Term	Explanation
Identifieringstjänst SITHS	IT service for managing electronic identities within municipalities and regions in Sweden
ID-administrator	Collection name for all roles within SITHS
Relying Party	Limitations defined in 1.3.4 but otherwise with the meaning ascribed to it in [RFC3647].
SITHS PKI	SITHS Public key infrastructure. A hierarchy of CA's. Refers to all active SITHS PKI's.
SITHS CA	Function/server for issuing certificates within SITHS. Refers to all active instances of SITHS CA's.
Subscriber	User of certificate
End-entity certificate	Certificate issued for a function or a person
SITHS PA Charter	Rules for SITHS PA

EASY	Audit tool
Declaration of assurance	Compliance statement regarding SITHS trust framework (Tillitsdeklaration)
SITHS trust framework	The common requirements that governs SITHS (Tillitsramverk för Identifieringstjänst SITHS)
Trust framework for Swedish e-id	The common requirements that govern e-id's for Swedish citizens (Tillitsramverket för Svensk e-legitimation).
SITHS Autentiseringstjänst	SITHS Out-of-band service
Function certificate	Certificate issued for a non-person, e.g. a server
Person certificate	Certificate issued for a person
Issuance domain	An entity that consists of the accountable organization and any third parties that they have a signed contract with
Accountable organization	The organization that signs the membership agreement with Inera
Accountable issuer	The person responsible for certificate issuance within an issuance domain
Third party	Sub-contractors that need end-entity certificates and have an agreement with the accountable issuer
Membership agreement	Legal agreement that regulate the rights and obligations for each part of SITHS
Authorized applicant	Person authorized to request a function certificate
HSA-id	Unique identifier for objects within the HSA-directory
Personal identity number	Swedish unique identifier for a person (personnummer)
Coordination number	Swedish unique identifier for a person (samordningsnummer)
SITHS Incident Response Plan	Refers to the routine "Hantering av rapporteringspliktiga säkerhetsincidenter"
Processing centers	Processing centers are entities that are not a CA but participate in the issuance process of certificates. For example smart card manufacturing facilities and portal applications used for requesting certificate issuance from the CA.
Registration authorities (RA)	Registration Authorities (RA) can refer to either the organization or the person ultimately responsible for certificate issuance within an issuance domain. • The organization is hence referred to as issuance domain • The person is hence referred to as accountable issuer

2 Publication and Repository Responsibilities

2.1 Repositories

Inera AB is responsible for making information regarding the SITHS PKI available according to the following:

- **Regulatory documents** (Trust framework, CP, CPS, Certificate profiles, issuance routines, AIA, CRL i.e.) – https://www.inera.se/siths/repository
- **SITHS audit process –** https://www.inera.se/siths
- **Declaration of assurance and audit information** – Not published.
  Are kept in a separate tool called the easy auditing system (EASY)

2.2 Publication of certificate information

Each PKI participant shall ensure that information for which it has a publishing responsibility shall be available through a publicly accessible, on-line, repository.

2.3 Time or frequency of publication

All information, including changes in the regulatory documents, is published promptly after it is formally approved. Regulatory documents are reviewed by the SITHS Policy Authority when necessary or at least every 12 months.

2.4 Access controls on repositories

Regulatory documents, AIA, CRL and OCSP shall be provided with unrestricted read access.

~~SITHS Autentiseringstjänst is provided using Mutual TLS for relying parties that are entitled to access.~~

Repositories must implement logical and physical controls to prevent unauthorized modification to such repositories

3 Identification and Authentication

3.1 Naming

3.1.1 Type 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~~organization within an issuance domain 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 Names within SITHS are ~~ensured to be unique by means of~~assigned a unique identifier. The unique identifier is contained within the Subject Serialnumber 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
  - not used for all for 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

Subscribers shall not use anonymous or pseudonymous names.

3.1.4 Rules for interpreting various name forms

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

3.1.5 Uniqueness of names

Distinguished Name uniqueness is ensured by the use of the Subject Serial number as described in 3.1.2

3.1.6 Recognition, authentication, and role of trademarks

Certificate applicants shall not use names in their certificate applications that infringe upon the intellectual property rights of another entity. Explicitly, no certificate request may use any trademark, nor the identifying marks of any entity other than the one issuing the request.

Inera AB shall not be required to determine whether a certificate applicant has intellectual property rights to the name appearing in a certificate application or to arbitrate, mediate, or otherwise resolve any dispute concerning the ownership of any domain name, trade name or trademark.

SITHS Policy Authority and SITHS issuance domains shall be entitled, without liability to any certificate applicant, to reject or suspend any certificate application because of such disputes.

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

Organizations within an issuance domain are verified with the Swedish Companies Registration Office and/or the Central Bureau of Statistics.

- **For individuals:**
  - Inera AB verifies accountable issuers upon initial application and through audits
  - Accountable issuers verifies third parties
- **For functions:**
  - Validation specialists verifies in accordance with the SITHS function validation routine. Verified functions are included within a ruleset that is unique per subscriber name, organization and type of certificate and that enforces the correct organization information.

3.2.3 Authentication of Individual Identity

For any certificate application the subscribers identity shall be verified in accordance with the SITHS issuance routines and the SITHS trust framework.

All persons that receive a certificate must have a professional relation with at least one of the organizations within an issuance domain. For all identity assurance levels, the professional

relation of each person shall be asserted by means of an automated control with the HSA directory.

All individuals with a Swedish personal identity number or a Swedish coordination number are verified with the National registration at the Swedish Tax Agency by SITHS.

For identity assurance level 3 or higher, the person must have a verified Swedish personal identity number.

For persons, issued certificates will have varying levels of identity assurance. Identity assurance levels for a certificate may vary over time and the current mapping between certificate OID's and the matching identity assurance level can be found in the SITHS repository.

For functions, issued certificates does not presently have any stipulations to the level of identity assurance. However, there is still a mapping in the SITHS repository that indicates which issuance routine was used.

3.2.4 Non-verified Subscriber information

No stipulation.

3.2.5 Validation of Authority

SITHS shall validate the authority of subscribers requesting any type of certificate, by verifying that they are either the requesting id-administrator or an authorized applicant within the issuance domain.

- Authentication within the SITHS Administrative portal shall rely upon certificates issued under SITHS e-id Root CA v2 for persons with identity assurance level 3.
- Authentication within the SITHS user pages may rely upon all certificates issued under SITHS e-id Root CA v2 and the below listed Telia CA's for persons. However, 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
    - Telia e-legitimation EU HW CA v1 (2019-05-10)
      SHA1 thumbprint = 07 cb 51 6e 66 12 bf a5 e2 7e b3 1f 02 10 78 80 57 18 a1 9d
    - Telia e-legitimation HW CA v3 (2024-03-13)
      SHA1 thumbprint = 8c 6f 3b 02 d0 10 fe 90 c6 0a 1b 44 85 17 5d 2c b3 5f 05 26
    - Telia e-legitimation HW CA v4 (2033-10-31)
      SHA1 thumbprint = 8b df 84 0b a3 e9 99 17 a6 48 d2 b2 35 1c df 22 70 12 92 5f
    - Telia Card Identifier CA v2 (2025-09-28)
      SHA1 thumbprint = 6e a8 31 00 aa c9 45 20 ac a7 8b 28 7e 24 f1 d8 ee ed 09 5c
    - Telia Card Identifier CA v3 (2040-03-02)
      SHA1 thumbprint = 98 88 85 73 92 a1 54 b6 91 70 e8 e5 38 2b 89 8d 0e 2f 6f ab

3.2.6 Criteria for inter-operation

Inter-operation is not allowed.

3.3 Identification and authentication for re-key requests

Re-keying is not allowed.

3.4 Identification and Authentication for Revocation Request

Revocation procedures ensure, prior to any revocation of a certificate, that the revocation has in fact been requested by either:

- The certificate subscriber
- An id-administrator or authorized applicant within the issuance domain
- The applicable processing centers
- The SITHS Policy Authority

If key compromise is suspected for a private key associated with an issued certificate, the certificate is allowed to be revoked even if the below identification and authentication requirements cannot be completely fulfilled.

Acceptable procedures for authenticating the revocation requests of a subscriber are as follows:

Revocation request from	Method for revocation	Identification method
Subscriber	Self-administration portal	Authentication by mutual TLS with a certificate issued by a CA that is trusted by SITHS.
	Telephone call	Call to the support center that asks control questions (for card number, personal id, HSA-identity) that proves that the caller has knowledge about the certificate to be revoked.
Id-administrator, authorized applicant or other authorized representative within issuance domain	Administration portal	Authentication by mutual TLS with a certificate issued by SITHS where the identity assurance level is 3.
	Telephone call	Call to the support center that asks control questions (for card number, personal id, HSA-identity) that proves that the caller has knowledge about the certificate to be revoked.
Person within SITHS Policy Authority	Administration portal	Authentication by mutual TLS with a certificate issued by SITHS where the identity assurance level is 3.
	Telephone call	Call to the SITHS technical operations that asks control questions (for card number, personal id, HSA-identity) that proves that the caller has knowledge about the certificate to be revoked.
Processing centers	API	Revokes certificates in case of production errors.

