SITHS Certificate Policy

Version 1.1.1
Effective Date: 2015-04-17

inera
LANDSTING OCH REGIONER
I SAMVERKAN FÖR E-HÄLSA

Table of contents

Version history		
Version	Author	Comment
1.0	Conny Balazs	Initial finalized version. Approved by SITHS Policy Authority
1.1	SITHS Policy Authority	Revised version. Approved by SITHS Policy Authority.
1.1.1	SITHS Policy Authority	Minor revisions after comments from the CA operating supplier. Approved by SITHS Policy Authority. (Changes are published in the redline version that contains all changes from version 1.0.)

1 Introduction

In general, a public-key certificate binds a public key held by an entity (such as a person or device) to a set of information that identifies the entity associated with use of the corresponding private key. In most cases involving identity certificates, this entity is known as the "subject" or "subscriber" of the certificate. Two exceptions, however, include devices (in which the subscriber is usually the individual or organization controlling the device) and anonymous certificates (in which the identity of the individual or organization is not available from the certificate itself). Other types of certificates bind public keys to attributes of an entity other than the entity's identity, such as a title.

A certificate is used by a "certificate user" or "relying party" that needs to use, and rely upon the accuracy of, the binding between the subject public key distributed via that certificate and the identity and/or other attributes of the subject contained in that certificate.

A relying party is frequently an entity that verifies a digital signature from a certificate subject where the digital signature is associated with an email, web form, electronic document, or other data. Other examples of relying parties can include a sender of encrypted email to the subscriber, a user of a web browser relying on a server certificate during an SSL/TLS session and an entity operating a server that controls access to online information using client certificates as an access control mechanism. In summary, a relying party is an entity that uses a public key in a certificate (for signature verification and/or encryption).

The degree to which a relying party can trust the binding embodied in a certificate depends on several factors. These factors can include:

- The practices followed by the certification authority (CA) in authenticating the subject
- The CAs operating policy, procedures and security controls
- The scope of the subscriber responsibilities
- The stated responsibilities and liability terms and conditions of the CA

SITHS is a PKI that accommodates a large, public, and widely distributed community of users within Sweden that 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.

SITHS member organizations must sign a formal contract with the SITHS Policy Authority before certificates can be issued. This contract must make references to this CP and the SITHS RA Policy which defines the circumstances under which certificates can be issued.

The SITHS Policy Authority must have a formal contract with subcontractors that define rights and obligations for each part in the contract. In this context an RA is also a subcontractor.

This document is the principal statement of policy governing the SITHS PKI. The Certificate Policy (CP) sets forth the business, legal, and technical requirements for approving, issuing, managing, revoking, and renewing, digital certificates within SITHS and providing associated trust services for all participants within SITHS. These requirements protect the security and integrity of SITHS and comprise a single set of rules that apply consistently across SITHS, thereby providing assurances of uniform trust throughout SITHS. The CP is not a legal agreement between Inera AB and organizations with a SITHS membership; rather, contractual obligations between Inera AB and SITHS participants are established by means of agreements with such participants.

This document is targeted at:

- CAs that operate within SITHS.
- RAs that operate within SITHS.
- SITHS PKI service providers and processing centers that have to operate in terms of their own Certification Practices Statement (CPS) that complies with the requirements laid down by the CP.
- SITHS certificate subscribers who need to understand how they are authenticated and what their obligations are as SITHS subscribers and how they are protected under SITHS.
- Relying parties who need to understand how much trust to place in a SITHS certificate, or a digital signature using a SITHS certificate.
- Auditors that conduct audits of different parts of SITHS.

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 is owned and maintained by the SITHS Policy Authority.

1.1 Overview

An overview of the SITHS policy structure is shown in diagram 1 below. At the top of the hierarchy is the SITHS Policy Authority that owns and maintains this CP and that sets out the policies which SITHS participants must comply with.

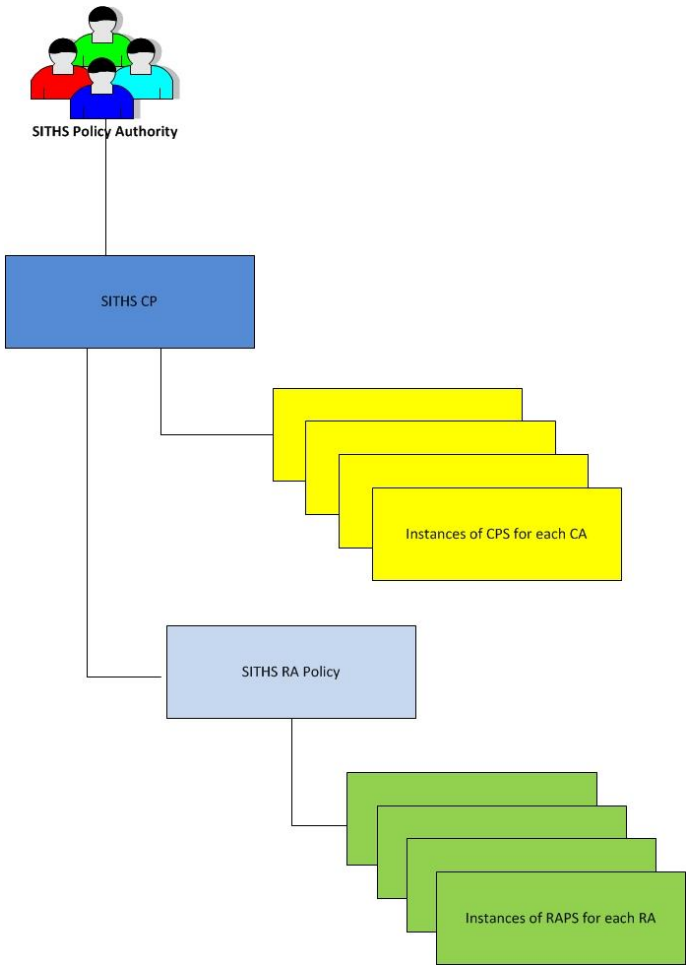

Diagram 1 – SITHS policy structure

Certification Authorities operate under the SITHS CP, issuing certificates.

Registration Authorities (RAs) are entities that authenticate certificate requests within SITHS. Inera AB and organizations that are members of SITHS can act as RAs for certificates they issue.

Depending on the type of certificate, digital certificates may be used by subscribers in a wide set of services, for example:

- Secure communication to/from websites
- Digitally sign code or other content
- Digitally sign documents and/or e-mails

The person who ultimately receives a signed document or communication, or accesses a secured website is referred to as a relying party, i.e., he/she is relying on the certificate and has to make a decision on whether to trust it or not. A relying party must rely on a certificate in terms of the relevant relying party agreement included in the certificate.

This certificate policy describes the procedures and routines that are applied when issuing certificates within SITHS for:

- Physical persons
- Functions/services

Within SITHS, certificates are issued according to different certificate profiles that govern certificate contents and possible subscribers, these profiles are labeled as HCC.

A CA that operates within SITHS must publish a Certification Practice Statement (CPS) that is approved by the SITHS Policy Authority. A CA without an approved CPS will not become a part of SITHS.

RAs that operate within SITHS must adhere to the SITHS Registration Authority Policy and publish a Registration Authority Practice Statement (RAPS) that is approved 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 for this CP is: 1.2.752.74.8.1.1.1

1.3 PKI participants

1.3.1 Certification authority (CA)

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

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

In accordance with this CP a CA must:

1. Guarantee that all information within issued certificates is correct and verified in accordance with this CP.
2. Generate keys for HCC Function when the RA requests this
3. Issue HCC certificates according to HCC Profiles approved by the SITHS Policy Authority
4. Provide information for repositories in accordance with section 2.1

5. Conduct audits in accordance with this CP
6. Conduct subject identification in accordance with chapter 3
7. Provide subscribers and trusting parties, that use issued certificates, with appropriate information as dictated by this CP and in accordance with applicable laws and regulations
8. Revoke certificates and issue revocation lists in accordance with chapter 4

Each CA that is part of the SITHS PKI must publish a CPS that is approved by the SITHS Policy Authority. Each CPS must also contain a reference to this CP.

Each CA is responsible for maintaining sufficient resources in the form of monetary means and insurances to be able to fulfill its duties according to this CP. The SITHS Policy Authority prohibits CAs from SITHS that cannot meet this requirement.

Inera AB must have a valid and signed agreement with each organization that certificates are issued to. Each agreement must refer to this CP.

1.3.2 Registration authorities (RA)

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

Each RA must operate in accordance with the SITHS RA Policy and have a RAPS published and approved by the SITHS Policy Authority. Each RA is accountable for the fulfillment of all stipulations of the SITHS RA Policy.

1.3.3 Subscribers

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

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

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

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

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

1.3.4 Relying Parties

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

1.3.5 Other Participants

Processing centers are entities that create secure facility housing, among other things, the cryptographic modules used for the issuance of certificates. Processing centers act as CAs within SITHS and perform all certificate lifecycle services of issuing, managing, revoking, and renewing certificates.

1.4 Certificate usage

1.4.1 Appropriate certificate uses

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

1.4.2 Prohibited certificate uses

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

1.4.3 Assurance levels and certificate categories

The CA-hierarchy is established according to diagram 2 below.

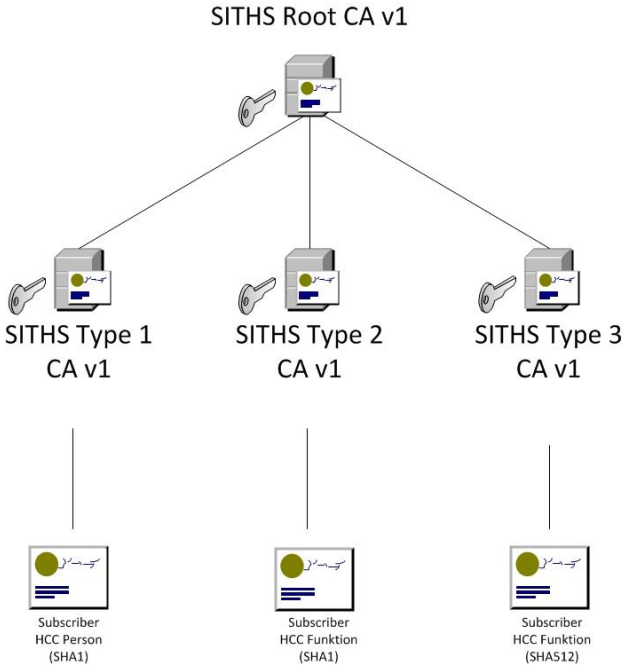

Diagram 2 – The SITHS CA hierarchy, the key symbol indicates the usage of HSM technology for CA keys

Based on the policy identifier within issued certificates it is possible to identify which policy that has been used in the issuance process and which certificate category that the issued certificate belong to. The different certificate categories are described below, note that in cases where the certificate category requires a certain technical solution (e.g. cryptographic module type) the entire certificate chain must meet such requirements.

