Försäkringskassan

Swedish Social Insurance Agency Hardware X.509 Certification Practices Statement

Key Information:

Formal title:	Swedish Social Insurance Agency Hardware X.509 Certification Practice Statement
OID:	1.2.752.146.2.4 [.0.0.1] { iso (1) member (2) sweden (752) swedish social insurance agency (146) ssia HWCA (2.4) [cpvn-top (0) cpvn-2nd (0) cp (1)] }
Responsible authority:	Försäkringskassan Infrastruktur Management Authority
Version:	*4.1.0*
Effective date:	*2016-03-15*
Classification / Distribution	Un-classified / Unlimited distribution
Published at:	http://www.myndighetsca.se/cps/
Author:	Richard G. Wilsher, Zygma LLC
PMA Point-of-Contact:	Försäkringskassan Infrastruktur Management Försäkringskassan, SE-851 93 Sundsvall, Sweden Email: MCA@forsakringskassan.se Tel: +46 70 208 44 63

Prepared by: 3xA Security AB

Zygma LLC

APPROVALS

Each formal release of this Certificate Policy (CP) requires approval by the board of Policy Management Authority for the Swedish Social Insurance Agency, whose signature shall be applied to an electronic PDF version of it.

Approval control:

Version identification has three levels requiring the approval authority identified below according to level. Version identification is a simple integer sequencing at each level.

Top-level:	A formal release of the applicable CP following a **significant policy change** requiring a change of the policy's OID which requires alignment of its accompanying CPS;
Second-level:	A formal release of this CPS which continues to describe practices relating to the CP described by the top-level version;
Third-level:	A draft of this CPS intended for review and/or recommendation as the next formal release.

When the identification at a given level is incremented all subordinate levels revert to zero. Only the first two levels need be shown in formal releases (level three is by default zero in any formal release). During the drafting of revisions this record shall record all draft versions and their approvals until such time as a formal release is approved. Records of ALL past drafting releases shall be preserved within the Försäkringskassan Infrastruktur Management Authority (SSIA PMA) for archival purposes.

On its effective date a formal version of this CPS shall become the applicable version of the policy for all operational purposes and shall supersede all previous versions which shall thereby become redundant. The SSIA PMA shall preserve records of all past versions.

Approval authorities:

Top-level:	Försäkringskassan Infrastruktur Manager & IT Production Manager for SSIA;
Second level:	As top-level;
Third level:	Author / Editor – for informal PMA member and development / editorial team review.

Approval record:

Version	Approval date	Approved (rôle)	Approved (name)	Reason / notes
4.1.0	2016-03-15	SSIA PMA	SSIA PMA Board	Approved
4.0.3	2016-02-29	SSIA PMA		Clarifications
4.0.2	2016-02-25	SSIA PMA		Clarifications
4.0.1	2016-02-23	SSIA PMA		Changed to version 4 of HW CA
3.0.1	2015-11-05	SSIA PMA		
3.0.0	2015-09-10	SSIA PMA		
2.0.0	2015-05-04	SSIA PMA	SSIA PMA Board	First version

CONTENTS

1. INTRODUCTION

1.1. Overview

This Certification Practice Statement (CPS) describes the Certification Practices employed in the provisioning of Extended Validation (EV) certificates to Swedish government agencies by Försäkringskassan (SSIA), the Swedish government's Social Insurance Agency (hereafter SSIA) to Swedish government agencies, in accordance with the Certificate Policy (CP) known as the Swedish Social Insurance Agency Hardware X.509 Certificate Policy v4.0.1. References in this document to 'CP' or 'applicable CP' refer to this explicit version of this CP.
This CPS conforms to the Internet Engineering Task Force's (IETF) RFC 3647, "*Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practice Statement Framework*" of 2003-11 [RFC3647] and in particular observes the structure of §6 of [RFC3647], "*Outline of a Set of Provisions"*.

This CPS also conforms to current version of the CA/Browser Forum's "*Baseline Requirements for the Issuance and Management of*
Publicly-Trusted Certificate" [CABF] (published at http://www.CABForum.org). This CPS describes practices employed in the issuance of the following three types of Certificate:

a) Agency Client HW Certificates (having the purposes described in [CABF] §6.1.1 (1));
b) Agency Server HW Certificates (having the purposes described in [CABF] §6.1.1 (1));
c) Agency Encryption Certificates (having the purposes described in [CABF] §6.1.1 (2)).