4 Certificate life-cycle operational requirements

4.1 Certificate application

4.1.1 Who can submit a certificate application?

Below is a list of entities that may submit certificate applications:

- 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

~~Id-administrators and authorized applicants within the~~Each issuance domain ~~have~~has the utmost responsibility in validating the ~~application itself as well as the~~ identity of ~~the individual or~~ individuals and function prior to ~~authorizing issuance of~~accepting a certificate application. All validations shall be done in accordance with the SITHS issuance routines and the SITHS trust framework.

For functions SITHS validation specialists are responsible for managing the function rulesets for each issuance domain. The function rulesets control the scope of allowed certificate subject names for id-administrators and authorized applicants.

Each Applicant shall submit sufficient information and documentation for SITHS or the issuance domain to perform the required verification of identity prior to issuing a Certificate.

All communication during the Certificate Application process, including delivery of public keys to be included in Certificates, shall be authenticated and protected from modification.

4.2 Certificate Application Processing

4.2.1 Performing identification and authentication functions

An id-administrator or authorized applicant shall perform identification and authentication of all required subscriber information according to the requirements in chapter 3. Identification and authentication shall be done in accordance with SITHS issuance routines and the SITHS trust framework and may vary depending on the type of certificate being issued.

The id-administrator or authorized applicant signs the application ensuring that all requirements regarding application processing have been fulfilled.

4.2.2 Approval or rejection of certificate applications

An id-administrator or authorized applicant will approve an application for a certificate if the following criteria are met:

- The certificate application can be verified in accordance with 4.2.1

An id-administrator or authorized applicant will reject an application for a certificate if the following criteria are met:

- The certificate application cannot be verified in accordance with chapter 4.2.1
- The applicant fails to provide supporting documentation upon request
- The applicant fails to respond to notices within a specified time
- The id-administrator or authorized applicant suspects that the applicant may have malicious intent.

4.2.3 Time to process certificate applications

CAs and id-administrators shall begin processing certificate applications within a reasonable time. There is no stipulation as to the completion time for an application.

A certificate application remains active until rejected.

4.3 Certificate issuance

4.3.1 CA actions during certificate issuance

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

Certificates are generated when a member of the SITHS Policy Authority, id-administrator or authorized applicant has determined that all application and control routines have been fulfilled.

Each certificate application from a member of the SITHS Policy Authority, id-administrator or authorized applicant can be traced back to the individual that signed the certificate application.

During the certificate issuance process, the SITHS administrative portal shall verify that the information regarding the individual is up to date with the National registration at the Swedish Tax Agency and/or the HSA directory.

4.3.2 Notifications to subscriber by the CA of issuance of certificate

SITHS enables subscribers that are persons to view, download or revoke their own certificates by means of the SITHS user pages. This serves as a means for the person to monitor, discover and revoke any wrongfully issued certificates.

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.
- Or accepting the terms and conditions prior to certificate issuance

4.4.2 Publication of the certificate by the CA

All certificates issued by the SITHS PKI shall be published in the corresponding SITHS CA's database.

4.4.3 Notification of certificate issuance by the CA to other entities

No notifications are sent to other entities.

4.5 Key pair and certificate usage

Certificates must only be used for their intended purpose:

- Persons - Authentication and signing certificates to smart cards and mobile devices indented to identify physical persons
- Function - TLS certificates for machines, servers and shared email addresses intended to identify non-human entities

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 SITHS terms and conditions.

Certificate use must be consistent with the Key Usage and Extended Key Usage field extensions included in the certificate.

Subscribers shall discontinue use of the private key following expiration or revocation. Subscribers shall protect their private keys from unauthorized use.

4.5.2 Relying party public key and certificate usage

Relying parties that use SITHS certificates to identify subscribers shall independently ensure:

- That certificates are only used to verify the identity of subscribers in accordance with this CP. SITHS and its issuance domains are not responsible for assessing the appropriateness of the use of a certificate.
- That the certificate is being used in accordance with the Key Usage and Extended Key Usage field extensions included in the certificate.

- That the status of the certificate, and all the CAs in the chain that issued the certificate, are valid and not revoked. ~~For SITHS AUTENTISERINGSTJÄNST, however, this control is ensured by SITHS.~~
- Relying parties shall utilize the appropriate software and/or hardware to perform digital signature verification or other cryptographic operations in accordance with RFC5280, X.509 and applicable IETF PKIX standards. Such operations include verifying the validity of each certificate relied upon, identifying a certificate chain and verifying the digital signatures on all certificates in the certificate chain.

~~Relying parties, that are not part of an issuance domain, and wish to use SITHS AUTENTISERINGSTJÄNST, must sign an additional agreement designed for this purpose.~~

4.6 Certificate renewal

Renewal is not allowed. Certificate renewals can only be conducted as new certificate applications.

4.7 Certificate re-key

Certificate re-keying is not allowed.

4.8 Certificate modification

Certificate modification is not allowed. Certificate modifications can only be conducted as new certificate applications.

4.9 Certificate revocation and suspension

4.9.1 Circumstances for revocation

If any of the below circumstances occur SITHS shall revoke the certificate in question:

- subject serial number and names of the subscriber whose information contained within certificate is changed
- the subject fails to retrieve the certificate within reasonable time of its availability
- the original Certificate Request was not authorized
- suspecting that a private key associated with a certificate is compromised or used by some entity that is not the subscriber
- suspecting that the smart card or equivalent cryptographic module that contains the private key is no longer in use, or possessed, by the subscriber
- suspecting that the subscriber violates the stipulations in the SITHS terms and conditions

- SITHS detects or otherwise becomes aware that the certificate or the subscriber is involved in malicious activities
- SITHS detects or otherwise becomes aware that the Subscriber has lost its rights to a Domain Name or Organizational information contained within the certificate
- an error in production occurs within a processing centers.
- an accountable organization terminates its relationship with Inera AB, SITHS shall revoke all certificates issued in its issuance domain. This does not apply if the issuance domain signs an agreement for business transition to another issuance domain that inherit the responsibilities of the withdrawing accountable issuer.
- a used CA-key is suspected of compromise
- a CA ends its duties as a CA
- additional events occur that the SITHS Policy Authority determines, at its sole discretion, warrant revocation.

Prior to revoking a certificate, SITHS shall verify that the revocation request was made in accordance with 3.4.

4.9.2 Who can submit a revocation request

Revocation requests ~~can be made by:~~are accepted in accordance with 3.4.

- ~~The certificate subscriber~~
- ~~An id-administrator or authorized applicant within the issuance domain~~
- ~~The applicable processing centres~~
- ~~The SITHS Policy Authority~~

4.9.3 Procedure for revocation request

Entities submitting certificate revocation requests shall be identified according to 3.4

Issuance domains are required to promptly revoke certificates involved in a security incident.

SITHS shall:

- Revoke a certificate within reasonable time if the request is authenticated in accordance with 3.4.
- Provide a 24/7/365 ability to act on any certificate security incident reports.
- List revoked certificates in applicable CRL and OCSP services where they shall be published until one full publication cycle after the end of the certificate’s validity.
- Publicly disclose its revocation and incident reporting procedures.

Initiations of a revocation request to the CA must be signed by an authorized individual or be performed with multi-person control.

For Processing centers however, revocation requests may be automated if the certificate being revoked is associated with the order being produced.

4.9.4 Revocation request grace period

Revocation requests shall be submitted as promptly as possible but still within a reasonable time.

4.9.5 Time within which CAs 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 done in relation to receiving the revocation request

4.9.6 Revocation checking requirements for relying parties

It is solely the responsibility of relying parties to verify certificates revocation and suspension status in accordance with this CP before a certificate is used.

Relying parties shall verify revocation status through CRLs or OCSPs identified in each certificate in the chain.

When conducting revocation control a relying party must make sure that:

- The revocation control is made against a current revocation list or an up to date OCSP response
- The revocation list or OCSP response is still valid
- The digital signature of the revocation list or OCSP response is valid

~~However, for SITHS AUTENTISERINGSTJÄNST, revocation status is checked by SITHS. Therefore it is not necessary for relying parties to repeat those checks.~~

4.9.7 CRL issuance frequency

SITHS CAs that issue end-entity certificates new CRLs will be issued at least every 30 minutes all days of the year. Issuing CA CRLs shall have its nextUpdate attribute set to 72 hours after the issuance of the CRL.

SITHS Root CA’s are maintained in an offline state and will issue a new CRL at least once per year or whenever a CA certificate is revoked. Root CA CRLs shall have its nextUpdate attribute set to maximum 1 year after the issuance of the CRL.