1. HCC Function
    a. Low Assurance 1.2.752.74.8.3.1
    b. Medium Assurance 1.2.752.74.8.3.2
    c. High Assurance 1.2.752.74.8.3.3
    d. Very High Assurance 1.2.752.74.8.3.4
2. HCC Person
    a. Low Assurance 1.2.752.74.8.3.1
    b. Medium Assurance 1.2.752.74.8.3.2
    c. High Assurance 1.2.752.74.8.3.3
    d. Very High Assurance 1.2.752.74.8.3.4

1.4.3.1 Assurance levels HCC Function

Low Assurance: Low assurance certificates are certificates that should not be used for authentication purposes or to support Non-repudiation. The digital signature provides modest assurances that a message originated from a specific sender. The Certificate, however, provides no proof of the identity of the subscriber. Certificates issued at this assurance level must meet requirements stated within the

NIST SP 800-63-1 Assurance level 1. Certificates issued in accordance with this level are marked with the following policy identifier:

- 1.2.752.74.8.3.1

Medium Assurance: This is an assurance level for use in scenarios where moderate risks for harmful or malicious actions are present and can have medium impact on subscribers and/or relying parties. Certificates issued at this assurance level must meet requirements stated within the NIST SP 800-63-1 Assurance level 2. Certificates issued in accordance with this level are marked with the following policy identifier:

- 1.2.752.74.8.3.2

High Assurance: This is an assurance level for use in scenarios where high risks for harmful or malicious actions are present and can have high impact on a subscribers and/or relying parties. Certificates issued at this assurance level must meet requirements stated within the NIST SP 800-63-1 Assurance level 3. Certificates issued in accordance with this level are marked with the following policy identifier:

- 1.2.752.74.8.3.3

Very High Assurance: This is an assurance level for use in scenarios where the highest level of assurance is required for protection of information and services that utilize certificates issued by SITHS. Typically high risks for harmful or malicious actions are present and can have high impact on a subscribers and/or relying parties. Certificates issued at this assurance level must meet requirements stated within the NIST SP 800-63-1 Assurance level 4. Certificates issued in accordance with this level are marked with the following policy identifier:

- 1.2.752.74.8.3.4

1.4.3.2 Assurance levels HCC Person

Low Assurance: Low assurance certificates are certificates that should not be used for authentication purposes or to support Non-repudiation. The digital signature provides modest assurances that a message originated from a specific sender. The Certificate, however, provides no proof of the identity of the subscriber. Certificates issued at this assurance level must meet requirements stated within the NIST SP 800-63-1 Assurance level 1. Certificates issued in accordance with this level are marked with the following policy identifier:

- 1.2.752.74.8.3.1

Medium Assurance: This is an assurance level for use in scenarios where moderate risks for harmful or malicious actions are present and can have medium impact on subscribers and/or relying parties. Certificates issued at this assurance level must meet requirements stated within the NIST SP 800-63-1 Assurance level 2. Certificates issued in accordance with this level are marked with the following policy identifier:

- 1.2.752.74.8.3.2

High Assurance: This is an assurance level for use in scenarios where high risks for harmful or malicious actions are present and can have high impact on a subscribers and/or relying parties. Certificates issued at this assurance level must meet requirements stated within the NIST SP 800-63-1 Assurance level 3. Certificates issued in accordance with this level are marked with the following policy identifier:

- 1.2.752.74.8.3.3

Very High Assurance: This is an assurance level for use in scenarios where the highest level of assurance is required for protection of information and services that utilize certificates issued by SITHS. Typically high risks for harmful or malicious actions are present and can have high impact on a

subscribers and/or relying parties. Certificates issued at this assurance level must meet requirements stated within the NIST SP 800-63-1 Assurance level 4. Certificates issued in accordance with this level are marked with the following policy identifier:

- 1.2.752.74.8.3.4

1.5 Policy administration

The SITHS Policy Authority is responsible for:

- Defining the requirements and policies for using digital certificates and specifying them in a CP and supporting agreements
- Specifying and approving CP(s) in accordance with a defined review process, including responsibilities for maintaining and tracking changes to the Certificate Policy(s)
- That a defined review process exists to assess that the CP(s) are capable of support by the controls specified in a CPS
- Approving Certification Practice Statements (CPS)
- Maintaining that CPS has been formally assigned
- That CPS are modified and approved in accordance with a defined review process
- That Certification Practice Statements (CPS) are made available to all appropriate parties
- That revisions to CPS are made available to all appropriate parties
- That CAs updates there CPS to reflect changes in the environment as they occur
- Ensuring that CA's control processes, as stated in there Certification Practice Statement (CPS) fully comply with the requirements of the CP
- That CAs addresses the requirements of the CP when developing its CPS
- That CAs assesses the impact of proposed CPS changes to ensure that they are consistent with the CP
- That a defined review process exists to ensure that Certificate Policy(s) are supported by CA's CPS
- Specifying and approving Registration Authority Policy(s)
- That Registration Authority Policy(s) are approved in accordance with a defined review process, including responsibilities for maintaining and tracking changes to the Registration Authority Policy(s)
- That a defined review process exists to assess that the Registration Authority Policy(s) are capable of support by the controls specified in a RAPS
- Make the Registration Authority Policies supported by the CA available to subscribers and relying Parties
- Approving Registration Authority Practice Statements (RAPS)
- That responsibilities for maintaining every RAPS have been formally assigned
- That RAPS are modified and approved in accordance with a defined review process

- That Registration Authority Practice Statements (RAPS) are made available to all appropriate parties. Note that only the SITHS Policy Authority is allowed to make RAPS available outside each RA boundary.
- That revisions to RAPS are made available to appropriate parties. Note that only the SITHS Policy Authority is allowed to make RAPS available outside each RA boundary.
- That RAs updates there RAPS to reflect changes as they occur
- That RA's control processes, as stated in a RAPS, fully comply with the requirements of the SITHS RA Policy
- That RAs addresses the requirements of the SITHS RA Policy when developing its RAPS
- That RAs assesses the impact of proposed RAPS changes to ensure that they are consistent with the SITHS RA Policy
- That a defined review process exists to ensure that Registration Authority Policy(s) are supported by RA's RAPS

The SITHS Policy Authority will at all times also publish a current version of:

- This CP
- CPS for every CA within SITHS
- The SITHS RA Policy
- Relying Party Agreements

1.5.1 Organization administering the document

Inera AB
Östgötagatan 12
118 93 Stockholm
Sweden

1.5.2 Contact Person

SITHS Policy Authority
(address as above)

The SITHS Policy Authority can also be contacted by email on the following address:

sithspolicyauthority@inera.se

1.5.3 Person determining CP suitability for the policy

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

1.5.4 CP approval procedure

Approval of this CP and subsequent amendments shall be made by the SITHS Policy Authority. Amendments shall either be in the form of a document containing an amended form of the CP or an update notice. Amended versions or updates shall be linked to the repository located at http://www.inera.se/siths/dokument/styrande

See section 9.12 regarding management of amendments.

1.6 Definitions and acronyms

See Appendix A for a table of acronyms and definitions.

2 Publication and Repository Responsibilities

2.1 Repositories

Processing centers are responsible for maintaining a publicly accessible online repository. Processing centers, as part of their contracts with Inera AB, publish certificates in repositories based on certificate applications approved by RAs, as well as revocation information concerning such certificates.

The following information is made available at the following locations:

- **CP** - http://www.inera.se/siths/dokument/styrande
- **CPS** - http://www.inera.se/siths/dokument/styrande
- **RA Policy** - http://www.inera.se/siths/dokument/styrande
- **Relying Party Agreements** - http://www.inera.se/siths/dokument/styrande
- **RAPS** - Not published. Are kept in an offline repository by the SITHS Policy Authority.
- **Certificate profiles** - http://www.inera.se/siths/dokument/certifikat
- **CRL** - http://crl1.siths.se and http://crl2.siths.sjunet.org
- **AIA** - http://aia.siths.se and http://aia.siths.sjunet.org
- **OCSP** - http://ocsp1.siths.se and http://ocsp2.siths.sjunet.org

2.2 Publication of certificate information

It is the responsibility of each CA within SITHS to make the following information/services publicly available:

1 A CPS that refer to this CP

2 Revocation lists that contain revoked certificates

3 Issued CA-certificates, self-signed CA-certificates and cross certified certificates for cross certified CAs

4 An OCSP (Online Certificate Status Protocol) responder

Every published revocation list (CRL) provides all available revocation information that is available at the time of publication, but only for certificates that the revocation list in question is intended to provide. The current CRL must also be published to the CA's associated OCSP responder at the time of publication.

CAs shall provide access to CA certificates associated with all public CA keys as long as these can be used for verification purposes.

2.3 Time or frequency of publication

CA information is published promptly after it is made available to a CA within SITHS. SITHS offers CRL and OCSP-services showing the revocation and status of SITHS certificates. CRL for end entity subscriber certificates shall be issued at least once every hour. CRL for CAs that only issue CA certificates shall be issued at least once every 6 months, and also whenever a CA Certificate is

revoked. If a Certificate listed in a CRL expires, it may be removed from later issued CRL after the certificates expiration.

This CP is reviewed by the SITHS Policy Authority every 12 months or according to needs. Changes to the CP are to be published according to section 2.4 and be communicated to subscribers and relying parties. The SITHS Policy Authority communicates by means of SITHS newsletters addressed to SITHS member organizations and by publishing information at http://www.inera.se/siths

2.4 Access controls on repositories

Inera AB shall not intentionally use technical means of limiting access to this CP, CPS, RA Policy, certificates, certificate status information, or CRL/OCSP-services. Inera AB offers free use of certificates, certificate status information and CRL as long as it is used in accordance with the RPA. Inera AB shall implement controls to prevent unauthorized persons from adding, deleting, or modifying repository entries.

3 Identification and Authentication

3.1 Naming

Unless where indicated otherwise in this CP, the relevant CPS or the content of the digital certificate, names appearing in certificates issued under SITHS are authenticated.

3.1.1 Type of names

Every subscriber identity is registered along with a set of attributes. Identities and attributes are verified by involved RAs before a certificate is issued and must also be continuously verified at least every 12 months.

The actual attributes contained within a certificate issued within SITHS is controlled by the certificate profile that a specific certificate is requested and issued in accordance with.

3.1.1.1 Subject types supported within SITHS

Certificates are issued to the following subject types within SITHS:

Subject type	***Certificate profile***	***Certificate type***
Person	HCC Person	Secondary certificate [1]
System or service	HCC Function	Primary certificate [2]

3.1.1.1.1 HCC Person

HCC Person is only issued to physical persons that meet the following base requirements:

1. Can prove a unique identity who's attributes can be controlled and verified by a trusted third party, and
2. Is an employee of, or by a formal agreement connected to, a SITHS member organization.

All attributes not defined as non-verifiable of HCC Person issued under this CP must be controlled and verified by a trusted third party. Trusted third parties include the following entities:

- The Swedish Tax Agency
- The HSA directory

HCC Person is issued as secondary certificates, by connection to a primary certificate. Primary certificates must only be issued by a CA that is trusted, validated and approved by the SITHS Policy Authority. For HCC Person primary certificates are issued by:

- Telia e-legitimation EU HW CA v1
  - 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

[1] *Secondary certificates are issued to a subscriber based on a previously issued primary certificate along with associated asymmetric keys. The SITHS Policy Authority approves trusted issuers of primary certificates that can be tied to secondary certificates.*

[2] *Primary certificates are issued to subscribers along with asymmetric keys and are not dependent on previously issued certificates.*

- SHA1 thumbprint = 8c 6f 3b 02 d0 10 fe 90 c6 0a 1b 44 85 17 5d 2c b3 5f 05 26
- Telia Enterprise CA v2
  - SHA1 thumbprint = 5a 43 0d 1e df da 3a c2 bc ca e5 88 a0 81 0d c3 c8 ad 61 aa
- Telia Enterprise CA v3
  - SHA1 thumbprint = 34 f4 df c8 bf fd ed 15 21 03 74 f2 5e c2 4d 5b 61 43 db e5
- Telia Card Identifier CA v2
  - SHA1 thumbprint = 6e a8 31 00 aa c9 45 20 ac a7 8b 28 7e 24 f1 d8 ee ed 09 5c

These CAs also issue cryptographic modules, where the private key is stored and protected. This means that no separate key pairs are generated for HCC Person in accordance with this CP.

The distinguishing factor for HCC Person is that the subject contains the full name of the subject, which is strongly connected to an organization by means of an HSA-id [3]. The HSA-id for a person is derived from the HSA-id series assigned to the organization hosting the person in question within the HSA directory.

3.1.1.1.2 HCC Function

HCC Function is only issued to named functions or services that can be:

1. An organizational function
2. A technical service or function within an organization

A HCC Function is never issued to a physical person. A function or service in this context is always subordinate to an organization.

All organizations that apply for HCC Function under this CP must be controlled and verified by a trusted third party. Trusted third parties include the following entities:

- The Swedish Companies Registration Office
- Statistics Sweden
- The Swedish Tax Agency

Organizations that are not registered with any of these parties are verified by a combination of:

- A formal signature from an individual that is an authorized signatory for the organization. Organizations that lack an authorized signatory have to get formal signatures from the organizations management committee.
- Verifying that the individual is listed in the organizations list of individuals that are authorized to sign for the organization. This is verified by contacting the administrative management of the organization.

The function that a certificate is issued to is referenced to as a subject in this CP. From a legal perspective the legal person (organization) that is the subscriber of a specific HCC Function is held accountable for the usage of such certificates.

HCC Function is issued as primary certificates. Before issuance a key pair is generated in accordance with section 6.1 in this CP.