In the event of any inconsistency between this CPS and the CP or those Guidelines, the latter shall take precedence. All special terms and definitions addressed in the CP apply from hereon.

This CPS is published under the authority of the Försäkringskassan Infrastruktur Operational Authority (SSIA OA).

For public-facing references, the English-language title of Försäkringskassan (Swedish government's Social Insurance Agency - SSIA) shall be used.

1.2. Document Identification

The OID for the Swedish Social Insurance Agency's HW CA v4 (ssia-HWCA) is defined in the applicable CP as {1.2.752.146.2.4}.

Certificates issued according to practices described in this CPS assert at least one of the following OIDs:

ssia-HWclient	::= { ssia- HWCA 100 } 1.2.752.146.2.4.100
ssia-HWserver	::= { ssia- HWCA 200 } 1.2.752.146.2.4.200
ssia-HWencrypt	::= { ssia- HWCA 300 } 1.2.752.146.2.4.300
ssia-HW-EFS	::= { ssia- HWCA 400 } 1.2.752.146.2.4.400

In order to provide a discrete OID for this document and the corresponding CPS the following schema has been devised to identify the current formal release of these documents, as follows:

Current Formal Release: Version x . y (.0)

ssia-HW CP	{ssia-HW cpvn-top cpvn-2nd } 1.2.752.146.2.4.x.y
ssia-HW CPS	{ssia-HW } 1.2.752.146.2.4.x.y.1

1.3. PKI Participants

This CPS observes the same definitions of and roles and responsibilities for PKI Participants as described in the CP.

1.4. Certificate Usage

1.4.1. Appropriate Certificate Uses

See CP § 1.4.1.

Refer to the applicable CP.

CP	SSIA_HWCA_v4_CP_Ver410

1.4.2. Prohibited Certificate Uses

See CP § 1.4.2.

1.5. Practices Statement Administration

1.5.1. Organization Administering the Document

The 'Responsible authority' cited on the cover page shall be responsible for the administration of this CPS.

1.5.2. Contact Person

The 'PMA Point-of-contact' cited on the cover page, shall be the initial point of contact for all matters.

1.5.3. Person determining CPS suitability for the policy

The Chairman of the 'Responsible authority' cited on the cover page of the SSIA HWCA CP shall determine the suitability of this CPS (see CP §1.3.1.2).

1.5.4. CPS Approval Procedures

The PMA board [see MCA PMA Charter] approves the CPS and any amendments. Amendments are made by either updating the entire CPS or by publishing an addendum. The PMA board determines whether an amendment to this CPS requires notice or an OID change. See also Section 9.10 and Section 9.12 below.

1.6. Definitions and Acronyms

Definitions, meanings and interpretations used within the CP are used in this CPS with the same meaning. **Inter-Agency Agreements** [IAA]: An agreement between participating Agencies within the Swedish government.

A register of **Inter-Agency Agreements** is held at Försäkringskassan and is called [IAARegister].

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1. Repositories

SSIA publishes revocation information (CRL) on issued digital certificates, root certificate, intermediate certificates, CP and this CPS in the official SSIA repository, available at http://www.myndighetsca.se.

2.2. Publication of Certification Information

Published information includes all revoked certificates in a certificate revocation list (CRL), the CP and this CPS. The CRL lists can be found at:

http://pki.myndighetsca.se/crl/

http://pki.forsakringskassan.se/crl/

2.3. Information Availability

The SSIA repository is open to public access and has a stable redundant infrastructure which ensures 99% availability on a 24 / 7 basis. The architecture which ensures this is described in internal SSIA documents. Information is made available with the frequencies and response times cited elsewhere in this CPS. The SSIA have a non-public repository with only government agency access where roadmaps and other relevant documents are published.

2.4. Repository Access Controls

Published information is generated from a secure data centre in Sweden hosted by SSIA (Försäkringskassan) in Sundsvall with multiple layers of both logical and physical controls to prevent unauthorized access. The published information is digitally-signed to provide for its integrity and published in the SSIA repository with only read-only access permitted.

3. IDENTIFICATION AND AUTHENTICATION

3.1. Naming

3.1.1. Names Types

Certificates are issued with a non-null subject Distinguished Name (DN) complying with ITU X.500 standards. DNs reflect the Agency naming and numbering conventions adopted from [StatsRegister] (see 3.1.5 below).