Certificates that have expired may be removed from later issued CRLs.

4.9.8 Maximum latency for CRLs

The publication to the CRL repositories shall not occur more than 30 minutes after CRL issuance.

4.9.9 On-line revocation/status checking availability

SITHS offers an on-line revocation/status checking service, OCSP.

OCSP services for issuing CAs shall be updated with the latest revocation information at least once every 15 minutes all days of the year

OCSP services for Root CAs shall be updated with the latest revocation information every time a new CRL is issued

4.9.10 On-line revocation checking requirements

A relying party must confirm the revocation status of a certificate via CRL or OCSP in accordance with section §4.9.6, prior to relying on the certificate.

~~This does however not apply to SITHS AUTENTISERINGSTJÄNST where SITHS performs the revocation checking.~~

4.9.11 Other forms of revocation advertisements available

Not applicable.

4.9.12 Special requirements regarding key compromise

Accountable issuers are required to report certificate security incidents according to the SITHS certificate security incident routine.

SITHS shall use reasonable efforts to notify potential Relying Parties upon the discovery or suspicion that its Private Key has been compromised and therefore has been or is to be revoked.

4.9.13 Circumstances for suspension

Certificate suspension is not allowed in SITHS at present

4.9.14 Who Can Request Suspension

Certificate suspension is not allowed in SITHS at present

4.9.15 Procedure for Suspension Request

Certificate suspension is not allowed in SITHS at present

4.9.16 Limits on Suspension Period

Certificate suspension is not allowed in SITHS at present

4.10 Certificate status services

4.10.1 Operational characteristics

SITHS shall make certificate status information available through CRL according to 4.9.7 and 4.9.8. SITHS will also make certificate status information available through OCSP according to 4.9.9 and 4.9.10.

4.10.2 Service availability
SITHS shall provide certificate status services 24x7 without interruption except for scheduled maintenance.

4.10.3 Optional features
Certificates that have expired may be removed from certificate status services.

4.11 End of subscription

Subscribers may end their subscription to certificate services either by:

- Requesting that their certificate(s) be revoked or;
- by allowing the certificate(s) to expire

4.12 Key escrow and recovery

End-entity Private Keys shall never be escrowed by SITHS.

4.12.1 Key escrow and recovery policy practices
No stipulation

4.12.2 Session key encapsulation and recovery policy and practices
No stipulation

5. Facility, management, and operational controls

5.1 Physical controls

5.1.1 Site location and construction
SITHS shall perform its CA and Processing center operations from a secure data center equipped with logical and physical controls that make the CA and Processing center operations inaccessible to non-trusted personnel. The site location and construction, when combined with other physical security protection mechanisms such as guards, door locks, and intrusion sensors, shall provide robust protection against unauthorized access to the CA system, services, documentation and records.

The facilities that host a CA must also employ active surveillance and alarms that are monitored by guards 24 hours every day of the year.

CAs shall describe their site location and construction in more detail in their CPS.

5.1.2 Physical access

Access to each tier of physical security shall be auditable and controlled so that only authorized personnel can access each tier.

Detailed information about the security procedures that provide physical access control is considered as confidential and is therefore not to be made public.

5.1.3 Power and air conditioning

SITHS shall ensure a back-up power supply and sufficient environmental controls to protect the CA systems and Processing centers. The protection must be sufficient for the CA and Processing center to be able to automatically complete pending operations and record the system state prior to a shutdown caused by lack of power or an environmental conditioning error.

5.1.4 Water exposures

SITHS shall protect its CAs and Processing centers equipment from water exposure.

5.1.5 Fire prevention and protection

SITHS shall protect its CAs and Processing centers equipment from fire by installing mechanisms which detect fire and act to suppress it.

5.1.6 Media storage

Media storage requirements for accountable issuers and their issuance domains are described and agreed upon in the SITHS membership agreement and the SITHS trust framework.

SITHS shall protect all media from accidental damage and unauthorized physical access. SITHS shall duplicate and store its audit and archive information in a back-up location that is physically separate from its primary operations facility.

CAs shall describe its media storage procedures in its CPS.

5.1.7 Waste disposal

When needed SITHS shall destroy all data (electronic and paper) in accordance with NIST NIST 800-88 procedures for permanently destroying such data. CAs shall describe its waste disposal procedures in its CPS.

5.1.8 Off-site backup

CAs and Processing centers shall maintain backups of critical system data or any other sensitive information, including audit data, in a secure off-site facility.

The offsite location shall have procedural and physical controls that correspond to the operational location of the backups.

CAs shall describe its off-site backup capabilities in its CPS.

5.2 Procedural controls

5.2.1 Trusted roles

SITHS personnel acting in Trusted Roles include system administration personnel and some of the personnel involved with subscriber applications, support and audit.

SITHS shall design, document and publish the functions and duties performed by persons in Trusted Roles in a way that prevents one person from circumventing security measures or subverting the security and trustworthiness of the PKI.

All personnel in Trusted Roles must be free from conflicts of interest that might prejudice the impartiality of CA and RA operations.

Inera AB, SITHS Policy Authority or the issuance domain shall be responsible for appointing individuals to Trusted Roles.

The list of Trusted roles for Processing centers are maintained by the Processing center itself.

Role	Explanation/tasks
CA admin	Also called “Förvaltningsadministratör” has the system role “CA”. Is responsible for the configuration of issuance domains on a day-to-day basis. This includes but is not limited to: • Delegated mandate to administer changes of trusted roles within established issuance domains • Assigning the role accountable issuer within an issuance domain on request from the SITHS policy authority • Read and revocation rights within all issuance domains. • Limited issuance rights within all issuance domains
Validation specialist	Also called “Domänvalideringsspecialist” has the system role “Domain admin” Is responsible for the verification, approval or denial of requests regarding rulesets for issuance of SITHS function certificates.
Internal auditor	This is an administrative role whose responsibility includes but is not limited to: • Reviewing, maintaining and archiving audit logs • Performing and/or ensuring internal and external compliance audits to determine whether the SITHS personnel and issuance domains are operating in accordance with this CP.
Accountable issuer	Also called “Ansvarig utgivare”. An id-administrator within an issuance domain and the person utmost responsible for issuance of certificates. Has the system role “RA”.

Accountable issuer security responsible	A person with an internal auditor role in the issuance domain. This person is responsible for reviewing, maintaining and performing or ensuring internal compliance audits. The aim of the audits are to determine whether the issuance domain is operating in accordance with this CP, the SITHS trust framework and the SITHS membership agreement.
Issuance domain id-administrator	Also called “id-administratör”. A group of different roles with rights in a hierarchical structure. One ore sometimes more of these roles are assigned to persons within an issuance domain. Persons with one of these roles are responsible for the issuance of certificates to subscribers on a day-to-day basis. Depending on the exact role the responsibility may consist of, but is not limited to: • Requesting the issuance and revocation of certificates for Subscribers. • Conducting identity verification upon issuance and/or extradition of certificates • Compliance with required issuance and revocation steps according to established instructions
Certification Authority Administrator (CAA)	Administrative/operational personnel at the operation center for a CA Typical tasks that can be conducted by a CAA: • Create certificates • Personalize smart card • Generate CA keys • Generate revocation lists • View CA logs
System Administrator (SA)	Technical operational personnel at the operation center for a CA Typical tasks that can be conducted by a SA: • Installations • System maintenance • Change media and execute backups
Information Systems Security Officer (ISSO)	Security responsible for CA’s at the operation center ISSO is not directly involved in the processes of generating certificates, smart cards or revocation lists but is responsible for that all operative roles act within the boundaries of its permissions.

5.2.2 Number of persons required per task

The trusted roles for CAs, that is CAA, SA and ISSO, are assigned to at least two persons each. A person that holds either of these roles must not also be assigned the any of the other roles.

At least the following tasks within CAs and Processing centers shall only be allowed to be performed with (n out of m) multi-person control, where "n" needs to be at least 2 persons:

- Access to the CA-vault where HSM, CA software, Private keys and related material are operated or stored
- Access to ~~CA software and CA private key backups~~HSM
- Access to CA software and CA private key backups. For example while performing activities such as:
    - The generation, issuing, revocation or destruction of a CA certificate
    - The loading of a CA to a production environment
- During migration of CA private keys between security modules access to encrypted CA private keys, activation data and private keys used for the encryption shall be separated between multiple persons.
- Initiation of a CA and generation of CA keys requires the presence of at least 2 persons that hold the ISSO or CAA roles and at least one auditor that is approved by the SITHS Policy Authority.
- Access to personalized, but not delivered, end-entity cryptographic modules stored within Processing centers
- Access to subscriber activation data during generation at Processing centers
- Access to and administration of Application servers for SITHS
- Access to and administration of Database servers for SITHS
- Access to and administration of SITHS PKI repository servers

At least the following tasks shall only be allowed to be performed if the user has been identified with strong authentication and identity assurance level 3 or with (n out of m) multi-person control:

- Access to and administration of SITHS infrastructural operation components, for example network devices.
- Access to and administration of SITHS declaration of assurance
- Issuance of certificates by means of the SITHS Administrative portal or SITHS user pages

5.2.3 Identification and authentication for each role

Access rights to all systems within SITHS shall only be granted if users have undergone strong authentication with identity assurance level 3.