[3] *The HSA-id is the unique identifier used for every object within the HSA directory.*

The distinguishing factor for HCC Function is that the subject contains the name of a function, which is strongly connected to an organization by means of HSA-id, but does not contain any information about any physical person. The HSA-id for a function is derived from the HSA-id-series assigned to the organization hosting the function in question within the HSA directory.

3.1.1.2 HCC Person certificate profile

The certificate profile is described in SITHS HCC Profile

3.1.1.3 HCC Function certificate profile

The certificate profile is described in SITHS HCC Profile

To be noted is that HCC Function does not make use of the “state” attribute that some CSR generators typically present. Attributes that are not part of the certificate profile that the request refers to shall not be included in the CSR, if this is the case the certificate request will be denied.

3.1.2 Need for names to be meaningful

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.

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

The unique identifier within a certificate serves as the general identification attribute for the end entity subscriber. For SITHS the unique identifier for all kinds of end entities are equal to the HSA-id for the person/function as represented in the HSA directory. The primary purpose of the unique identifier is to make sure that end entity subscribers are unique. All distinguished names (DN) of end entities are guaranteed to be unique within SITHS by means of the HSA-id associated with the subject. A HSA-id is generated in accordance with the HSA directory policy.

Organization names are to be equal to the subscriber organizations officially registered names with the government authorities within the specified country. All organization names shall be verified in accordance with section 3.1.1.1.2 in this CP. An exception to this rule is made for county councils and municipalities that can use their public names.

Organizational unit is a named entity that represents either a business unit or organizational branch within the subscriber organization that holds a specific end entity certificate. The names of organizational units are arbitrary specified according to the needs of subscriber organizations.

Subscribers are identified by using a combination of the attributes associated with the certificate profile in use for a specific certificate request, as long as the combination includes all mandatory attributes and contains a unique identifier.

3.1.2.1 HCC Person attributes

The subject attributes are described in SITHS HCC Profile

3.1.2.2 HCC Function attributes

The subject attributes are described in SITHS HCC Profile

3.1.3 Anonymity or pseudonymity of subscribers

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

3.1.4 Rules for interpreting various name forms

No stipulations.

3.1.5 Uniqueness of names

The names of subscribers within SITHS shall be unique by means of the mandatory HSA-id unique identifier. This applies to all certificate profiles.

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 others. 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. Inera AB and SITHS member organizations 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 method to prove possession of a private key shall be PKCS #10 or other cryptographically equivalent demonstrations. This requirement does not apply where a key pair is generated by a CA on behalf of a subscriber, for example when PKCS#12-objects are issued When PKCS#12-objects are issued the authorized representative for the certificate is separate issued a PIN-code that must be used in order to unlock the PKCS#12-object.

3.2.2 Authentication of organization identity

Whenever a certificate contains an organization name, the identity of the organization and other enrollment information provided by certificate applicants (except for non-verified subscriber information) is to be confirmed in accordance with the procedures set forth by the SITHS Policy Authority.

The subscriber organization is to be authenticated by means of an authorized representative for the specified organization.

The rules for appointing authorized representatives for each subscriber organization are specified in each RAPS.

3.2.2.1 Authentication of functions within organizations

When requesting a certificate for an organizational function (HCC function) a signed application form from an authorized representative for the specified organization is required. This application form must also state the common name of the function that the request applies to. RAs shall verify that the request comes from an authorized representative.

3.2.2.2 Authentication of authorized representative

Authorized representatives shall be authenticated in accordance with section 3.2.3.1 in this CP. Distribution of private keys and codes associated with keys require physical presence from the authorized representative that applied for the certificate. An alternative to this is that codes are delivered by means of encrypted S/MIME to the authorized representative that made the request. The authorized representative shall in that case us a SITHS HCC Person certificate to receive and decrypt the S/MIME message.
If the xRA has an established and prolonged relation with the authorized representative the authenticated may be done with a physical meeting, or other equivalent method, with no other identification.
RAs that cannot fulfill these requirements can however develop equivalent methods; such methods must be approved by the SITHS Policy Authority and shall be documented in the RAPS of RAs that employ such other approved methods.

3.2.2.3 Verification of domain ownership

Domain ownership is verified for all HCC Function before such certificates are issued. Each SITHS member organization must register domains for which they wish to issue certificates with the SITHS Policy Authority. The SITHS Policy Authority then verifies domain ownership with the parent domain owner. If verification is successful the SITHS Policy Authority approves the member organization to issue certificates for the domain in question. The SITHS Policy Authority reviews and verifies the domain owner list associated with each member organization every three months, if a member organization no longer is the owner of a registered domain all certificates that are issued to that domain shall be revoked.

A SITHS member organization may issue certificates for domains owned by another organization if a written consent is presented to and approved by the SITHS Policy Authority. The consent shall contain the exact address or the domain in question and it should be signed by the domain owing organization. The original consent shall be archived by the certificate issuing SITHS membership organization in accordance with Section 5.5.2. Control of ownership is performed as above.

All domain owner verifications shall be documented and archived by the SITHS Policy Authority in accordance with Section 5.5.2.

3.2.3 Authentication of individual identity

End entities are to be identified according to section 3.3.3.1 in this CP. An RA, or xRA appointed by an RA, within a subscriber organization investigates if the requesting person fulfills all requirements in order to be authorized to enroll for the certificate that the request specifies.

Approval of the request can be conducted at the time of the request and/or when the requesting person receives the certificate, the RA, or xRA, then specifies how the requesting person has identified itself. The RA, or xRA, then digitally signs that identity control has been conducted according to chapter 3 in this CP.

3.2.3.1 Requirements for identity control

Identity control is conducted by means of one of the following procedures:

1 The end entity subscriber proves its identity by means of a valid and approved ID card. Approved ID-cards are those defined in SBC 151-U with the following additions:
- Swedish Tax Agency ID-card

2 The end entity subscriber identifies itself and signs the request by means of a valid and approved electronic ID. Approved electronic IDs include:

- Telia electronic ID, issued by:
  - **Telia e-legitimation EU HW CA v1**
    (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**
    (SHA1 thumbprint = 8c 6f 3b 02 d0 10 fe 90 c6 0a 1b 44 85 17 5d 2c b3 5f 05 26)
  - **Telia Enterprise CA v2**
    (SHA1 thumbprint = 5a 43 0d 1e df da 3a c2 bc ca e5 88 a0 81 0d c3 c8 ad 61 aa
  - **Telia Enterprise CA v3**
    (SHA1 thumbprint = 34 f4 df c8 bf fd ed 15 21 03 74 f2 5e c2 4d 5b 61 43 db e5
    These four electronic ID contains information about the identity of the end entity subscriber and are issued after identification in accordance with point 1 above. They can be used to renew HCC Person on already extradited cards and to digitally sign the extradition itself.
  - **Telia Card Identifier CA v2**
    (SHA1 thumbprint = 6e a8 31 00 aa c9 45 20 ac a7 8b 28 7e 24 f1 d8 ee ed 09 5c)
    Generic certificate present on smartcards without information about the end entity subscriber. It is used to retrieve a temporary HCC Person. Mainly used when a card is lost or for substitute workers. Extradition of such cards requires physical identification of the end entity subscriber according to point 1 above or point 3 or 4 below. Can subsequently be used to retrieve renewals of SITHS HCC Person for the same end entity subscriber to the same smartcard.

3 Subscribers that cannot identify themselves by means of an approved ID-card can be identified by means of proxy identification invoked by the subscriber's organizational manager or some other person that have a responsibility for the subscriber within the organization. Such proxy identification also means that the person doing the proxy identification is held responsible for correctness of the subscriber identity and is documented as part of the certificate application. A xRa is not allowed to perform a proxy identification.

4 When issuing a temporary HCC on a smartcard with a Telia Card Identifier CA v2 the end entity can be identified by means of proxy identification invoked by two colleagues with valid HCC. Such proxy identification also means that the two persons are held responsible for correctness of the subscriber identity and are documented as part of the certificate application.

5 When issuing a temporary HCC on a smartcard with a Telia Card Identifier CA v2 the end entity can be identified by means of proxy identification invoked by a colleague that:
• can access the unit's temporary smartcard,
• can verify the end user identification
• and, after contacting a xRA, can answer the phone call that the xRA makes to the phone number that is pre-registered in the callback list for that organizational unit.
Such proxy identification also means that the person who is submitting the smartcard is held responsible for correctness of the subscriber identity and are documented as part of the certificate application.

Electronic identity control that is conducted at the time of the request does not require physical presence by the end entity subscriber. All other forms of identity control require physical presence.

3.2.3.2 Procedure for authentication

Before a certificate is generated, all end entity attributes are controlled and verified against the HSA directory. A certificate will only be generated if all controls pass without exceptions.

3.2.4 Non-verified subscriber information

All subject information shall be verified by RAs with the following exceptions:

- HCC Person
  - Organizational Unit
  - Title

- HCC Function
  - Organizational Unit

Note that subscribers are responsible for verifying information within certificates when they are issued, as part of the certificate acceptance responsibilities.

3.2.5 Validation of authority

Whenever an individual's name is associated with an organization name in a certificate in such a way to indicate the individuals affiliation or authorization to act on behalf of the organization the RA-organization determines that the individual exists within the boundaries of the RA-organization and that the individual is authorized to act on behalf of the organization by verifying this with the individuals business manager. If unsuccessful such certificate applications will be denied.

3.2.6 Criteria for interoperation

SITHS may provide interoperation services that allow a non-SITHS CA to be able to interoperate with one or more SITHS CAs by unilaterally certifying that CA. CAs enabled to interoperate in this way will comply with this CP as supplemented by additional policies when required.

3.3 Identification and authentication for re-key requests

3.3.1 Identification and authentication for routine re-key

SITHS do not allow re-key requests for issued end entity certificates. CA certificates may be re-keyed under the stipulations of chapter 6 in this CP.

3.3.2 Identification and authentication for re-key after revocation

SITHS do not allow re-key requests for issued end entity certificates.

3.4 Identification and authentication for revocation request

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

- The certificate subscriber
- The RA-entity that approved the certificate application
- The applicable processing center
- The SITHS Policy Authority

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

Revocation 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. Subscriber can revoke their own HCC Person certificates
	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.
RA or other authorized representative for RA	Administration portal	Authentication by mutual TLS with a certificate issued by SITHS CA v3 or SITHS Type 1 CA v1. Only certain system roles may perform revocation operations.
	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.
Authorized representative for CA (processing center CA operator or SITHS PA)	Administration portal	Authentication by mutual TLS with a certificate issued by Telia Officers CA v2 or Telia Officers CA v3. Only certain system roles may perform revocation operations.
	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.

If key compromise is suspected for a private key associated with an issued certificate, the certificate is allowed to be revoked even if the above identification and authentication requirements cannot be completely fulfilled. Information about such revocations shall however be passed on to the associated RA and the SITHS Policy Authority.

The method for identification and authentication for every revocation request shall be logged by the CA, along with eventual reasons for simplified identification and authentication.

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:

- Individual who is the subject of the certificate and who is an employee of, or by a formal agreement is connected to, a SITHS member organization.
- Authorized representatives of an organization
- Authorized representatives of a CA
- RAs or authorized representatives of an RA

4.1.2 Enrollment process and responsibilities

4.1.2.1 End entity certificate subscribers

All end entity certificate subscribers shall manifest assent to the relevant subscriber and undergo an enrollment process consisting of:

- Completing a certificate application and providing true and correct information
- Generating, or arranging to have generated, a key pair
- Delivering his, her, or its public key, directly or through an RA, to the processing center
- Demonstrating possession and/or exclusive control of the private key corresponding to the public key delivered to the processing center

4.1.2.2 CA and RA Certificates

Subscribers of CA and RA certificates enter into a contract with the SITHS Policy Authority that will issue the CA or RA Certificate. CA and RA applicants shall provide their credentials to demonstrate their identity and provide contact information during the contracting process. During this contracting process or, at the latest, prior to the key generation ceremony to create a CA or RA key pair, the applicant shall cooperate with the SITHS Policy Authority to determine the appropriate distinguished name and the content of the certificates to be issued to the applicant.

4.2 Certificate Application Processing

4.2.1 Performing identification and authentication functions

An RA, or xRA, shall perform identification and authentication of all required subscriber information according to the requirements in chapter 3.