3.1.2. Need for Names to be meaningful

SSIA ensures that the Organization (O) and Organizational Unit (OU) attributes in the Subject field are derived from information in [StatsRegister], thereby ensuring that the name accurately identifies the legal entity that is the subject of the certificate (see appendix 1 for details).

3.1.3. Anonymity or Pseudonymity of Subscribers

SSIA does not issue anonymous or pseudonymous certificates.

3.1.4. Name Forming Rules

DNs are formed, and should be interpreted, based on X.500 standards and ASN.1 syntax.

3.1.5. Name Uniqueness

Individual Agencies are responsible for assigning names to Agency Entities. In the event of any potential name clashes at the Agency Entity level, RAs are responsible for resolving these and submitting a unique DN within Certificate Requests. Name uniqueness is ensured through the use of the Common Name (CN), Organization (O) and Organizational Unit (OU) attributes in the Subject field using the form:

C = SE
O = Agency name from [StatsRegister]
OU = Agency number from [StatsRegister]
CN = Agency Entity name

3.1.6. Recognition, Authentication, and Rôle of Trademarks

The SSIA OA does not specifically make any checks to avoid IPR infringements. Individual Agencies are responsible for ensuring that they do not use names in their Certificate Applications that infringe upon the Intellectual Property Rights (IPR) of any other Agencies, or other bodies. In the event that a third party makes a substantiated claim of infringement of its IPR, the OA will revoke all credentials so infringing that IPR.

3.2. Initial Identity Validation

On an initial application the Agency identity is only recognized according to [StatsRegister].

3.2.1. Method to Prove Possession of Private Key

The applicant Subscriber 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 requires PKCS #10 or another cryptographically-equivalent demonstration. This requirement does not apply where a key pair is generated by a CA on behalf of a Subscriber.

3.2.2. Authentication of Organization Identity

Only Agencies defined in [StatsRegister] are eligible as applicant Subscribers.

On initial application the OA verifies, by reference to [StatsRegister], that the Agency exists, that the application is being submitted in the correct name of the Agency and that the application is authorized by a designated recognized representative of the Agency. The OA also ensures that the Agency representative has signed and submitted a copy of [IAA], thereby accepting its terms on behalf of their agency. This process describes, through [IAA] who may request that a certificate be issued on behalf of the Agency in question (the signatory serves as the [CABF] Authorized Representative; the agreement fulfilling [CABF]'s requirements for Terms of Use).

The authority of a person to request a certificate on behalf of an Agency is verified in accordance with Section 3.2.5.

These checks fulfil the requirements of [CABF] §4.2.1.

3.2.3. Authentication of Individual Identity

Any application for a certificate must be supported by the host Agency's RA or appointed Agency Server Administrator signing the request with their valid certificate from "Swedish Government User CA". The OA will authenticate the authorizing signature on the request. The authentication process must map to the Agency name and Agency number from [StatsRegister] before processing the application.

3.2.4. Non-verified Subscriber information

No non-verified Subscriber information is placed into Certificates issued by the OA.

3.2.5. Validation of Authority

In the [IAA] the agency states one or more representatives who are entitled to request server certificates and answer questions related to certificate requests. These persons shall be the only ones in their agency to request certificates according to the provisions outlined in 3.2.3. The signatures of these individuals with the private key associated with the certified public key are sufficient for information exchanges with that agency. When the agency rescinds the individual's authorization it has to inform the SSIA in the same way as it has made the authorization known.

The entity's identity is verified thru role based Authentication and a certificate request can only be made for a Subject in the same Agency's domain as the requesting RA.

Before proceeding with the creation of a new certificate the request is verified as having come from an authorised source as stated above.

3.2.6. Criteria for inter-operation

No provision for inter-operation with other CAs is provided.

3.3. Identification and Authentication for Re-Key Requests

There is no provision for re-keying.

3.4. Identification and Authentication for Revocation Request

Prior to the revocation of a Certificate, either the OA or the Agency's Administrator verifies that the revocation has been legitimately requested if the requester has been logged in to the Portal and asked for revocation. The revocation is then effected and published automatically.

4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1. Certificate Application

In keeping with [CABF], this CPS uses the term 'Certificate Application' rather than 'Certificate Request' per [RFC3647].