Central systems involved in the operations of SITHS may allow access with a lower grade of authentication but only if (n out of m) multi-person control is applied.

5.2.4 Roles requiring separation of duties

Roles requiring separation of duties include (but are not limited to):

- A SITHS internal auditor:
  - shall ~~serve~~review adherence to ~~fulfil the requirement of multi-party~~ access control ~~for~~requirements (e.g. Multi-person control, multi-factor authentication, physical access ~~to the CA-vault, but may not have logical access rights to any of the systems within the vault.~~etc.)
  - may only have ~~the system role "Läs" and~~ read access to systems involved in the operations of the SITHS PKI
  - shall not have any other rights than read access to logs, documents and similar
- A validation specialist should not be assigned the roles:
  - SA
  - CA admin
  - CAA
  - Id-administrator
  - ~~The generation, issuing, revocation or destruction of a CA certificate~~
  - ~~The loading of a CA to a production environment~~

Separation of duties may be enforced either by the ~~SITHS administrative portal, SITHS user pages, the~~ CA equipment~~, or~~ procedurally, physically or by ~~both means.~~ a combination of these.

There shall exist means to audit adherence to these rules.

5.3 Personnel controls

The SITHS Policy Authority has documented detailed personnel control and security policies for SITHS and accountable issuers to adhere to and be audited against.

All persons that hold a trusted role shall, beyond personnel controls, also be properly identified.

A selection of the listed personnel controls must be applied to both the SITHS personnel and for the accountable issuer for each issuance domain. Proof of performed personnel controls shall be documented and provided to the SITHS Policy Authority upon demand.

Accountable issuers shall describe which personnel controls are performed on id-administrators within their issuance domain in the declaration of assurance. For other personnel within the issuance domain the same procedures are recommended but optional.

Personnel controls and documentation of proof shall only be gathered in adherence to applicable laws and local policies.

5.3.1 Qualifications, experience, and clearance requirements

SITHS and accountable issuers shall require that personnel seeking to become trusted persons present proof of trustworthiness, qualifications, and experience needed to perform their prospective job responsibilities competently and satisfactorily.

5.3.2 Background check procedures

SITHS and accountable issuers shall conduct background checks for personnel seeking to become trusted persons.

Background checks for these persons shall be repeated periodically as part of the SITHS revision plan.

Background checks for accountable issuers, accountable issuer security responsible and id-administrator acknowledged by SITHS are e.g.:

- A confirmation of current employment
- A check of professional suitability and relevant education in the field
- A confirmation of passed education for the applicable role
- Financial status checks
- Legal suitability

Reports from background checks shall be evaluated and result in actions that are reasonable compared to 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.

5.3.3 Training requirements

SITHS will enable requisite training to all personnel with a Trusted Role.

Training should be started or completed before the person may assume his or her duties.

SITHS shall maintain records of who received training and what level of training was completed for all trusted roles except id-administrators and security responsible persons within the accountable issuers.

Accountable issuers are responsible for ensuring that id-administrators in their issuance domain have received training and have the knowledge and ability to perform duties according to their role.

All training materials shall be periodically reviewed and address the elements relevant to functions performed by the personnel.

The training relates to the person’s job functions and covers but is not limited to:

- Security principles and mechanisms of SITHS
- basic knowledge about Public Key Infrastructure (PKI)
- administration and knowledge of hardware and software versions used by the SITHS
- ITIL process handling within SITHS
- disaster recovery and business continuity procedures
- common threats to the validation process, including phishing and other social engineering tactics.
- All duties the person is expected to perform

- Knowledge of SITHS routines and policies
- Incident and compromise reporting and handling
- Authentication, identification and verification routines and policies
- Validation of ownership for functions

5.3.4 Retraining frequency requirements

SITHS personnel shall maintain skill levels that are consistent with industry-relevant training in order to continue acting in Trusted Roles.

SITHS and accountable issuers shall ensure that personnel acting in Trusted Roles:

- have knowledge and ability to perform duties according to their role over time.
- are made aware of any changes to the changes in policies and routines.

SITHS Policy Authority may enforce retraining requirements upon major changes in routines and policies.

5.3.5 Job rotation frequency and sequence

No stipulations.

5.3.6 Sanctions for unauthorized actions

No stipulations.

5.3.7 Independent contractor requirements

SITHS and accountable issuers may permit independent contractors or consultants to become trusted persons only to the extent necessary to accommodate clearly defined outsourcing relationships and only under the following conditions:

- The entity using the independent contractors or consultants as trusted persons does not have suitable employees available to fill the roles of trusted persons, and
- The contractors or consultants are trusted by the entity to the same extent as if they were employees.

Otherwise, independent contractors and consultants shall have access to secure facilities used within SITHS only to the extent they are escorted and directly supervised by trusted persons.

5.3.8 Documentation supplied to personnel

SITHS and accountable issuers shall provide personnel in Trusted Roles with documentation or tools necessary to perform their duties.

5.4 Audit logging procedures

Audit logs shall be reviewed both periodically and in response to alerts based on irregularities and incidents within SITHS systems.

Automated tools may be used to scan for anomalies or specific conditions.

Audit log processing shall consist of a review of the audit logs and documenting the reason for all significant events in an audit log summary. During processing a statistically significant set of security audit data generated since the last review and make a reasonable search for any evidence of malicious activity.

Audit log reviews shall include a verification that the log has not been tampered with.

Actions taken based on audit log reviews shall be documented.

Processing centers shall compare their audit logs with the supporting manual and electronic logs from SITHS and accountable issuers when any action is deemed suspicious.

5.4.1 Types of events recorded

The types of auditable events that must be recorded by SITHS and/or accountable issuers are set forth below. All logs, whether electronic or manual shall contain:

- the date and time of the event traceable to UTC (SP)
- the identity of the entity that caused the event
- the identity of the affected entity
- the event type
- type of the affected entity
- if the operation was successful or failed

CAs shall state the logs and types of events they record in their CPS.

Types of auditable events include:

- Operational events (including but not limited to (1) the generation of CA's own keys and the keys of subordinate CAs, (2) start-up and shutdown of systems and applications, (3) changes to CA details or keys, (4) cryptographic module lifecycle management-related events (e.g., receipt, use, de-installation, and retirement), (5) possession of activation data for CA private key operations, physical access logs, (6) system configuration changes and maintenance, (7) Records of the destruction of media containing key material, activation data, or personal subscriber information)
- Certificate lifecycle events (including but not limited to initial issuance, renew, revocation)
- Trusted employee events (including but not limited to (1) logon and logoff attempts, (2) attempts to create, remove, set passwords or change the system privileges of the privileged users, (3) personnel changes)
- Discrepancy and compromise reports (including but not limited to unauthorized system and network logon attempts)
- Operations performed on SITHS repositories, servers and infrastructural components
- Changes to certificate creation policies and templates e.g., validity period and certificate content

- Ruleset and configuration events

If the event cannot be recorded automatically, a manual procedure shall be implemented to satisfy the requirements.

All event records shall be made available to auditors upon request as proof of the SITHS and/or accountable issuers' adherence to SITHS routines and policies.

5.4.2 Frequency of processing log

SITHS shall, at least every two months:

- review and consolidate system and audit logs
- make system and file integrity checks

5.4.3 Retention period for audit log

SITHS shall retain audit logs on-site until they have been reviewed.

After review audit logs may be archived according to 5.5.2

5.4.4 Protection of audit log

Audit logs shall be protected with an electronic audit log system that includes mechanisms to protect the log files from unauthorized viewing, modification, deletion, or other tampering.

Logs are protected from unauthorized access and modification by:

- Using logical protection mechanisms within the operating system or the application
- Making the systems physically and logically inaccessible for unauthorized persons
- Ensuring that access to logs are only given to authorized trusted persons
- Monitoring access to logs by all entities

Audit log access is reviewed and verified at least once every month.

SITHS shall implement procedures that protect archived data from destruction prior to the end of the audit log retention period.

SITHS may disclose audit logs to relevant parties, e.g. auditors, upon request and if not prohibited by applicable law.

5.4.5 Audit log backup procedures

Incremental backups of audit logs shall be created daily and full backups are performed weekly. A copy of backups shall be stored off-site.

5.4.6 Audit collection system

SITHS may use an internal and automated audit collection system.