A certificate application must fulfill the following procedures:

1. RA or other authorized representative for RA fills out application forms and signs the application ensuring that all applicable terms and conditions are accepted. In this procedure the subscriber declares all relevant subscriber information according to chapter 3.
2. The subscriber is identified and authenticated according to chapter 3 in this CP. All subscriber information is also verified according to chapter 3 in this CP.
3. Application forms are archived in accordance with Section 5.5.2.

4.2.2 Approval or rejection of certificate applications

An RA will approve an application for a certificate if the following criteria are met:

- Successful identification and authentication of all required subscriber information in terms of chapter 3 in this CP.

An RA will reject a certificate application if:

- Identification and authentication of all required subscriber information in terms of chapter 3 in this CP cannot be completed
- The subscriber fails to furnish supporting documentation upon request
- The subscriber fails to respond to notices within a specified time
- The RA believes that issuing a certificate to the subscriber may bring SITHS into disrepute

4.2.3 Time to process certificate applications

CAs and RAs begin processing certificate applications within a reasonable time of receipt. There is no time stipulation to complete the processing of an application unless otherwise indicated in the relevant subscriber agreement, CPS or other agreement between SITHS participants.

A certificate application remains active until rejected.

4.3 Certificate issuance

4.3.1 CA actions during certificate issuance

A certificate is created and issued following the approval of a certificate application by a CA or following receipt of an RA request to issue the certificate. The CA creates and issues to a certificate applicant a certificate based on the information in a certificate application following approval of such certificate application.

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

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

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

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

4.3.2 Notifications to subscriber by the CA of issuance of certificate

CAs issuing certificates to end entity subscribers shall, either directly or through an RA, notify subscribers that they have created such certificates, and provide subscribers with access to the certificates by notifying them that their certificates are available and the means for obtaining them. Certificates shall be made available to end entity subscribers, either by means of an xRA, allowing them to download them from a web site or via a message sent to the subscriber containing the certificate.

inera
LANDSTING OCH REGIONER
I SAMVERKAN FÖR E-HÄLSA

4.4 Certificate acceptance

4.4.1 Conduct constituting certificate acceptance

The following conduct constitutes certificate acceptance:

- Downloading a certificate or installing a certificate from a message attaching it constitutes the subscribers acceptance of the certificate.
- Accepting a card with a certificate on constitutes the subscribers acceptance of the certificate.

Failure of the subscriber to object to the certificate or its content constitutes certificate acceptance.

4.4.2 Publication of the certificate by the CA

CAs publishes the certificates they issue in HSA as an attribute of the directory object that represents the certificate subject.

4.4.3 Notification of certificate issuance by the CA to other entities

RAs may receive notification of the issuance of certificates they approve.

4.5 Key pair and certificate usage

4.5.1 Subscriber private key and certificate usage

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

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

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

4.5.2 Relying party public key and certificate usage

Relying parties shall assent to the terms of the applicable relying party agreement as a condition of relying on the certificate.

Reliance on a certificate must be reasonable under the circumstances. If the circumstances indicate a need for additional assurances, the relying party must obtain such assurances for such reliance to be deemed reasonable. Before any act of reliance, relying parties shall independently assess:

- The appropriateness of the use of a certificate for any given purpose and determine that the certificate will, in fact, be used for an appropriate purpose that is not prohibited or otherwise restricted by this CP. SITHS CAs, and RAs are not responsible for assessing the appropriateness of the use of a certificate.
- That the certificate is being used in accordance with the KeyUsage field extensions included in the certificate.

- The status of the certificate and all the CAs in the chain that issued the certificate. If any of the certificates in the certificate chain have been revoked, the relying party is solely responsible to investigate whether reliance on a digital signature performed by an end entity subscriber certificate prior to revocation of a certificate in the certificate chain is reasonable. Any such reliance is made solely at the risk of the relying party.

Assuming that the use of the certificate is appropriate, relying parties shall utilize the appropriate software and/or hardware to perform digital signature verification or other cryptographic operations they wish to perform, as a condition of relying on certificates in connection with each such operation. Such operations include identifying a certificate chain and verifying the digital signatures on all certificates in the certificate chain.

4.6 Certificate renewal

Certificate renewals are conducted in the same manner as new certificate applications.

4.7 Certificate re-key

SITHS do not allow re-key requests for existing issued end entity certificates. CA certificates may be re-keyed under the stipulations of chapter 6 in this CP.

4.8 Certificate modification

Certificate modifications are conducted in the same manner as new certificate applications.

4.9 Certificate revocation and suspension

CAs provides means for revocation of issued certificates. Functionality for temporary revocations is not available. The revocation service is always available. Each CA continuously creates signed revocation lists (CRL). The latest version is always stored at the following locations:

- http://crl1.siths.se/
- http://crl2.siths.sjunet.org/

Revocation lists must always be available in relation to the requirements from relying parties to be able to verify the validity of an issued certificate. The current revocation list from a CA contains information for each revoked certificate that the validity period has not expired for.

Revocation controls can also be executed by using an OCSP service associated with a subscriber certificate. All CAs shall use the following OCSP responders:

- http://ocsp1.siths.se
- http://ocsp2.siths.sjunet.org

The contents of such OCSP-services must be as up to date as the issued revocation lists. Every CA within SITHS shall express how this is assured in its associated CPS.

4.9.1 Circumstances for revocation

A CA revokes issued certificates under the following circumstances:

- If any of the information contained within a certificate is changed
- If receiving a revocation request according to section 3.4 in this CP
- If suspecting that a private key associated with a certificate is compromised or used by some entity that is not the subscriber
- If suspecting that the smart card or equivalent cryptographic module that contains the private key is no longer in use, or possessed, by the subscriber
- If suspecting that the subscriber violates this CP
- If a used CA-key is suspected of compromise
- If a CA ends its duties as a CA

If an RA, or xRA, ends its duties as RA or xRA their certificates shall only be revoked if the personal smart card will also be revoked. If the smart card is not to be revoked only the RA and xRA permissions shall be revoked within SITHS.

RAs and xRAs have the ability to revoke smart cards and certificates outside its own RA boundary if:

1 The subscriber have an existing smart card and certificates issued from another SITHS RA boundary, and
2 The RA or xRA will issued a new smart card with certificates that replace the previously issued smart card and certificates

If a CA revokes a certificate in accordance with one of the above circumstances under a mistake of fact the CA's responsibilities are determined by the SITHS Policy Authority from case to case.

4.9.2 Who can submit a revocation request

Revocation requests can be made by:

- RA
- xRA authorized by RA
- Authorized representative for SITHS member organization
- Certificate subscriber

A CA can however decide to revoke a certificate based on information gathered from other part if this is in alignment with section 3.2.9 of this CP.

4.9.3 Procedure for revocation request

A revocation service connected to every SITHS CA that issue certificates receive the request for revocation. The request must be signed by an authorized individual according to section 3.2.9 of this CP.

All revocation requests are archived along with the following information:

- How the request was received
- When the request was received
- The reason for revocation
- How the individual that requested the revocation was identified and authenticated
- The result of the revocation request
- The time of publication in revocation list
- A unique log-ID for the revocation request

4.9.4 Revocation request grace period

Revocation requests shall be submitted as promptly as possible within a commercially 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. In doubtful situations the decision can however be postponed until sufficient confirmation is given, there is no maximum time for such confirmations.

4.9.6 Revocation checking requirements for relying parties

Relying parties shall check the status of certificates on which they wish to rely. One method by which relying parties may check certificate status is by consulting the most recent CRL from the CA that issued the certificate on which the relying party wishes to rely. Alternatively, relying parties may meet this requirement by checking certificate status using the applicable OCSP-service. CAs shall provide relying parties with information on how to find the appropriate CRL or OCSP responder to check for revocation status.

- For SITHS CAs, CRLs are posted in the Inera AB repository at http://crl1.siths.se and http://crl2.siths.sjunet.org
- OCSP-services are available at http://ocsp1.siths.se and http://ocsp2.siths.sjunet.org

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.

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

- The revocation control is made against a current revocation list
- The revocation list is still valid
- The digital signature of the revocation list is valid

4.9.7 CRL issuance frequency

CRLs issued by issuing CAs are issued at least once every hour during all days of a year. Issuing CA CRLs shall have its nextUpdate attribute set to 48 hours after the issuance of the CRL.

CRLs issued by Root CAs are issued at least every six months, but also whenever a CA certificate is revoked. Root CA CRLs shall have its nextUpdate attribute set to 1 year after the issuance of the CRL.

If a certificate listed in a CRL expires, it may be removed from later issued CRLs.

Situations when the function that updates revocation lists is unavailable shall be regulated in accordance with the applicable Service Level Agreements signed with processing centers hosting the SITHS revocation function. Each CA's CPS shall state the applicable service availability guarantees that are governed by the CA's Service Level Agreements.

Any deviation from this general policy must get approval from the SITHS Policy Authority and be published in the appropriate CPS.

4.9.8 Maximum latency for CRLs

The publication to the CRL repositories shall not occur more than 20 minutes after the CRL generation if a revocation has taken place and not more than 120 minutes after if no changes have been made. Revocation information that is updated more frequently is provided by means of Online Certificate Status Protocol (OCSP), see 4.9.9
Each CA shall state the publication interval for each CRL repository in its CPS.

4.9.9 On-line revocation/status checking availability

Online revocation and other certificate status information are available via a web-based repository and, where offered, OCSP. Each CA within SITHS shall have a web-based repository that permits relying parties to make online inquiries regarding revocation and other certificate status information. The SITHS Policy Authority provides relying parties with information on how to find the appropriate repository to check certificate status and how to find the correct OCSP responder. Every end entity certificate issued by a CA within SITHS will also publish this information within issued certificates.

OCSP services shall at least every 15 minutes update its revocation information by checking the current CRL for each CA it is connected to.

4.9.10 On-line revocation checking requirements

A relying party must check the status of a certificate on which he/she/it wishes to rely. If a relying party does not check the status of a certificate on which the relying party wishes to rely by consulting the most recent relevant CRL, the relying party shall check certificate status by consulting the applicable repository or by requesting certificate status using the applicable OCSP responder.

4.9.11 Other forms of revocation advertisements available

Not applicable.

4.9.12 Special requirements regarding key compromise

SITHS participants shall be notified of an actual or suspected CA private key compromise using commercially reasonable efforts. Processing centers shall use commercially reasonable efforts to notify potential relying parties if they discover, or have reason to believe, that there has been a compromise of the private key of one of the CAs.

4.9.13 Circumstances for suspension

SITHS do not allow suspension for existing issued end entity certificates.

4.10 Certificate status services

4.10.1 Operational characteristics

The status of public certificates is available via CRL/OCSP-service through a processing center (at a URLs specified within each issued certificate).

4.10.2 Service availability

Certificate status services shall be available 24x7 excluding scheduled interruptions that are approved by the SITHS Policy Authority.

4.10.3 Optional features

No stipulations.

4.11 End of subscription

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

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

4.12 Key escrow and recovery

No SITHS participant may escrow CA, RA or end entity subscriber private keys.

5 Facility, management, and operational controls

5.1 Physical controls

Physical controls refer to the physical protection of sites, equipment and information that are related to CAs. The goals of physical controls are to prevent unauthorized physical access, damage and disruptions. These controls must be related to the risks and threats that CAs within SITHS are subject to.

CAs are required to be protected by a combination of perimeter protection, fire- and water protection, access controls and routines for work in protected areas.

Stipulations for RA physical controls are described in RAP

5.1.1 Site location and construction

All SITHS CA operations shall be conducted within a physically protected environment that deters, prevents, and detects unauthorized use of, access to, or disclosure of sensitive information and systems.

Such requirements are based in part on the establishment of physical security tiers. A tier is a barrier such as a locked door or gate that provides mandatory access control for individuals and requires a positive response (e.g., door or gate unlocks or opens) for each individual to proceed to the next area. Each successive tier provides more restricted access and greater physical security against intrusion or unauthorized access.

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 each tier can be accessed only by authorized personnel.

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

The secure facilities of CAs shall be equipped with primary and backup power systems to ensure continuous, uninterrupted access to electric power. Also, these secure facilities shall be equipped with primary and backup heating/ventilation/air conditioning systems to control temperature and relative humidity.

5.1.4 Water exposures

The secure facilities of CAs shall be constructed and equipped, and procedures shall be implemented, to prevent floods or other damaging exposure to water.

5.1.5 Fire prevention and protection

The secure facilities of CAs shall be constructed and equipped, and procedures shall be implemented, to prevent and extinguish fires or other damaging exposure to flame or smoke. These measures shall meet all local applicable safety regulations.