4.1.1. Who Can Submit a Certificate Request

In the [IAA] shall it be specified which user have the role "Server Administrator". They should be specified by name and Swedish personal number. Agencies are responsible to keep correct user in this role. Any change of users in the role Server Administrator, must be communicated to SSIA and be specified in the [IAA].

Every RA or appointed Agency Server Administrator must have a valid certificate from "Swedish Government User CA" or "Swedish Government Auth CA" to be able to make a certificate request. See also 3.2.2 and 3.2.5.

The SSIA HWCA only accept Certificate Requests from a designated RA, who shall only be permitted to request certificates for their own Agency's Subjects in accordance with [CABF] §4.2.1(2). SSIA PortAdmin can request certificates for other Agency's Subjects.

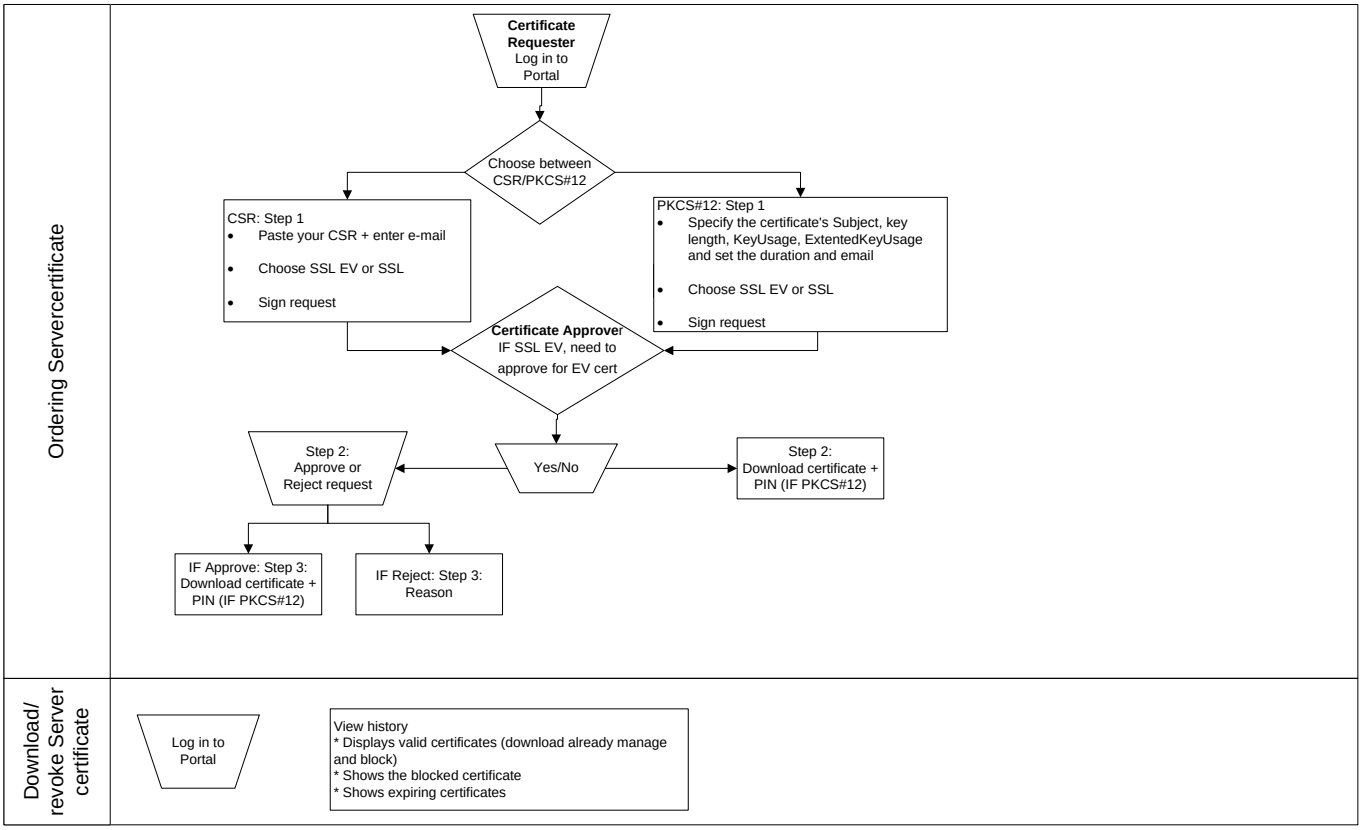
4.1.2. Enrolment Process and Responsibilities

In the [IAA] shall all addresses that the Agency want to use for Common Name (CN), be specified. All addresses are checked against https://www.iis.se/ to see if the Agency has the owner right to that address. These addresses are then added to the Portal. When enrolling for a server certificate a check is made to validate the address. If other addresses (non-registered in the [IAA]) are stated in the request, it will be rejected. Any change of addresses, must be communicated to SSIA and be specified in the [IAA].