5.4.7 Notification to event-causing subject

No stipulation

5.4.8 Vulnerability assessments

Vulnerability scans and penetrations tests shall, when possible, be performed in accordance with business internal guidelines ~~from CA Browser Forum~~. Any findings are documented and prioritized on severity by those performing the test.

SITHS personnel later assesses and takes actions based on the report. The work is documented for future reference. Findings and actions taken shall be reported to the SITHS Policy Authority.

SITHS and accountable issuers shall perform risk assessments when needed, but at least annually. Risk assessments shall identify and assess reasonably foreseeable internal and external threats that could result in unauthorized access, disclosure, misuse, alteration, or destruction of any certificate data or certificate issuance process.

5.5 Records archival

5.5.1 Types of records archived

SITHS shall retain the following information in its archives:

- Current and previous versions of: SITHS trust framework, SITHS CP, SITHS CPS, SITHS Certificate profiles, RPA, SITHS terms and conditions.
- Current version of: Declaration of assurance and SITHS membership agreements
- Results and measures taken to comply to audits of SITHS operations
- All current and previous: Public and private CA-key and related cryptographic module operations, at least, generation, access to, modification, export, import and destruction
- System and equipment configurations, modifications; and updates
- All transactions that contain signed requests for lifecycle management of certificates
- Issued and revoked certificates and related updates to certificate repositories
- Any documentation related to the receipt or acceptance of a certificate or token
- All security incidents, at least:
    - Any attempt to delete or modify audit logs
    - Violations of the CP or CPS
    - Suspected and confirmed key compromise issues
    - Actions taken as a result of violations of physical security
- Appointment of an individual to a Trusted Role

If the archive contains digitally signed information, data that is required for signature verification is also archived.

SITHS may archive data manually or automatically. If automatic archival is implemented, SITHS shall synchronize its archived data on a daily basis.

5.5.2 Retention period for archive

SITHS shall retain archived data for at least 10 years from the time of data generation, unless a greater retention is required by any other applicable law or local policy.

Up to now and currently there is no culling of the archived information.

5.5.3 Protection of archive

SITHS shall store its archived records at a secure off-site location in a manner that prevents unauthorized access, modification, substitution, or destruction.

If the original media cannot retain the data for the required period, the archive site must define a mechanism to periodically transfer the archived data to new media.

SITHS shall maintain any software application and a suitable software/hardware host system required to process the archive data until the data is either expired or then destroyed, or it is transferred to a newer medium.

5.5.4 Archive backup procedures

SITHS shall back up system archives incrementally on a daily basis and perform full backups on a weekly basis. Further description of archive backup procedures shall be described in the CPS.

5.5.5 Requirements for time-stamping of records

SITHS shall automatically time-stamp archive records as they are created in accordance with chapter 6.8. Cryptographic time-stamping of archive records is not required.

5.5.6 Archive collection system (Internal or External)

SITHS shall collect archive information internally.

5.5.7 Procedures to obtain and verify archive information

SITHS shall not release archives unless requested by the SITHS Policy Authority or as required by law. Only authorized trusted personnel are able to obtain access to the archive

SITHS may allow subscribers and accountable issuers to obtain a copy of their own archived information

The integrity of information is verified when it is restored from archive

5.6 Key Changeover

A CA certificate may be renewed upon approval from the SITHS Policy Authority.

Following an approval of a renewal request, SITHS shall conduct a key generation ceremony in order to generate a new key pair for the CA. Such key generation ceremony shall meet the key ceremony requirements documented by the CA/Browser Forum’s Baseline Requirements. New CA certificates containing the new CA public keys generated during such key generation

ceremony shall be made available to relying parties through PKI repositories and communicated by means of newsletters.

New CA keys are created at least 3 months before the existing CA key ceases to be used for signing issued certificates.

SITHS shall periodically change its private keys in a manner set forth in the CPS that prevents downtime in the SITHS PKI operation. After key changeover, SITHS shall sign certificates using only the new key. SITHS shall still protect its old Private Keys and shall make the old Public Key Certificate available to verify signatures until all of the certificates signed with the old Private Key have expired.

5.7 Compromise and disaster recovery

5.7.1 Incident and compromise handling procedures

SITHS vital services shall be redundant and should be located at separate, geographically diverse locations and that should be configured for automatic failover in the event of a disaster (Disaster Recovery/Mirror Site).

SITHS shall implement data back-up and recovery procedures and shall develop a Disaster Recovery and/or Business Continuity Plan (DR/BCP).

SITHS shall review, test, and update the DR/BCP and supporting procedures annually. If a disaster occurs, SITHS shall re-establish operational capabilities as quickly as possible.

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

Following corruption of computing resources, software, and/or data SITHS shall be able to restore from the last known correct backup. Audit logs will be reviewed to ensure corrections of any missing data from the period between the used backup and the time of corruption.

Procedures for this shall be described in the applicable CPS.

5.7.3 Entity private key compromise procedures

If SITHS suspects that a CA Private Key is compromised or lost then SITHS shall follow Ineras Incident process and the SITHS Incident Response Plan for high priority incidents and immediately assess the situation, determine the degree and scope of the incident, and take appropriate action. If necessary, a CA certificate and the related private key may be revoked.

If there is a compromise or loss SITHS shall notify relying parties and accountable issuers and make information available that can be used to identify which certificates are affected, unless doing so would compromise the security of the Subscribers or SITHS

After a CA private key compromise SITHS personnel shall report the results of the investigation in accordance with the SITHS Incident Response Plan. The report must detail the cause of the compromise or loss and the measures that should be taken to prevent a re-occurrence.

Following revocation of a SITHS CA certificate, SITHS will generate a new CA Key Pair and sign a new CA certificate in accordance with its CPS. SITHS shall then distribute the CA-certificate in accordance with Section 6.1.4.

5.7.4 Business continuity capabilities after a disaster

SITHS shall establish a secure facility in at least one secondary location, to ensure that all components remain operational in the event of a disaster at the SITHS main site.

SITHS shall at least annually verify backup restore procedures for all components to be prepared for the event that all sites suffer a disaster

SITHS shall give priority to re-establishing the generation of certificate status information and thereafter certificate revocation and issuance. All these functions shall be restored within 24 hours following a disaster.

Disaster recovery equipment shall have the same physical security protections as described for production environments.

5.8 CA or RA termination

If an accountable issuer is terminated from SITHS, the accountable issuer is obligated to perform the termination in accordance with the SITHS trust framework.

In the event a CA is terminated from SITHS, SITHS is obligated to fulfil the following procedures:

- Inform subscribers and other parties that the CA has a relation with regarding the conditions for the termination, at least three months before termination
- Publicly inform relying parties and SITHS accountable issuers regarding the conditions for the termination, at least three months before termination
- Upon a CA's termination cease with issuance and remove functions for:
    - revocation lists
    - OCSP
    - publication of chain certificates that are related to the CA whose keys are terminated. This also means that current revocation lists are removed from their repositories and that no new revocation lists are published as replacements.
- Terminate all permissions that are held by subcontractors in regard to a CA that is targeted for termination
- Ensure that all archived information and logs are kept for the entire duration of the archival period

A CA within SITHS must provide guarantees and insurances that the necessary means are available to fulfil the above requirements in a termination situation.

6. Technical security controls

6.1 Key pair generation and installation

6.1.1 Key pair generation

SITHS shall generate and protect cryptographic keying material for CA's and Processing centers on a FIPS 140-2 level 3 or CEN EN 419221-5 validated cryptographic module using multiple individuals acting in Trusted Roles. When generating keying material for CA private keys SITHS shall create auditable evidence to show that the SITHS PKI enforced role separation and followed its key generation process for CA keys.

SITHS shall generate CA private keys based on random numbers that cannot be calculated regardless of what knowledge an entity might have regarding the circumstances for the key generation.

SITHS shall have an independent third party auditor validate the execution of the key process by either witnessing the key generation or by examining the signed and documented record of the key generation.

Private key generation for CA's will be performed in accordance with the "Telia ~~Production~~SITHS Certificate Practice Statement version 2.0"

~~Subscriber private keys must be generated using a FIPS-approved method.~~

Generation of subscriber private keys for functions are either:

- If the method for issuing is PKCS#10 – Generated by the subscriber and beyond the control of SITHS

Generation of subscriber private keys for persons must either be:

- For dedicated hardware cryptographic modules
  - 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 ~~EAL4~~EAL5+ and use a random number generation according to NIST SP800-90A.
  - ~~For certificates issued from CA's used when~~ Or generated within the ~~subscriber private key is stored within a~~boundaries of an external HSM and then securely injected into the secure ~~application delivered by SITHS.~~cryptographic module according to EN 419211-3 and thereafter immediately removed from the external HSM. The ~~secure application~~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 subscribers

For persons the generation- and delivery method of private keys including the ~~following~~ delivery method for activation data and the quality of the subscriber identification result in different identity assurance levels are achieved.