5.1.6 Media storage

CAs shall protect the magnetic media holding back ups of critical system data or any other sensitive information from water, fire, or other environmental hazards, and shall use protective measures to deter, detect, and prevent the unauthorized use of, access to, or disclosure of such media. CAs shall describe its media storage procedures in its CPS.

5.1.7 Waste disposal

CAs shall implement procedures for the disposal of waste (paper, media, or any other waste) to prevent the unauthorized use of, access to, or disclosure of waste containing confidential/private information. CAs shall describe its waste disposal procedures in its CPS.

5.1.8 Off-site backup

CAs shall maintain backups of critical system data or any other sensitive information, including audit data, in a secure off-site facility. CAs shall describe its off-site backup capabilities in its CPS.

5.2 Procedural controls

Employees, contractors, and consultants that are designated to manage infrastructural trustworthiness shall be considered to be “trusted persons” serving in a “trusted position.” Persons seeking to become trusted persons by obtaining a trusted position shall meet the screening requirements of this CP.

Trusted Persons include, but are not limited to:

- System administration personnel
- Designated engineering personnel
- Executives that are designated to manage infrastructural trustworthiness

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

- The validation of information in certificate applications
- The acceptance, rejection, or other processing of certificate applications, revocation requests, or renewal requests, or enrollment information
- The issuance or revocation of certificates, including (in the case of Processing Centers) personnel having access to restricted portions of its repository or the handling of subscriber information or requests.

5.2.1 Trusted roles

The following roles are specified for administration, operation and maintenance for a CA within SITHS:

Role	***Explanation/tasks***
Certification Authority Administrator (CAA)	Administrative/operational personnel 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 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 CAs 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.

A CA can however choose to further divide the permissions of the roles described above into more granular roles if necessary. The implementation of trusted roles is to be included in the CPS of every CA.

5.2.2 Number of persons required per task

CAs and RAs shall establish, maintain, and enforce rigorous control procedures to ensure the segregation of duties based on job responsibility and to ensure that multiple trusted persons are required to perform sensitive tasks.

Policy and control procedures are in place to ensure segregation of duties based on job responsibilities. The most sensitive tasks, such as access to and management of CA cryptographic hardware (cryptographic signing unit or CSU) and associated key material, require multiple trusted persons.

These internal control procedures are designed to ensure that, at a minimum, two trusted personnel are required to have either physical or logical access to the device. Access to CA cryptographic hardware is strictly enforced by multiple trusted persons throughout its lifecycle, from incoming receipt and inspection to final logical and/or physical destruction. Once a module is activated with operational keys, further access controls are invoked to maintain split control over both physical and logical access to the device.

The trusted roles for CAs are assigned to at least two persons each. A person that holds either the ISSO or SA role must not also be assigned the other role.

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.

5.2.3 Identification and authentication for each role

CAs and RAs shall confirm the identity and authorization of all personnel seeking to become trusted before such personnel are:

- Issued with their access devices and granted access to the required facilities
- Given electronic credentials to access and perform specific functions on information systems and CA or RA systems

Authentication of identity shall include the personal (physical) presence of such personnel before trusted persons performing HR or security functions within an entity, and a check of well-recognized forms of identification, such as passports and drivers licenses. Identity shall be further confirmed through background checking procedures specified in this CP.

Identification and authentication of roles in a CA system are to meet the following requirements:

- Identification and authentication of the SA role is handled by the operating system hosting a CA system
- Identification and authentication of CAA is handled by the CA system and requires multifactor authentication by using personal operating smart cards that at least meet the same assurance level as the highest assurance level issued by the CA that the CAA is provided access to, as defined by this CP.

5.2.4 Roles requiring separation of duties

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

- The validation of information in certificate applications
- The acceptance, rejection, or other processing of certificate applications, revocation requests, key recovery requests or renewal requests, or enrollment information
- The issuance, or revocation of certificates, including personnel having access to restricted portions of a repository
- The handling of subscriber information or requests
- The generation, issuing or destruction of a CA certificate
- The loading of a CA to a production environment

5.3 Personnel controls

The SITHS Policy Authority has documented detailed personnel control and security policies for CAs and RAs to adhere to and be audited against. These personnel controls contain sensitive information and are only available to SITHS member organizations after explicit agreement with the SITHS Policy Authority. An overview of the requirements is described in the subsections following.

5.3.1 Qualifications, experience, and clearance requirements

CAs and RAs shall require that personnel seeking to become trusted persons present proof of the requisite background, qualifications, and experience needed to perform their prospective job responsibilities competently and satisfactorily.

5.3.2 Background check procedures

CAs shall conduct background checks for personnel seeking to become trusted persons. SITHS PA shall conduct background checks for personnel seeking to become RAs. Background checks for these persons shall be repeated at least every three years. These procedures shall be subject to any limitations on background checks imposed by local law.

To the extent one of the requirements imposed by this section cannot be met due to a prohibition or limitation in local law, the investigating entity shall utilize a substitute investigative technique permitted by law that provides substantially similar information, including but not limited to obtaining a background check performed by the applicable governmental agency.

Background investigation of persons seeking to become a trusted person includes:

- A confirmation of current employment
- A check of professional suitability
- A confirmation of relevant education in the field
- A search of criminal records (local, state or provincial, and national)
- Drug tests and/or financial status checks

Reports from background checks shall be evaluated by processing centers and and result in actions that are reasonable in light of the type, magnitude, and frequency of the behavior uncovered by the background check. Such actions may include measures up to and including the cancellation of offers of employment made to candidates for trusted positions or the termination of existing trusted persons.

The use of information revealed in a background check to take such actions shall be subject to applicable law.

5.3.3 Training requirements

CAs and RAs shall provide their personnel with the requisite training needed for their personnel to perform their job responsibilities relating to CA or RA operations competently and satisfactorily. They shall also periodically review their training programs, and their training shall address the elements relevant to functions performed by their personnel.

Training programs must address the elements relevant to the particular environment of the person being trained, including:

- Security principles and mechanisms of SITHS
- Hardware and software versions in use
- All duties the person is expected to perform
- Incident and compromise reporting and handling
- Disaster recovery and business continuity procedures

5.3.4 Retraining frequency requirements

CAs and RAs shall provide refresher training and updates to their personnel to the extent and frequency required to ensure that such personnel maintain the required level of proficiency to perform their job responsibilities competently and satisfactorily.

5.3.5 Job rotation frequency and sequence

No stipulations.

5.3.6 Sanctions for unauthorized actions

No stipulations.

5.3.7 Independent contractor requirements

CAs and RAs 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 by SITHS only to the extent they are escorted and directly supervised by trusted persons.

5.3.8 Documentation supplied to personnel

Inera AB, processing centers and SITHS member organizations shall provide their personnel with (including Trusted Persons) the requisite training and access to other documentation needed to perform their job responsibilities competently and satisfactorily.

5.4 Audit logging procedures

5.4.1 Types of events recorded

The types of auditable events that must be recorded by CAs and RAs are set forth below. All logs, whether electronic or manual, shall contain the date and time of the event, and the identity of the entity that caused the event. CAs shall state in their CPS the logs and types of events they record.
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)
- Failed read and write operations on repositories
- Changes to certificate creation policies e.g., validity period

5.4.2 Frequency of processing log

Audit logs shall be reviewed in response to alerts based on irregularities and incidents within their CA/RA systems. Processing centers shall compare their audit logs with the supporting manual and electronic logs from RAs when any action is deemed suspicious.

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

5.4.3 Retention period for audit log

Audit logs shall be retained for at least ten years after processing and thereafter archived in accordance with Section 5.5.2.

5.4.4 Protection of audit log

Audit logs are 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 in the operating system of CAs
- Making the CAs physically and logically inaccessible for unauthorized persons
- Ensuring access to logs are only given to trusted CA administrators
- Monitoring access to logs by all entities

Logs are verified and consolidated at least once every month under the supervision of at least two individuals with either the SA- or ISSO-roles.

5.4.5 Audit log backup procedures

Incremental backups of audit logs are created daily and full backups are performed weekly.

5.4.6 Audit collection system

No stipulations.

5.4.7 Notification to event-causing subject

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

5.4.8 Vulnerability assessments

Annual revisions of RA organizations are performed to ensure compliance to SITHS Policies and Guideline documents. The CA is also subject to annual revision from external revisers to ensure that it complies with the required guidelines. These two practices help discovering, assessing and fixing administrative and operational vulnerabilities.

To assess technical vulnerabilities penetration tests are performed by external parties. Any findings are documented and prioritized on severity by those performing the test. The CA later assesses and takes actions based on the report. The work is documented for future reference.

Vulnerability scans shall be performed at least quarterly by the supplier of the CA-system.

5.5 Records archival

5.5.1 Types of records archived

The following information is archived continuously:

- Transactions that contain signed requests for certificate issuance and revocation
- Certificate applications signed by RA or other authorized representative
- Signed acceptances for distribution of keys and access codes for keys
- Issued certificates and related updates to certificate repositories
- History for all previous CA-keys, key identifiers and cross certification between different generations of CA-keys
- Requests for revocation and information sent along with revocation requests
- Issued revocation lists and related updates to certificate repositories
- Results from audits of CAs in relation to compliance with this CP
- Terms and conditions and signed agreements for SITHS member organizations
- This CP and all previous versions of the CP
- Current and previous versions of: RAP, CPS, RPA, HCC specification and RAPS

In cases when the archived information consists of digitally signed information, information that is required for signature verification is also archived.

5.5.2 Retention period for archive

All archived information is kept for at least 15 years from the time of data generation.

5.5.3 Protection of archive

An entity maintaining an archive of records shall protect the archive so that only the entities authorized trusted persons are able to obtain access to the archive. The archive is protected against unauthorized viewing, modification, deletion, or other tampering by storage within a trustworthy system. The media holding the archive data and the applications required to process the archive data shall be maintained to ensure that the archive data can be accessed for the time period set forth in this CP.

5.5.4 Archive backup procedures

Entities compiling electronic information shall incrementally back up system archives of such information on a daily basis and perform full backups on a weekly basis. Copies of paper-based records shall be maintained in an off-site secure facility.

5.5.5 Requirements for time-stamping of records

Certificates, CRLs, and other revocation database entries shall contain time and date information. Such time information need not be cryptographic-based.

5.5.6 Archive collection system (Internal or External)

Archive collection systems for entities within SITHS shall be internal, except for RAs. Processing centers shall assist RAs in preserving an audit trail. Such an archive collection system therefore is external to that RA.

5.5.7 Procedures to obtain and verify archive information

Only authorized trusted personnel are able to obtain access to the archive. The integrity of the information is verified when it is restored. Archived information is not available for external individuals other than what is required by law and rulings from a court of law.

Access to information regarding a specific subscriber or CA transaction can be authorized after individual assessment by the SITHS Policy Authority.
Archived information is stored in a manner that ensures readability during the specified archive period.

In the event that a CA ceases with its CA duties within SITHS the CA is still required to provide access to archived information for the entire duration of the archive period. CAs that cannot guarantee this is not allowed to operate within SITHS.

If technology changes occurs that affect access to archived information over time a CA is obligated to either retain the older technology during the archive period or to transfer archived information to current technology.

5.6 Key changeover

A CA certificate may be renewed if the CA's superior entity reconfirms the identity of the CA. Following such reconfirmation, the superior entity shall either approve or reject the renewal application. Following an approval of a renewal request, the superior entity shall conduct a key generation ceremony in order to generate a new key pair for the CA. During such key generation ceremony, the superior entity shall sign and issue the CA a new certificate. 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.

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

5.6.1 Root CA key changeover

When changing Root CA keys the following occur:

- A new self-signed CA certificate is created along with a new key pair
- A cross certificate is issued where the previous CA key is signed by the new CA key
- A cross certificate is issued where the new CA key is signed by the previous CA key
- The certificates above are published in the CA repositories

5.6.2 Issuing CA key changeover

When changing Issuing CA keys the following occur:

- A new CA certificate is requested from the Root CA along with a new key pair by using PKCS#10

- The certificates above are published in the CA repositories

5.7 Compromise and disaster recovery

5.7.1 Incident and compromise handling procedures

Backups of the following CA information shall be kept in off-site storage and made available in the event of a compromise or disaster:

- Certificate application data
- Audit data
- Database records for all certificates issued

Back-ups of CA private keys shall be generated and maintained in accordance with section 6.2.4 in this CP.