The following Applicant roles are required for the issuance of a certificate:

☐ Certificate Requester – The certificate Request Form MUST be submitted by an authorized Certificate Requester which is stated in the [IAA].

☐ Certificate Approver – The certificate Request Form MUST be approved by an authorized Certificate Approver.



Requesters must complete the online forms at SSIA website, otherwise SSIA can´t approve the certificate request. The process of requesting a certificate is illustrated above. The Agency Registration Agent requester needs to be in the role “Server Administrator” and have a valid certificate from “Swedish Government User CA” or “Swedish Government Auth CA” to be able to make a certificate request.

The user can choose to paste a CSR (preferred) or specify information in the request and then sign the request with the user’s valid certificate from “Swedish Government User CA”. A certificate approver reads the certificate and validates the request. The requester gets the certificate and a generate key to the certificate directly at the website.

From this portal the user (with the role “Server Administrator”) have the possibility to see all requests and have the possibility to revoke a certificate if the private key is lost or compromise or if there is other valid reasons, see §4.9.1.

The user needs to handle the key to the certificate in a secure way which is stated in the [IAA].
During the certificate approval process SSIA PortAdmin employ controls to validate the identity of the Subscriber and other information featured in the certificate application. SSIA PortAdmin reviews the application information provided by the Applicant to ensure compliance with the Guidelines.

SSIA PortAdmin has the ability to request a certificate, without using the online website. They can create a certificate using the command “certreq” at SSIA HWCA, if the CSR or online form don´t support the wanted design of the certificate. SSIA PortAdmin must then manually see that the certificate have the correct attribute and the process must be documented in detailed and saved for external auditors.

4.2. Certificate Application Processing

4.2.1. Performing Identification and Authentication Functions

SSIA HWCA maintains systems and processes that sufficiently authenticate the applicants identity in line with the applicable statements made in this CPS. Initial identity vetting may be performed by SSIA PortAdmin in line with

§3.2 or by Registration Authorities under contract and stipulated in each individual [IAA] Applications for certificates are authenticated using multi factor authentication.

4.2.2. Approval or Rejection of Certificate Application

Before issuing a certificate, SSIA HWCA ensures that all subject organisation information in the certificate conforms to the requirements of, and has been verified in accordance with, the Guidelines and matches the information confirmed and documented by the CA pursuant to its verification processes.

Certificate Requests that cannot be verified shall be rejected. The SSIA HWCA may also reject a Certificate Request on any reasonable basis. Unless there is cause for criminal investigation, procedural discipline or disclosure presents a security risk to the CA or other participants within the SSIA PKI, rejection shall be supported by a reason.

4.2.3. Time to Process Certificate Application

There is dedicated personal for this purpose to ensure that the Certificate Requests are processed in a timely manner. The time to process a certificate request is equal to 24 hours business time provided that the SSIA HWCA was able to proceed to all required verifications and validations.

4.3. Certificate Issuance

4.3.1. CA Actions during Certificate Issuance

During the certificate issuance process, the SSIA HWCA shall verify that the identified and authenticated Applicant is the source of the certificate request and that the Subject individual or entity exists within the indicated Agency. The contents of the certificate requests verifies for compliance with the technical specification as outlined in chapter 7.1.2. Databases used to confirm Subscriber identity information shall be protected from unauthorized modification or use. CA actions during the certificate issuance process shall be performed in a secure manner.

4.3.2. Notification to Subject by the CA of Issuance of Certificate

Notification is embedded in the automated process to deliver requested certificates within two business days. The Subject is notified to a predefined e-mail address which is stated in the [IAA].

4.4. Certificate Acceptance

4.4.1. Conduct Constituting Certificate Acceptance

A period of five business days after the retrieval of the certificate by the Subject, or use of the certificate by the Subject, constitutes the Subject's acceptance of the certificate.