Private key activation or delivery to subscribers must always be preceded by an identification of the subscriber.

To achieve identity assurance level 3 private keys shall either be generated by the subscriber and stored in a secure hardware based module. following an authentication with at least the same identity assurance level or, if generated by a Processing center, be delivered by means of a channel that is separated and secluded from the activation data. The channel must also be protected against manipulation.

Subscriber shall sign a receipt or accept SITHS terms and conditions in connection to delivery or activation of the private key. Before the receipt is signed the private key is not considered to be delivered and remain the in the responsibility of the entity holding it.

For functions private keys are generated by the subscriber and are beyond the control of SITHS.

6.1.3 Public key delivery to certificate issuer

Transfer of public keys from the subscriber to a CA only occurs when:

- Requesting person certificates via the SITHS user pages and a certified PKI middleware
- Requesting person certificates by means of the SITHS eID user application in combination with the SITHS user pages to establish a secure connection between key hardware storage, user and PKI backend.
- Requesting function certificates by means of a PKCS#10-request

Public Keys shall be delivered to the SITHS PKI in a secure fashion and in a manner that binds the Subscriber's verified identity to the Public Key.

The certificate issuance shall ensure that the subscriber possesses the Private Key associated with the Public Key presented for certification.

6.1.4 CA public key delivery to relying parties

SITHS shall provide its public keys to Relying Parties in a secure fashion and in a manner that prevents substitution attacks. SITHS will deliver its CA Public Keys to Relying Parties by means of:

- The SITHS PKI repository, see 2.1
- Authority Information Access links within a X.509 v3 certificate extension specified in the certificate.

6.1.5 Key sizes

SITHS shall aim to follow the NIST timelines in using and retiring signature algorithms and key sizes.

SITHS shall generate and use the following: keys, signature algorithms, and hash algorithms for signing end-entity certificates, CRLs, and certificate status responses:

- ~~2048-bit RSA~~prime256v1/secp256r1 ECC Key with Secure Hash Algorithm version 2 (SHA-256)
- ~~3072~~2048-bit RSA Key or higher with Secure Hash Algorithm version 2 (SHA-256) or higher
- ~~4096-bit RSA Key with Secure Hash Algorithm version 2 (SHA-256);~~
- ~~4096-bit RSA Key with Secure Hash Algorithm version 2 (SHA-512);~~

SITHS may require higher bit keys in its sole discretion.

Any certificates, whether CA or end-entity, expiring after 2030-12-31 must be at least 3072 bit for RSA and 521 bit for ECDSA.

6.1.6 Public key parameters generation and quality checking

The SITHS PKI shall generate Public Key parameters for CAs and perform parameter quality checking in accordance with FIPS 140-2 level 3 or CEN EN 419221-5.

All CAs are required to keep up to date with developments and findings regarding cryptography and to adjust its algorithms in accordance with such developments and findings.

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

The SITHS PKI shall include key usage extension fields that specify the intended use of the certificate and technically limit the certificate's functionality in X.509v3 compliant software.

The SITHS PKI shall set key usage bits and assert extended key usage OIDs for each CA certificate in accordance with the SITHS certificate profile documents.

The SITHS PKI shall set key usage bits and assert extended key usage OIDs for end-entity certificate type in accordance with the SITHS certificate profile documents.

6.2 Private key protection and cryptographic module engineering controls

The procedures dictated by this CP regarding generation, storage and distribution of private keys is intended to provide protection for private keys in a way that minimize the risk that keys are inappropriately or maliciously exposed or used.

The responsibility for private key protection is divided as follows:

- CA private keys is the sole responsibility of the SITHS PKI
- End-entity cryptographic modules that are completed for delivery but are not yet sent to its recipient shall be ~~locked~~stored in a controlled storage vault

- End-entity cryptographic modules that are ready for extradition but are not yet extradited to the subscriber are locked in a controlled storage vault within the issuance domain until it is extradited.
- Private keys for persons that are signed for or generated by the subscriber is the sole responsibility of the subscriber
- Private keys for functions that are signed for by the id-administrator is the sole responsibility of the id-administrator

6.2.1 Cryptographic module standards and controls

SITHS CA's shall use cryptographic modules validated to at least FIPS 140-2 level 3 or CEN EN 419221-5.

Subscriber private keys for functions should be stored, used and protected in a fashion that prevents key compromise and unauthorized access.

Subscriber private keys for persons must either be:

- Stored 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 EAL4+.
- ~~For certificates issued from CA's used when the subscriber private key is~~ Or, for mobile devices, stored within a hardware based secure ~~application must be stored within a secure application delivered by SITHS~~storage that is part of the storage device itself.

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

See 5.2.2

6.2.3 Private key escrow

SITHS CA's shall not escrow its private keys.

6.2.4 Private key backup

SITHS shall back-up private keys needed for CA functions, CRL publishing, and providing online certificate status information. Security controls for private key backups are implemented using multi-person control (n of m persons), se 5.2.2.

6.2.5 Private key archival

SITHS shall not archive CA or centrally generated subscriber Private Keys.

6.2.6 Private key transfer into or from a cryptographic module

All CA private keys must be generated by and in a cryptographic module.

SITHS shall only export its CA Private Keys from the cryptographic module to perform CA key back-up procedures or in case of a future migration to other cryptographic modules. Migration of private keys shall be performed according to applicable criteria within the WebTrust Principles and Criteria for Certification Authorities.

When transported between cryptographic modules, SITHS shall encrypt CA private keys and protect the keys used for encryption according to 5.2.2.

For subscribers that are persons, private key transfer into or from cryptographic modules is ~~not allowed~~controlled by the Processing centers, SITHS portals and clients

For subscribers, that are functions, private key transfer into or from cryptographic modules is beyond the control of SITHS.

6.2.7 Private key storage on cryptographic module

SITHS shall store its CA Private Keys on a cryptographic module which has been evaluated to at least FIPS 140-2 Level 3 or CEN EN 419221-5.

Subscriber private keys shall be stored according to 6.2.1

6.2.8 Method of activating private key

SITHS shall activate its CA Private Keys in accordance with the specifications of the cryptographic module manufacturer and using multi-person control according to 5.2.2.

For person certificates, subscribers must authenticate themselves to the cryptographic module before activating their private keys. Entry of activation data shall be protected from disclosure.

For function certificates subscribers shall implement procedures to ensure that only the applicable function may activate the private key.

6.2.9 Method of deactivating private key

SITHS shall deactivate its CA Private Keys and store its cryptographic modules in secure containers when not in use. SITHS shall prevent unauthorized access to any deactivated cryptographic modules.

Person certificate subscribers are responsible for deactivating their private keys when not in use. The private key may be deactivated after each operation, upon logging off their system, or upon removal of a smart card from the smart card reader depending upon the authentication mechanism employed by the user. However deactivation of the private key is not equal to an actual logout from the system where the private key was used to gain access.

Deactivation of private keys for function certificates are the entity installing and/or using the certificate.

6.2.10 Method of destroying private key

When required, CA private keys are destroyed in a manner that reasonably ensures that there are no residuals remains of the key that could lead to the reconstruction of the key. For hardware cryptographic modules storing SITHS CA private keys, SITHS personnel with trusted roles may destroy the Private Keys by ~~executing a "zeroize" command or equal functions as described by~~according to the instructions from the cryptographic module manufacturer.

Physical destruction of hardware cryptographic modules for CA private keys is not required unless the cryptographic module has been compromised or is to be discarded.

Upon final destruction of a CA private key SITHS shall ensure that the private key backups and its associated storage media is destroyed.

SITHS may destroy the subscriber Private Keys by overwriting the data upon request from the subscriber or and authorized id-administrator.

6.2.11 Cryptographic module rating

See Section 6.2.1

6.3 Other aspects of key pair management

6.3.1 Public key archival

SITHS shall archive a copy of each issued certificate and the corresponding public key.

6.3.2 Certificate operational periods and key pair usage periods

SITHS certificates, including renewed certificates, have maximum validity periods of:

Type	Private Key Use	Certificate Term
Root CA	~~35~~31 years	~~35~~31 years
Sub CA	~~35~~31 years	~~35~~31 years
Subscriber Person Certificate	See certificate profiles	See certificate profiles
Subscriber Function Certificate	See certificate profiles	See certificate profiles

Upon the end of the usage period for a subscriber or CA key pair, the subscriber or CA shall thereafter cease all use of the key pair. However expired certificates may still be used to validate signatures generated before expiration and decrypt data encrypted before expiration.

SITHS may retire its CA Private Keys before the periods listed above to accommodate key changeover processes.

SITHS shall not issue a Subscriber certificate with an expiration date that is past the signing CA's validity.

6.4 Activation data

6.4.1 Activation data generation and installation

SITHS shall generate activation data that has sufficient strength to protect its CA Private Keys. If a CA uses passwords as activation data for a signing key, SITHS CA shall change the activation data upon renewal of the CA certificate.