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

Following corruption of computing resources, software, and/or data, a report of the incident and a response to the event, shall be promptly made by the affected CA or RA in accordance with processing centers documented incident and compromise reporting and handling procedures in the applicable CPS.

5.7.3 Entity private key compromise procedures

In the event of a CA private key compromise that CA will be revoked. Processing Centers use commercially reasonable efforts to notify potential relying parties if they discover, or have reason to believe, that there has been a compromise of the private key of a CA.

5.7.4 Business continuity capabilities after a disaster

SITHS entities operating secure facilities for CA and RA operations develop, test, maintain and, if necessary, implement a disaster recovery plan designed to mitigate the effects of any kind of natural or man-made disaster. Disaster recovery plans address the restoration of information systems services and key business functions. Disaster recovery sites have the equivalent physical security protections specified by Inera AB.

A disaster can occur during a discontinuity situation or when confidential information is accessible for unauthorized parties. Also flaws in the correctness of information can impose that misinformed decisions are made that could possibly lead to harm for subscribers, relying parties and SITHS member organizations.

All CA are responsible for establishing processes for:

- Risk and threat analysis and management
- Vulnerability analysis and management
- Risk and threat reduction
- Disaster recovery
- Tests of disaster recovery
- Rebuild and restart of services
- Automatic monitoring

- Security upgrades

All CA that are part of SITHS are required to continuously verify that they can be started from recent backups. Such verifications shall occur at least once every three months.

Disaster recovery plans shall be established and consist of routines that cover areas such as:

- Power loss
- Flooding
- Natural disasters
- Fire
- Terrorism
- Technical errors
- Administrative malpractice
- Malicious attacks

Processing Centers have the capability of restoring or recovering essential operations within twenty-four (24) hours following a disaster with, at a minimum, support for the following functions:

- Certificate issuance
- Certificate revocation
- Publication of revocation information

A Processing Centers disaster recovery equipment shall have the physical security protections documented in the CPS for each CA, which includes the enforcement of physical security tiers.

5.8 CA or RA termination

In the event a RA is terminated from SITHS, the RA is obligated to fulfill the following procedures:

- Inform subscribers and other parties that the RA has a relation with, at least three months before termination
- Inform SITHS Policy Authority regarding the termination at least three months before termination

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

- Inform subscribers and other parties that the CA has a relation with, at least three months before termination
- Publicly inform relying parties and SITHS member organizations regarding the termination at least three months before termination
- Cease with issuance of revocation lists that are related to certificates that are signed by 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 regards 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 fulfill the above requirements in a termination situation.

6 Technical security controls

6.1 Key pair generation and installation

6.1.1 Key pair generation

Key pair generation shall be performed using trustworthy systems and processes that provide the required cryptographic strength of the generated keys and prevent the loss, disclosure, modification, or unauthorized use of private keys. CA keys are generated in a key generation ceremony. All key generation ceremonies conform to the requirements in this chapter.

Keys that are created by a CA are generated based on random numbers. The process that generates random numbers is entirely random in a manner that prevents the recreation of a generated random number no matter what knowledge are held in regards to:

- The actual generation process
- The time of generation
- The equipment used to generate the random number

The key generation process is established in a way that prevents keys to be exposed outside the key generation system, except for safe transfers to explicitly defined storage units.
Keys uniqueness is achieved by generating random numbers of a size of a sufficient size that ensures that the probability that multiple keys are identical is negligible.

6.1.1.1 Specific requirements for CA private keys

Generation of CA private keys is executed in the hardware security module where the keys are to be used and stored during the key lifetime. The private keys are to be protected in hardware security modules that are certified according to at least NIST FIPS 140-2 level 3. Hardware security modules are also to be physically protected according to chapter 5 and access to such hardware security modules requires the presence of at least 2 different CAA operators.

6.1.1.2 Specific requirements for subscriber private keys

- SITHS Type 1 CA v1
  Private keys must be either:
  - Generated and stored locally in the chip of a secure cryptographic module in the form of an EID smartcard. These cards shall be certified to at least NIST FIPS 140-2 level 2 or Common Criteria EAL4.
  - Generated centrally in a hardware security module, stored in the chip of a secure cryptographic module in the form of an EID smartcard and then erased from the hardware security module. The hardware security module should be certified according to at least NIST FIPS 140-2 level 3 and physically protected according to chapter 5. The EID smartcards shall be certified to at least NIST FIPS 140-2 level 2 or Common Criteria EAL4.
- SITHS Type 2 CA v1
  The subscriber private keys are either:
  - Generated by the subscriber and the degree of randomization is beyond the control of the CA.
  - Generated centrally in a strongly protected server and stored in a suitable format, then erased from the server's primary memory upon retrieval.
  - Generated centrally in a hardware security module, stored in a suitable format and then erased from the hardware security module. The hardware security module

should be certified according to at least NIST FIPS 140-2 level 3 and physically protected according to chapter 5.

- SITHS Type 3 CA v1
  The private keys are generated by the subscriber and the degree of randomization is beyond the control of the CA.

Subscriber responsibilities regarding private keys are stated in this CP under 9.6.3.

6.1.2 Private Key delivery to subscribers

For HCC Person subscribers, keys and its associated smart card are delivered by secure postal service (registered mail) to the RA-function that approved the certificate request. Forwarding of such mail is not permitted.

Smart cards that are completed for delivery but are not yet sent to its recipient are locked in a controlled storage vault until it is sent.

PIN/PUK-codes associated with smart cards are sent by regular postal service and is delivered to the subject address registered with the Swedish Tax Agency. In the case of smart cards that are issued to persons without a social security number, PIN/PUK codes can be delivered to addresses specified by the local RA organization.

Issuance of new PUK-codes requested by subscribers are sent by secure postal service to the subject address registered with the Swedish Tax Agency

Keys associated with HCC Function certificates that are generated by the issuing CA is only distributed to authorized representatives that have been identified and authenticated in accordance with chapter 3 in the SITHS Certificate Policy. Keys associated with HCC Function are only delivered to authorized representatives after they have been signed for in a formal recipient form; however codes associated with PKCS#12 objects may be delivered to authorized representatives when the CA issues the certificate. Recipient forms are archived in accordance with Section 5.5.2.

6.1.3 Public key delivery to certificate issuer

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

1. Requesting secondary certificates (HCC Person)
2. Requesting HCC Function by means of a PKCS#10-request

When issuing secondary certificates, a CA is obligated to verify that public key is associated with a private key that is held by the subject by invoking a cryptographic challenge to the subjects private key. When issuing HCC Function by means of PKCS#10 requests the subject will prove its possession of the private key when associating the PKCS#10 response with the locally generated key.

6.1.4 CA public key delivery to relying parties

Relying parties are responsible for collecting correct CA keys in current versions. CA certificates can be collected from http://www.inera.se/siths/dokument/certifikat. Issuing CA certificates are also published as part of issued certificates within SITHS.

6.1.5 Key sizes

Key pairs shall be of sufficient length to prevent others from determining the key pair's private key using cryptanalysis during the period of expected utilization of such key pairs. The SITHS standard for minimum key sizes is the use of key pairs equivalent in strength to 4096 bit RSA for CAs.

SITHS issues a minimum key size equivalent in strength to 2048 bit RSA for RAs and end entity certificates key pairs.

The SITHS standard for digital signature hash algorithm is the use of either SHA-1 or SHA-512, depending on the certificate profile specified in the request.

6.1.6 Public key parameters generation and quality checking

All keys are given public exponents that prevent known attacks. 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.

6.1.6.1 Generation of keys in hardware/software

All keys within SITHS are generated in software or hardware modules.

For HCC Person, keys are generated either:

1. In an off board secure processor when cards are personalized
2. In the smart card processor when cards are personalized

For HCC Function that are requested as a PKCS#12-object, the keys are generated by the involved RA by means of software security modules. HCC Function that are requested by means of PKCS#10-requests that can support keys generated in software and hardware security modules.

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

X.509 Version 3 Certificates are generally populated in accordance with RFC 5280: Internet X.509 Public Key Infrastructure Certificate and CRL Profile. The criticality field of the KeyUsage extension is set to TRUE for end entity subscriber certificates and CA certificates within SITHS.
All issued certificates contain information that defines the key usage purposes associated with the certificates keys. Certificates issued in accordance with this CP can have the following key usage purposes:

1. Digital signature
2. Key encryption
3. Non-repudiation

The key usage purposes 1 and 2 can be represented by a single certificate. The non-repudiation key usage must however always be represented in a separate certificate that do not have any of the other key usage purposes. If the non-repudiation key usage is set in a certificate this imposes that the certificate and its keys shall only be used for non-repudiation services.

CA private keys must only be used to sign the following data:

- Issued certificates
- Issued revocation lists
- Internal logs that is relevant in operating a CA
- Other information that is considered as associated with the operation of a CA, e.g. timestamps. Only the SITHS Policy Authority can approve CA signatures of this type.

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.

It is the responsibility of RAs that sufficient security controls are implemented in the local environments where subscriber certificates are used. However it is the responsibility of individual subscribers that certificates are used in accordance with the SITHS subscriber agreement.

Subscribers are obligated to only use private keys in situations, applications and devices where it cannot be suspected that private keys can be misused or abused.

6.2.1 Cryptographic module standards and controls

Private keys within SITHS shall be protected using a trustworthy system and private key holders shall take necessary precautions to prevent the loss, disclosure, modification, or unauthorized use of such private keys in accordance with this CP and contractual obligations.

- **CA certificates**
  Processing centers shall perform all CA cryptographic operations on cryptographic modules rated at a minimum of FIPS 140-2 level 3.
- **SITHS Type 1 CA v1**
  RA cryptographic operations for certificates issued by this CA shall be performed on cryptographic modules rated at a minimum FIPS 140-2 level 2 or Common Criteria EAL4. The private keys are generated and stored on the cryptographic modules.
  All smart card profiles used by smart cards within SITHS shall be approved by the SITHS Policy Authority.
- **SITHS Type 2 CA v1**
  Issues and signs software protected keys that are either:
  - Generated by the end entity subscriber and signed by the issuing CA. The private keys should be generated and stored on a secure and strongly protected server.
  - Generated by the issuing CA and then delivered to an authorized representative in accordance with 6.1.2 in this CP. The private keys shall be generated on a secure and strongly protected server and stored in a suitable format, then erased from the server's primary memory upon retrieval.

  The end entity subscriber is committed to comply with SITHS policy documents and thereby bound to protect the private keys in accordance with section 9.6.3 in this CP.
- **SITHS Type 3 CA v1**
  Generates software protected keys that are generated by the end entity subscriber and signed by the issuing CA. The private keys should be generated and stored on a secure and strongly protected server.

  The end entity subscriber is committed to comply with SITHS policy documents and thereby bound to protect the private keys in accordance with section 9.6.3 in this CP

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

Multi-person control is enforced to protect the activation data needed to activate CA private keys held by processing centers. Processing centers use "secret sharing" to split the private key or activation data needed to operate the private key into separate parts called "secret shares" held by individuals called "shareholders." Some threshold number of secret shares (m) out of the total number of secret shares (n) shall be required to operate the private key.

Processing centers utilize secret sharing to protect the activation data needed to activate their CA private keys. Processing centers also use secret sharing to protect the activation data needed to activate private keys located at their respective disaster recovery sites.

The threshold number of shares needed to sign a CA certificate is 3. It should be noted that the number of shares distributed for disaster recovery tokens may be less than the number distributed for operational tokens, while the threshold number of required shares remains the same.

6.2.3 Private key escrow

CA private keys are not escrowed. Escrow of private keys for end user subscribers is explained in more detail in Section 4.12.

6.2.4 Private key backup

CAs shall back up their own private keys to be able to recover from disasters and equipment malfunction in accordance with this CP. Private keys that are backed up are to be protected from unauthorized modification or disclosure through physical or cryptographic means. Backups are protected with a level of physical and cryptographic protection equal to or exceeding that for cryptographic modules within the CA site, such as at a disaster recovery site or at another secure off-site facility, such as a bank safe.

CA keys must not be archived for any other purpose than disaster recovery. Archiving of private CA keys involving third parties that are not contracted by the SITHS Policy Authority is not allowed.

6.2.5 Private key archival

No centrally generated keys for subscribers or RAs are allowed to be archived by CAs. CA's private keys must not be archived for other purposes than backup/restore in accordance with this CP.

6.2.6 Private key transfer into or from a cryptographic module

Entry of a private key into a cryptographic module shall use mechanisms to prevent loss, theft, modification, unauthorized disclosure, or unauthorized use of such private key.

Processing centers generating CA or RA private keys on one hardware cryptographic module and transferring them into another shall securely transfer such private keys into the second cryptographic module to the extent necessary to prevent loss, theft, modification, unauthorized disclosure, or unauthorized use of such private keys. Private keys shall be encrypted during such transfer.

SITHS participants pre-generating private keys and transferring them into a hardware token, for example transferring generated subscriber private keys into a smart card, shall securely transfer such private keys into the token to the extent necessary to prevent loss, theft, modification, unauthorized disclosure, or unauthorized use of such private keys.

6.2.7 Private key storage on cryptographic module

CA or RA private keys held on hardware cryptographic modules are stored in encrypted form.

6.2.8 Method of activating private key

All SITHS participants shall protect the activation data for their private keys against loss, theft, modification, unauthorized disclosure, or unauthorized use.

6.2.9 Method of deactivating private key

SITHS end entity subscribers have an obligation to protect their private keys. Such obligations extend to protection of the private key after a private key operation has taken place. 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.
When an online CA is taken offline by a processing center, the processing center personnel shall remove the token containing such CA's private key from the reader in order to deactivate it. With respect to the private keys of offline CA, after the completion of a key generation ceremony, in which such private keys are used for private key operations, the processing center personnel shall remove the token containing such CA's private keys from the reader in order to deactivate them.

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. Processing center personnel decommission the CA's private key by deleting it using functionality of the token containing such CA's private keys so as to prevent its recovery following deletion, while not adversely affecting the private keys of other CAs contained on the token. Also key backups and its associated storage media is destroyed when CA keys are destroyed.

6.2.11 Cryptographic module rating

See Section 6.2.1

6.3 Other aspects of key pair management

No private keys or other confidential information for a CA or RA shall leave its designated protected environment. In maintenance or equal scenarios when designated protective measures cannot be fulfilled, all keys, confidential information and its associated storage media is destroyed according to chapter 6 in this CP.

6.3.1 Public key archival

CAs shall archive their own public keys in accordance with section 5.5.

6.3.2 Certificate operational periods and key pair usage periods

The operational period for certificates shall be set according to the time limits set forth in the table below. The usage period for end entity subscriber key pairs is the same as the operational period for their certificates, except that private keys may continue to be used after the operational period for decryption and signature verification. The operational period of a certificate ends upon its expiration or revocation. A CA shall not issue certificates if their operational periods would extend beyond the usage period of the key pair of the CA. Therefore, the CA key pair usage period is necessarily shorter than the operational period of the CA Certificate. Specifically, the usage period is the operational period of the CA Certificate minus the operational period of the certificates that the CA issues. 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, except to the extent a CA needs to sign revocation information until the end of the operational period of the last certificate it has issued.

Certificate profile	Operational period
HCC Person	Maximum 1827 days
HCC Function SHA1	Maximum 730 days
HCC Function SHA512	Maximum 730 days
CA operator certificate	Maximum 1096 days

6.4 Activation data

6.4.1 Activation data generation and installation

SITHS participants generating and installing activation data for their private keys shall use methods that protect the activation data to the extent necessary to prevent the loss, theft, modification, unauthorized disclosure, or unauthorized use of such private keys.

To the extent passwords are used as activation data, subscribers shall generate passwords that cannot easily be guessed or cracked by dictionary attacks. All subscribers may not need to generate activation data, for example if they use biometric access devices.

Processing centers generate activation data for their own CA's private keys in accordance with the secret sharing requirements of this CP.

6.4.2 Activation data protection

SITHS participants shall protect the activation data for their private keys using methods that protect against the loss, theft, modification, unauthorized disclosure, or unauthorized use of such private keys. End entity subscribers shall protect the activation data for their private keys, if any, to the extent necessary to prevent the loss, theft, modification, unauthorized disclosure, or unauthorized use of such private keys
Processing centers utilize secret sharing in accordance with this CP. Processing centers provide the procedures and means to enable shareholders to take the precautions necessary to prevent the loss, theft, modification, unauthorized disclosure, or unauthorized use of the secret shares that they possess. Shareholders shall not:

- Copy, disclose, or make the secret share available to a third party, or make any unauthorized use of it whatsoever; or
- Disclose his, her, or any other persons status as a shareholder to any third party.

The secret shares and any information disclosed to the shareholder in connection with his or her duties as a shareholder constitute confidential/private information.

Processing centers include in their disaster recovery plans provisions for shareholders making their secret shares available at a disaster recovery site after a disaster. Each processing center maintains an audit trail of secret shares, and shareholders shall participate in the maintenance of an audit trail.

6.4.3 Other aspects of activation data

6.4.3.1 Activation data transmission

To the extent activation data for their private keys are transmitted, SITHS participants shall protect the transmission using methods that protect against the loss, theft, modification, unauthorized disclosure, or unauthorized use of such private keys.

6.4.3.2 Activation data destruction

Activation data for CA private keys shall be decommissioned using methods that protect against the loss, theft, modification, unauthorized disclosure, or unauthorized use of the private keys protected by such activation data. After the record retention periods in Section 5.5.2 lapses, processing centers shall decommission activation data by overwriting and/or physical destruction.

6.5 Computer security controls

6.5.1 Specific computer security technical requirements

CA and RA functions take place on trustworthy systems in accordance with the standards documented in the contractual agreements with processing centers. Processing centers shall ensure that the systems maintaining CA software and data files are secure from unauthorized access, which can be demonstrated by compliance with this CP. In addition, processing centers limit access to production servers to those individuals with a valid business reason for access. General users shall not have accounts on the production servers.

Processing centers shall have production networks logically separated from other components. This separation prevents network access except through defined application processes. 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. Processing centers shall require the use of passwords with 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.

RAs shall ensure that the systems maintaining RA software and data files are trustworthy systems secure from unauthorized access, which can be demonstrated by compliance with this CP.

RAs shall logically separate access to these systems and this information from other components. This separation prevents access except through defined processes. RAs shall use firewalls to protect the network from internal and external intrusion and limit the nature and source of activities that may access such systems and information. RAs shall require the use of SITHS certificates for all operations. Direct access to RAs database maintaining subscriber information shall be limited to trusted persons in the RA operations group having a valid business reason for such access. 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.

CA and RA functions are performed using networks secured in accordance with the standards documented in the contractual agreements with processing centers to prevent unauthorized access, tampering, and denial-of-service attacks. Communications of sensitive information shall be protected using point-to-point encryption for confidentiality and digital signatures for non-repudiation and authentication. Only communication that is required for appropriate CA and RA operation shall be allowed, other communication is to be blocked at the network layer.

All CA systems shall be built in a manner that allows for separation of duties according to this CP. All access controls shall be constructed in a manner that allows every individual opeartor to be uniquely identified and authorized.

Software and hardware features that are not used by CAs or RAs shall be deactivated.

6.5.2 Computer security rating

No stipulations.

6.6 Life cycle security controls

6.6.1 System development controls

CA and RA software shall be developed and maintained by developers and vendors that use a controlled and well documented quality management system.

Operational manuals and documentation that in detail specifies how roles and permissions are implemented shall be maintained by processing centers and may be audited by the SITHS Policy Authority.

6.6.2 Security management controls

Software for CA and RA functions designed to manage SITHS certificates shall be subject to checks to verify its integrity. Processing centers shall 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.

6.6.3 Life cycle security controls

No stipulations.

6.7 Network security controls

CA and RA functions are performed using networks secured in order to prevent unauthorized access, tampering, and denial-of-service attacks. Communications of sensitive information shall be protected using point-to-point encryption for confidentiality and digital signatures for non-repudiation and authentication.

6.8 Time-stamping

Certificates, CRLs, and other revocation database entries shall contain time and date information. Such time information does not need to be cryptographic-based.

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 (HCC). These certificate profiles are maintained by the SITHS Policy Authority. The HCC certificate profiles are available at http://www.inera.se/siths/dokument/certifikat.

7.2 CRL Profile

CRLs conform to RFC 5280 and contain the basic fields and contents specified in the table below:

Field	Value or Value constraint
Version	X509v2
Signature Algorithm	Algorithm used to sign the CRL in accordance with RFC 3279. SITHS use sha-1WithRSAEncryption [4] or sha-512WithRSAEncryption [5]
Issuer	Entity that has signed and issued the CRL.
Effective Date	Issue date of the CRL. CRLs are effective upon issuance.
Next Update	Date by which the next CRL will be issued.
Revoked Certificates	Listing of revoked certificates, including the serial number of the revoked certificate and the revocation date.

7.2.1 Version number(s)

SITHS supports X.509 version 2 CRLs.

7.2.2 CRL and CRL entry extensions

No stipulations.

7.3 OCSP Profile

OCSP (Online Certificate Status Protocol) is a way to obtain timely information about the revocation status of a particular certificate.

7.3.1 Version number(s)

Version 1 of the OCSP specification as defined by RFC2560 and Version 1 of the OCSP specification as defined by RFC 5019 are supported.

7.3.2 OCSP extensions

SITHS OCSP services use secure timestamp and validity period to establish the current freshness of each OCSP response. SITHS does use a nonce to establish the current freshness of each OCSP

[4] *Used by SITHS Root CA v1, SITHS Type 1 CA v1 and SITHS Type 2 CA v1*

[5] *Used by SITHS Type 3 CA v1*

response when this is requested by relying parties. If not using nonce, clients shall use the local clock to check for response freshness.

8 Compliance audit and other assessments

The SITHS Policy Authority must continuous conduct audits to ensure CPS, RA Policy and RAPS compliance with this CP.

In an audit, especially the following must be examined:

- CPS, RA and RAPS consistency with this CP
- Comparisons between CA/RA routines and operational guidelines and this CP
- Signed agreements and other information that applies to CA relations with RAs

When the SITHS Policy Authority identifies flaws of needs of changes CAs/RAs must act in accordance with the SITHS Policy Authority guidelines to update its routines.

If the SITHS Policy Authority updates this CP in a way that is considered to alter the general security level of SITHS a new CP with a new identity is to be established.

8.1 Frequency and circumstances of assessment

Compliance audits are conducted at least annually at the sole expense of the audited entity.

8.2 Identity/qualifications of assessor

Compliance audits of SITHS participants are performed by either:

- SITHS Policy Authority (or someone SITHS Policy Authority appoints); and/or
- A third party auditing firm. Reviews and audits performed by a third party audit firm shall be performed by a certified public accounting firm with demonstrated expertise in computer security or by accredited computer security professionals employed by a competent security consultancy. Such firm shall also have demonstrated expertise in the performance of IT security and PKI compliance audits.

8.3 Assessor's relationship to assessed entity

Compliance Audits performed by third-party audit firms shall be conducted by firms independent of the audited entity. Such firms shall not have a conflict of interest that hinders their ability to perform auditing services.

8.4 Topics covered by assessment

CAs and processing centers shall be audited in compliance with WebTrust for Certification Authorities or an equivalent audit standard approved by the SITHS Policy Authority.

8.5 Actions taken as a result of deficiency

After receiving a compliance audit report, the SITHS Policy Authority shall contact the audited party to discuss any exceptions or deficiencies shown by the compliance audit. The audited entity and the SITHS Policy Authority shall, in good faith, use commercially reasonable efforts to agree on a corrective action plan for correcting the problems causing the exceptions or deficiencies and to implement the plan.
In the event of the audited entities failure to develop such a corrective action plan or implement it, or if the report reveals exceptions or deficiencies that the SITHS Policy Authority believe pose an immediate threat to the security or integrity of SITHS, then:

1. The SITHS Policy Authority shall determine whether revocation and compromise reporting are necessary,
2. The SITHS Policy Authority shall be entitled to suspend services to the audited entity, and
3. If necessary, The SITHS Policy Authority may terminate such services subject to this CP and the terms of the audited entities contract.

8.6 Communications of results

Following the third party compliance audit The SITHS Policy Authority shall be provided with the annual report and attestations based on its audit at the next SITHS Policy Authority meeting.

9 Other business and legal matters

9.1 Fees

9.1.1 Certificate issuance or renewal fees

No stipulations.