SITHS may only transmit activation data for CA's outside the CA-vault by means of a channel that is separated and secluded from the associated cryptographic module and according to 5.2.2. The channel must also be secured against manipulation.

When passwords are used as activation data for function certificates, subscribers shall generate passwords that cannot easily be guessed or cracked by for example dictionary attacks.

Activation data for subscribers of person certificates is either:

- Generated by the Processing center upon manufacturing the cryptographic module. Activation data (PIN/PUK-codes) shall be generated with good entropy ~~and using~~without interaction from technicians. In cases where technician interaction is needed multi-person control according 5.2.2 shall be applied.
- Chosen by the subscriber as part of the certificate issuance process. Subscribers shall choose activation data with good entropy.

6.4.2 Activation data protection

SITHS CA shall protect activation data used to unlock CA private keys from disclosure using a combination of cryptographic and physical access control mechanisms achieving multi-person control according to 5.2.2.

SITHS shall require SITHS personnel to memorize and not write down their password or share their passwords with other individuals. SITHS shall implement processes to temporarily lock access to secure CA processes if a specified number of failed log-in attempts occur.

Subscriber activation data (PIN/PUK-codes) for persons that is delivered from a Processing center directly to the subscriber shall be protected in envelopes that are tamper proof and that ensure that the codes are protected from unauthorized access.

Subscriber activation data, in the form of PUK-codes, for persons may also be derived in the CA and Processing center using an agreed upon secure method. This enables both the Processing center and the portal to use PUK-codes in the processes of enabling Subscribers to retrieve or unblock their private keys.

During delivery from the Processing center, the activation codes are protected by using a delivery channel that is separated and secluded from the subscriber private keys. The channel must also be protected against manipulation.

Subscribers shall protect their activation data using methods that protect against the loss, theft, modification, unauthorized disclosure, or unauthorized use of the corresponding private keys.

6.4.3 Other aspects of activation data

No stipulations

6.5 Computer security controls

SITHS PKI systems and Processing centers shall:

- aim to comply with the CA Browser Forum Baseline Requirements Network and Certificate System Security and/or “Anvisning för Säkerhet i Drift” from Inera.
- comply with the trust framework for Swedish e-ID

6.5.1 Specific computer security technical requirements

SITHS PKI systems and Processing centers shall have production networks logically separated from other components. This separation prevents network access except through defined application processes. SITHS PKI systems and Processing centers shall use firewalls to protect the production network from internal and external intrusion and limit the nature and source of network activities that may access production systems. SITHS PKI systems and Processing centers shall primarily use strong authentication equal to identity assurance level 3. Scenarios where this is not supported shall be documented and disclosed to Inera on request.

If passwords are used a password policy shall be enforced requiring a minimum character length and a combination of alphanumeric and special characters, and shall require that passwords be changed on a periodic basis and whenever necessary.

Direct access to a Processing center database maintaining the Processing centers repository shall be limited to trusted persons in the Processing centers operations group having a valid business reason for such access.

All SITHS PKI systems and Processing centers CA systems shall be built in a manner that allows for separation of duties according to this CP. They shall also implement multi-person control in accordance with 5.2.2

SITHS PKI systems and Processing centers shall also have mechanisms and/or policies in place to control and monitor the configuration of their CA systems. Upon installation, and at least once a day, Processing centers shall validate the integrity of the CA system.

All access controls shall be constructed in a manner that allows every individual operator to be uniquely identified and authorized.

6.5.2 Computer security rating

No stipulations.

6.6 Life cycle security controls

SITHS PKI systems and Processing centers shall:

- aim to comply with the CA Browser Forum Baseline Requirements Network and Certificate System Security and/or “Anvisning för Säkerhet i Drift” from Inera.
- comply with the trust framework for Swedish e-ID

6.6.1 System development controls

For CA’s, systems involved with PKI operations and workstations used to gain access to such systems, SITHS shall only use:

- Software that was designed and developed under a formal and documented development methodology,
- Approved hardware and software developed by verified personnel, using structured development approach and a controlled development environment,

- Open source software that meets security requirements through software verification and validation and structured development/life-cycle management,
- Hardware and software purchased and shipped in a fashion that reduces the likelihood of tampering, and
- For CA operations, hardware and software that is dedicated only to performing the CA functions.

SITHS and its software suppliers shall implement procedures to prevent malicious software from being loaded onto CA's and systems involved with PKI operations. Such procedures shall include but is not limited to:

- Continuous code revisions during development
- Code revisions upon request from SITHS or independent auditors
- Startup and continuous scans of hardware and software for malicious code
- Penetration tests on major changes ~~and at least annually~~
- Continuously purchase or regularly develop updates to maintain security and functionality
- Using trusted and trained personnel to install the software and equipment.
- Not installing any software on its CA's and systems involved with PKI operations systems that are not part of the CA's operations.

SITHS shall use a formal configuration management methodology for installation and on-going maintenance.

Any modifications and upgrades shall be documented and controlled.

SITHS shall implement a mechanism for detecting unauthorized modifications to CA's and servers involved with PKI operations.

6.6.2 Security management controls

SITHS shall establish formal mechanisms to document, control, monitor, and maintain the installation and configuration of its CA's and systems involved with PKI operations, including any modifications or upgrades.

SITHS shall include procedures to detect unauthorized modification to the SITHS CA systems and data entries that are processed, logged and tracked for any security-related changes to CA systems, firewalls, routers, software and other access controls.

When loading software onto a CA or a system involved with PKI operations system, SITHS shall verify that the software is the correct version and is supplied by the vendor free of any modifications.

SITHS shall verify the integrity of software used with its CA and systems involved with PKI operations at least once a week.

6.6.3 Life cycle security controls

No stipulations.

6.7 Network security controls

Network security controls shall comply with the trust framework for Swedish e-ID and aim to comply with:

- the CA Browser Forum Baseline Requirements Network and Certificate System Security
- "Anvisning för Säkerhet i Drift" from Inera.
- " RIV Tekniska Anvisningar – Kryptering"

SITHS shall document and control the installation, configurations and maintenance of network components involved with PKI operations, including any upgrades or modifications made.

SITHS shall implement a process for detecting unauthorized modifications to hardware or software for network components involved with PKI operations.

SITHS shall verify all software for network components, when first loaded, as the unmodified software.

SITHS shall implement appropriate network security controls, including turning off any unused network ports and services and only using network software that is necessary for the proper functioning of the CA's and systems involved with PKI operations.

6.8 Time-stamping

SITHS shall ensure that the accuracy of clocks used for time-stamping are synchronized and traceable to UTC (SP).

Electronic of manual procedures may be used to maintain system time.

Clock adjustments are auditable events.

7. Certificate, CRL, and OCSP Profiles

7.1 Certificate Profile

All certificates issued within SITHS are subject to the certificate profiles that are in use for SITHS. These certificate profiles are maintained by the SITHS Policy Authority. The SITHS certificate profiles are available at the online repository in accordance with Section 2.1.

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
SITHS shall use distinguished names that are composed of standard attribute types, such as those identified in RFC 5280.

7.1.5 Name Constraints
SITHS may include name constraints in the nameConstraints field when appropriate.

7.1.6 Certificate policy object identifier
See SITHS Certificate profiles

7.1.7 Usage of Policy Constraints extension
Not applicable

7.1.8 Policy qualifiers syntax and semantics
SITHS may include brief statements in the Policy Qualifier field of the certificatePolicies extension.

7.1.9 Processing semantics for the critical Certificate Policies
No stipulation.

7.2 CRL Profile

7.2.1 Version number(s)
SITHS shall issue X.509 version 2 CRLs that conform to RFC5280

7.2.2 CRL and CRL entry extensions
SITHS PKI CRL extensions shall conform to the Extensions profile in RFC5280.

7.3 OCSP Profile

7.3.1 Version number(s)
SITHS shall use the OCSP specification as defined by RFC6960.

7.3.2 OCSP extensions
SITHS shall only use OCSP extensions that conform to the Extensions profile in RFC6960.

8. Compliance audit and other assessments

8.1 Frequency and circumstances of assessment

On at least an annual basis, SITHS shall appoint one or more independent, third-party, auditors who shall assess its conformity with this CP.

SITHS shall have a program for compliance control.

SITHS shall have an audit program that covers audits of accountable issuers conducted by Inera AB.

8.2 Identity/qualifications of assessor

Independent, third-party, auditors must meet requirements equal to at least one or more of the following:

- Licensed WebTrust Practitioner according to http://www.webrust.org
- Qualified auditor of the trust framework for Swedish e-ID and SITHS declaration of assurance to that federation

General requirements on personnel performing audits and other assessments:

- The scope of the audit or the assessment must be within the expertise of the personnel
- Must have a documented knowledge of the Swedish Public Sector, Identity Assurance practices and PKI standards and implementations.
- Must have a general knowledge of SITHS
- Must be trained and skilled in the auditing or assessment of secure information systems
- Must be familiar with organization compliance to trust frameworks, Information security management systems and IT, Internet and network security
- Must have a reputation for conducting its auditing and assessment business competently and correctly
- If a third-party is contracted the business must maintain Professional Liability/Errors and Omissions Insurance

8.3 Assessor's relationship to assessed entity

Audits within SITHS shall use independent, third-party auditors that has no financial interest, business relationship, or course of dealing that could foreseeably create a significant bias for or against the audited entity.

Internal audits within an issuance domain may use independent auditors from within their own organization.

8.4 Topics covered by assessment

Assessments by independent auditors shall cover adherence to at least the following:

That SITHS and all issuance domains comply with the requirements of this CP and the SITHS trust framework.

That this CP and all certificates for persons issued within SITHS are compliant to the SITHS declaration of assurance towards the Swedish e-ID federation and the current version of the trust framework for Swedish e-ID's.

~~That this CP and all certificates for functions issued within SITHS are compliant to the current versions of the following external audit requirements. However, as this PKI is a vital part in the infrastructure of the Swedish public sector some deviations may exist. Major deviations will be documented.~~

- ~~WebTrust Principles and Criteria for Certification Authorities, published at http://www.webtrust.org~~
- ~~CA Browser Forum Baseline Requirements, published at http://www.cabforum.org, for the Issuance and Management of Publicly-Trusted Certificates.~~

The SITHS Policy Authority shall continuously conduct audits to ensure compliance to the SITHS trust framework and this CP. The SITHS Policy Authority has the right to demand that accountable issuers take action on deficiencies found during audits in order to continue operating within SITHS.

8.5 Actions taken as a result of deficiency

Deficiencies shall be dealt with in accordance to the SITHS audit process "Ineras process för risk, revision och förbättring", see 2.1.

8.6 Communications of results

A report of the results of each audit shall be delivered to the SITHS Policy Authority for review, approval and to decide upon recommended actions.

The results shall also be communicated to any entities entitled by law, regulation, or agreement to receive a copy of the audit results.

9. Other business and legal matters

9.1 Fees

Any fees associated with the use of SITHS shall be regulated in the SITHS membership agreement.

Accountable issuers may set their own fees in their agreements with third parties.

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, processing centers and accountable issuers shall maintain a commercially reasonable level of insurance coverage for errors and omissions, either through an errors and omissions insurance program with an insurance carrier or a self-insured retention.

9.2.2 Other assets

Inera AB, processing centers and accountable issuers shall have sufficient financial resources to maintain their operations and perform their duties, and they must be reasonably able to bear the risk of liability to subscribers and relying parties.

9.2.3 Insurance or warranty coverage for end-entities

No stipulations.

9.3 Confidentiality of business information

9.3.1 Scope of confidential information

Information that is not explicitly or by other means defined as public in this CP is treated as confidential and is not given access to without an explicit agreement with the SITHS Policy Authority.

9.3.2 Information not within the scope of confidential information

The following information is not considered as confidential:

- Issued certificates including associated public keys
- Revocation lists (CRL and OCSP)
- Relying Party Agreements
- Certification Practice Statements
- Certificate Policies
- Technical and supporting documents

Exceptions can apply for information related to specific issuance domains if this is formally agreed upon between the SITHS Policy Authority and the accountable organization.

9.3.3 Responsibility to protect confidential information

SITHS personnel and contractors are responsible for protecting confidential information in accordance with the Offentlighets- och sekretesslag 2009:400 (Public Access to Information Act).

9.4 Privacy of personal information

9.4.1 Privacy plan

SITHS shall develop a privacy plan in accordance with the European general data protection regulation (EU) 2016/679, hence referred to as “Dataskyddsförordningen”.

CAs and processing centers shall implement a privacy policy that conforms to applicable local privacy laws. SITHS participants shall not disclose or sell the names of certificate applicants or other identifying information about them.

All personnel involved with the SITHS PKI are expected to handle personal information in strict confidence and meet the requirements of Swedish and European law concerning the protection of personal data. SITHS shall securely store and protect sensitive against accidental disclosure.

9.4.2 Information treated as private

Any information about subscribers that is not made available to a relying party through the subscriber’s own use of the subscribers certificate is treated as private.

9.4.3 Information not deemed private

Information disclosed through certificate status services are not considered private information.

9.4.4 Responsibility to protect private information

SITHS PKI participants receiving private information shall secure it from compromise and disclosure to third parties and shall comply to applicable laws.

9.4.5 Notice and consent to use private information

Private information should not be used without giving notice to the party to whom that information applies. This section is subject to applicable laws.

9.4.6 Disclosure pursuant to judicial or administrative process

SITHS may disclose private information, without notice, when required to do so by law, regulation or other requirements in this CP. All disclosure shall be made in accordance to applicable laws.

9.4.7 Other information disclosure circumstances

No stipulations.

9.5 Intellectual property rights

Intellectual property rights are regulated in the SITHS membership agreement.

Private and public keys are the property of the Subscribers who rightfully hold them.

SITHS shall not knowingly violate the intellectual property rights of any third party.

9.6 Representations and warranties

9.6.1 CA representations and warranties

Inera AB warrants that the SITHS PKI complies with this CP, the applicable CPS and all other stipulations referenced in these documents.

9.6.2 RA representations and warranties

Accountable issuers warrant that they comply to the requirements of this CP, the SITHS trust framework and the SITHS membership agreement.

9.6.3 Subscriber representations and warranties

Subscribers warrant to comply with the SITHS terms and conditions.

9.6.4 Relying party representations and warranties

Relying Parties warrants to follow the procedures and requirements of this CP and the applicable Relying Party Agreement prior to relying on or using a certificate issued by the SITHS PKI.

9.6.5 Representations and warranties of other participants

No stipulation.

9.7 Disclaimers of warranties

No stipulations.

9.8 Limitations of liability

No stipulations.

9.9 Indemnities

No stipulations.

9.10 Term and termination

9.10.1 Term

This CP and any amendments are effective according to the effective dates set forth in this CP.

9.10.2 Termination

Each CP remains in effect until terminated or replaced with a newer version

9.10.3 Effect of termination and survival

Upon termination of this CP, SITHS participants and subscribers are still bound by the terms for each issued certificate for the remainder of the certificates validity period.

Responsibilities related to audit logs, archiving and the protection of confidential information will survive termination.

Upon termination SITHS may communicate additional conditions and requirements.

9.11 Individual notices and communications with participants

Unless otherwise specified by agreement between the parties, SITHS participants shall use commercially reasonable methods to communicate with each other, taking into account the criticality and subject matter of the communication.

9.12 Amendments

9.12.1 Procedure for amendment

The SITHS Policy Authority determines what amendments should be made to this CP or the CPS. Controls are in place to ensure that this CP and the CPS is not amended and published without the prior authorization of the SITHS Policy Authority. The SITHS Policy Authority reviews this CP and the CPS when necessary or at least annually.

Amendments to this CP or a CPS are posted to the online repository.

9.12.2 Notification mechanism and period

SITHS will notify participants upon significant changes to this CP or a CPS. Notifications shall be made through at least the following:

- Publications on SITHS and/or Inera website
- Newsletters
- Communication directly with accountable issuers

SITHS may, without notice, make editorial and typographical corrections and other changes that do not materially impact the SITHS participants.

SITHS does not have a fixed notification period.

9.12.3 Circumstances under which OID must be changed

If the SITHS Policy Authority determines an amendment requires a change in an OID, then the revised version of this CP will also contain a revised OID. Otherwise, amendments do not require an OID change.

9.13 Dispute resolution provisions

Before resorting to any dispute resolution mechanism, the disputing party shall notify SITHS of the dispute with a view to seek dispute resolution.

Disputes that cannot be settled between SITHS and the party themselves shall ultimately be resolved within the Swedish legal system.

9.14 Governing law

The laws of Sweden shall govern the interpretation, construction, enforcement and validity of this CP.

9.15 Compliance with applicable law

This CP is subject to all laws and regulations within the jurisdiction within which the SITHS PKI operates.

9.16 Miscellaneous provisions

9.16.1 Entire Agreement

See 1.1 and the SITHS membership agreement.

9.16.2 Assignment
See 1.1 and the SITHS membership agreement.

9.16.3 Severability
See 1.1 and the SITHS membership agreement.

9.16.4 Enforcement (attorneys' fees and waiver of rights)
No stipulations

9.16.5 Force Majeure
Inera AB is not liable for a delay or failure to perform an obligation under this CP to the extent that the delay or failure is caused by an occurrence beyond SITHS reasonable control. The operation of the entire Internet is e.g. beyond SITHS reasonable control.

Force majeure may be regulated in the SITHS membership agreement

9.17 Other provisions

No stipulations.