9.1.2 Certificate access fees

No stipulations.

9.1.3 Revocation or status information access fees

No stipulations.

9.1.4 Fees for other services

The SITHS Policy Authority must not apply fees that are above the actual cost for reproducing and distributing copies of this CP, an RA Policy or a CPS that refer to this CP.

9.1.5 Refund policy

No stipulations.

9.2 Financial responsibility

9.2.1 Insurance coverage

Inera AB, processing centers, CAs and RAs (when required) 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, CAs and RAs (when required) 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

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

9.3.3 Responsibility to protect confidential information

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

9.4 Privacy of personal information

9.4.1 Privacy plan

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, subject to Section 9.3.2 and to the right of a terminating CA to transfer such information to a successor CA under Section 5.8.

9.4.2 Information treated as private

Any information about subscribers that is not publicly available through the content of the issued certificate, certificate directory and online CRLs is treated as private.

9.4.3 Information not deemed private

Subject to local laws, all information made public in a certificate is deemed not private.

9.4.4 Responsibility to protect private information

SITHS participants receiving private information shall secure it from compromise and disclosure to third parties and shall comply with all local privacy laws in their jurisdiction.

9.4.5 Notice and consent to use private information

Unless where otherwise stated in this CP private information will not be used without the consent of the party to whom that information applies. This section is subject to applicable privacy laws.

9.4.6 Disclosure pursuant to judicial or administrative process

SITHS participants acknowledge that the SITHS Policy Authority, CAs and processing centers shall be entitled to disclose confidential/private information if they, in good faith, believes that:

- Disclosure is necessary in response to subpoenas and search warrants.

- Disclosure is necessary in response to judicial, administrative, or other legal process during the discovery process in a civil or administrative action, such as subpoenas, interrogatories, requests for admission, and requests for production of documents.

This section is subject to applicable privacy laws.

9.4.7 Other information disclosure circumstances

No stipulations.

9.5 Intellectual property rights

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

9.6 Representations and warranties

9.6.1 CA representations and warranties

SITHS CAs warrant that:

- There are no material misrepresentations of fact in the certificate known to or originating from the entities approving the certificate application or issuing the certificate,
- There are no errors in the information in the certificate that were introduced by the entities approving the certificate application or issuing the certificate as a result of a failure to exercise reasonable care in managing the certificate application or creating the certificate,
- Their certificates meet all material requirements of this CP and the applicable CPS, and
- Revocation services and use of a repository conform to all material requirements of this CP and the applicable CPS in all material aspects.

Subscriber agreements may include additional representations and warranties.

9.6.2 RA representations and warranties

SITHS RAs warrant that:

- There are no material misrepresentations of fact in the certificate known to or originating from the entities approving the Certificate Application or issuing the Certificate,
- There are no errors in the information in the Certificate that were introduced by the entities approving the certificate application as a result of a failure to exercise reasonable care in managing the certificate application,
- Their certificates meet all material requirements of this CP and the applicable CPS, and
- Revocation services (when applicable) and use of a repository conform to all material requirements of this CP and the applicable CPS in all material aspects.

Subscriber Agreements may include additional representations and warranties.

9.6.3 Subscriber representations and warranties

Subscribers warrant that:

- Each digital signature created using the private key corresponding to the public key listed in the certificate is the digital signature of the subscriber and the certificate has been accepted and is operational (not expired or revoked) at the time the digital signature is created,

- Their private key is protected and that no unauthorized person has ever had access to the subscriber's private key,
- All representations made by the subscriber in the certificate application the subscriber submitted are true,
- All information supplied by the subscriber and contained in the certificate is true,
- The certificate is being used exclusively for authorized and legal purposes, consistent with all material requirements of this CP and the applicable CPS, and
- The subscriber is an end entity subscriber and not a CA, and is not using the private key corresponding to any public key listed in the certificate for purposes of digitally signing any certificate (or any other format of certified public key) or CRL, as a CA or otherwise.

Subscriber Agreements may include additional representations and warranties.

9.6.4 Relying party representations and warranties

Relying party agreements require relying parties to acknowledge that they have sufficient information to make an informed decision as to the extent to which they choose to rely on the information in a certificate, that they are solely responsible for deciding whether or not to rely on such information, and that they shall bear the legal consequences of their failure to perform the relying party obligations in terms of this CP.

Relying party agreements may include additional representations and warranties.

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

The CP becomes effective upon publication in the SITHS repositories specified in section 2.1. Amendments to this CP become effective upon publication in the SITHS repositories specified in section 2.1.

9.10.2 Termination

This CP as amended from time to time shall remain in force until it is replaced by a new version.

9.10.3 Effect of termination and survival

Upon termination of this CP, SITHS participants are nevertheless bound by its terms for all certificates issued for the remainder of the validity periods of such certificates.

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

Amendments to this CP may be made by the SITHS Policy Authority. Amendments shall either be in the form of a document containing an amended form of the CP or an update. Amended versions or updates shall be linked to the SITHS repository located in accordance with section 2.1. Updates supersede any designated or conflicting provisions of the referenced version of the CP. The SITHS Policy Authority shall determine whether changes to the CP require a change in the certificate policy object identifiers of the certificate policy.

9.12.2 Notification mechanism and period

The SITHS Policy Authority reserve the right to amend the CP without notification for amendments that are not material, including without limitation corrections of typographical errors, changes to URLs, and changes to contact information. The SITHS Policy Authority's decision to designate amendments as material or non-material shall be within the SITHS Policy Authority's sole discretion.
The SITHS Policy Authority shall send CAs, RAs and processing centers notice of material amendments to the CP proposed by the SITHS Policy Authority. The notice shall state the text of the proposed amendments and the comment period. Proposed amendments to the CP shall also appear in the SITHS repository, which is located according to section 2.1.

The SITHS Policy Authority solicits proposed amendments to the CP from other SITHS Participants. If the SITHS Policy Authority considers such an amendment desirable and proposes to implement the amendment, the SITHS Policy Authority shall provide notice of such amendment in accordance with this section.

Notwithstanding anything in the CP to the contrary, if the SITHS Policy Authority believes that material amendments to the CP are necessary immediately to stop or prevent a breach of the security of the SITHS or any portion of it, the SITHS Policy Authority shall be entitled to make such amendments by publication in the SITHS repository. Such amendments will be effective immediately upon publication. Within a reasonable time after publication, the SITHS Policy Authority shall provide notice to CAs, RAs and processing centers of such amendments.

9.12.3 Circumstances under which OID must be changed

If the SITHS Policy Authority determines that a change is necessary in the object identifier corresponding to a certificate policy, the amendment shall contain new object identifiers for the certificate policy. Otherwise, amendments shall not require a change in certificate policy object identifier.

9.13 Dispute resolution provisions

Disputes in relation to this CP will ultimately be resolved in Swedish law court.

9.14 Governing law

Subject to any limits appearing in applicable law, the laws of Sweden shall govern the enforceability, construction, interpretation, and validity of this CP. CAs provides information in accordance with Swedish applicable laws. Access to private keys associated with issued certificates cannot be provided since these are not archived by CAs or any subcontractors used by a CA within SITHS.

9.15 Compliance with applicable law

No stipulations.

9.16 Miscellaneous provisions

No stipulations.

9.17 Other provisions

No stipulations.

10 Referenced documents

The following documents are referenced in this CP and the latest version of each document can be found at http://www.inera.se/siths/dokument/styrande.

- SITHS HCC Profile
- HSA Policy
- SITHS RA Policy
- SITHS RAPS template
- SBC 151-U

Appendix A. Table of acronyms and definitions

Acronyms

Acronym	Expansion
CA	Certification Authority
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
FIPS	United State Federal Information Processing Standards
OCSP	Online Certificate Status Protocol
PIN	Personal Identification Number
PKCS	Public-Key Cryptography Standard
PKI	Public Key Infrastructure
PA	Policy Authority
RA	Registration Authority
RFC	Request For Comment
S/MIME	Secure Multipurpose Internet Mail Extensions
SSL/TLS	Secure Sockets Layer/Transport Layer Security

Definitions

Term	Definition
Administrator	A Trusted Person within a Processing Center.
Certificate	In this context *public key certificate*; An electronic document that uses a digital signature to bind a public key with an identity.
Certificate Applicant	An individual or organization that requests the issuance of a certificate by a CA.
Certificate Application	A request from a certificate applicant (or authorized representative) to a CA for the issuance of a certificate.
Certificate Chain	An ordered list of certificates containing an end entity subscriber certificate and CA certificates, which terminates in a root Certificate.
Certificate Policy	This document, which is the principal statement of policy governing SITHS CA.
Certificate Revocation List	A periodically (or exigently) issued list, digitally signed by a CA, of identified certificates that have been revoked prior to their expiration dates. The list generally indicates the CRL issuer name, the date of issue, the date of the next scheduled CRL issue, the revoked certificate serial numbers, and the specific times and reasons for revocation.
Certification Authority	An entity authorized to issue, manage, revoke, and renew certificates.
Certification Practice Statement	A statement of the practices that is employed by a CA under a specific CP.
Compliance Audit	A periodic audit that participants within a CA undergoes to determine its conformance with the regulations that applies to it.
Compromise	A violation (or suspected violation) of a security policy, in which an unauthorized disclosure of, or loss of control over, sensitive information may have occurred. With respect to private keys, a compromise is a loss, theft, disclosure, modification, unauthorized use, or other compromise of the security of such private key.
Confidential/Private Information	Information required to be kept confidential and private pursuant to this CP.
HCC Profile	The certificate profiles used within SITHS are labeled as HCC Profiles.
HSA	The directory service used by SITHS,
Intellectual Property Rights	Rights under one or more of the following: any copyright, patent, trade secret, trademark, and any other intellectual property rights.
Non-repudiation	An attribute of a communication that provides protection against a party to a communication falsely denying its origin, denying that it was submitted, or denying its delivery. Denial of origin includes the denial that a communication originated from the same source as a sequence of one or more prior messages, even if the identity associated with the sender is unknown.
Online CA	A CA that sign end entity subscriber certificates are maintained online so as to provide continuous signing services.
Online Certificate Status Protocol	A protocol for providing relying parties with real-time certificate status information.
Operational Period	The period starting with the date and time a certificate is issued (or on a later date and time certain if stated in the certificate) and ending with the date and time on

	which the certificate expires or is revoked.
PKCS#10	Defines a structure for a certificate signing request. Developed by RSA Security Inc.
PKCS#12	Defines a secure means for the transfer of private keys. Developed by RSA Security Inc.
SITHS Policy Authority	The organization within SITHS responsible for enforcing this policy throughout SITHS.
Processing Center	An organization that creates, among other things, secure facility housing and the cryptographic modules used for the issuance of certificates.
Public Key Infrastructure	The architecture, organization, techniques, practices, and procedures that collectively support the implementation and operation of a certificate-based public key cryptographic system.
Registration Authority	An entity approved by a CA to assist certificate applicants in applying for certificates and to approve or reject certificate applications, revoke certificates or renew certificates.
Relying Party	An individual or organization that acts in reliance on a certificate and/or a digital signature.
Relying Party Agreement	An agreement used by a CA setting forth the terms and conditions under which an individual or organization acts as a relying party.
RSA	A public key cryptographic algorithm invented by Rivest, Shamir, and Adelman.
Subject	The holder of a private key corresponding to a public key. The term subject can, in the case of a HCC Function certificate, refer to the equipment or device that holds a private key. A subject is assigned an unambiguous name, which is bound to the public key contained in the subject certificate.
Subscriber	In the case of an individual certificate, a person who is the subject of, and has been issued, a certificate. In the case of an organizational certificate, an organization that owns the equipment or device that is the subject of, and that has been issued, a certificate. A subscriber is capable of using, and is authorized to use, the private key that corresponds to the public key listed in the certificate.
Subscriber Agreement	An agreement used by a CA or RA setting forth the terms and conditions under which an individual or organization acts as a subscriber.
Trusted Person	An employee, contractor, or consultant of an entity within SITHS responsible for managing infrastructural trustworthiness of the entity, its products, its services, its facilities, and/or its practices.
Trustworthy System	Computer hardware, software, and procedures that are reasonably secure from intrusion and misuse; provide a reasonable level of availability, reliability, and correct operation; are reasonably suited to performing their intended functions; and enforce the applicable security policy.
xRA	A trusted operator holding a role within an RA-organization.