4.4.2. Publication of the Certificate by the CA

SSIA publishes the certificate by delivering it to the Subscriber. No other publication or notification to others occurs.

4.4.3. Notification of Certificate Issuance by the CA to Other Entities

No stipulation.

4.5. Key Pair and Certificate Usage

4.5.1. Subscriber Private Key and Certificate Usage

All Subjects shall protect their Private Keys from unauthorized use or disclosure by third parties and shall use their Private Keys only as specified in the key usage extension of the corresponding Certificate. Subscribers must protect their Private Key taking care to avoid disclosure to third parties. Private Keys must only be used as specified in the appropriate key usage and extended key usage fields as indicated in the corresponding digital certificate. Where it is possible to make a backup of a private key, Subscribers must use the same level of care and protection attributed to the live private key. At the end of the useful life of a Key, Subscribers must securely delete the key and any fragments that it has been split into for the purposes of backup. See also §9.6.3.

4.5.2. Relying Party Public Key and Certificate Usage

Within this CPS SSIA HWCA provides the conditions under which digital certificates may be relied upon by relying parties including the appropriate certificate services available to verify certificate validity such as CRL. SSIA HWCA also provides an [IAA] to Subscribers of which the content should be presented to the relying party prior to reliance upon a digital certificate from the SSIA HWCA.

Relying parties should use the information to make a risk assessment and as such are solely responsible for performing the risk assessment prior to relying on the certificate or any assurances made. Software used by relying parties should be fully compliant with X.509 applicable IETF PKIX standards.

4.6. Certificate Renewal

4.6.1. Circumstance for Certificate Renewal

Certificate renewal shall not be supported.

4.6.2. Who May Request Renewal

No stipulation.

4.6.3. Processing Certificate Renewal Requests

No stipulation.

4.6.4. Notification of New Certificate Issuance to Subscriber

No stipulation.

4.6.5. Conduct Constituting Acceptance of a Renewal Certificate

No stipulation.

4.6.6. Publication of the Renewal Certificate by the CA

No stipulation.

4.6.7. Notification of Certificate Issuance by the CA to Other Entities

No stipulation.

4.7. Certificate Re-Key

Certificate re-keying shall not be supported.

4.7.1. Circumstance for Certificate Re-key

No stipulation

4.7.2. Who May Request Certificate Re-key

No stipulation.

4.7.3. Processing Certificate Re-key Requests

No stipulation.

4.7.4. Notification of Certificate Re-key to Subject

No stipulation.

4.7.5. Conduct Constituting Acceptance of a Re-keyed Certificate

No stipulation.

4.7.6. Publication of the Issued Certificate by the CA

No stipulation.

4.7.7. Notification of Certificate Issuance by the CA to Other Entities

No stipulation.

4.8. Certificate Modification

4.8.1. Circumstance for Certificate Modification

Certificate modification is considered and handled the same as an application for a new certificate. Certificate modification may never take place after the certificate has been revoked because of key compromise or a significant risk of key compromise.

After modifying a certificate, the SSIA HWCA may revoke the old certificate but may not further re-key, renew, or modify the old certificate.

4.8.2. Who May Request Certificate Modification

The SSIA HWCA may modify certificates at the request of roles stated in §4.1.1 or at its own discretion. Identity validation may be in accordance with this CPS.

4.8.3. Processing Certificate Modification Requests

After receiving a request for modification, the SSIA HWCA verifies any information that will change in the modified certificate. The SSIA HWCA shall issue the modified certificate only after completing the verification process on all modified information. The validity period of a modified certificate shall not extend beyond the applicable time limits found in §6.3.2.

4.8.4. Notification of Certificate Modification to Subscriber

See §4.3.2, in the context of a certificate modification.

4.8.5. Conduct Constituting Acceptance of a Modified Certificate

See §4.4.1, in the context of a certificate modification.

4.8.6. Publication of the Modified Certificate by the CA

See §4.4.2.

4.8.7. Notification of Certificate Modification by the CA to Other Entities

No stipulation.

4.9. Certificate Revocation and Suspension

4.9.1. Circumstances for Revocation

Prior to revoking a certificate, the SSIA HWCA shall verify that the revocation request was made by either the Subject or the applicable RA that made the Certificate Request, or by an entity with the legal jurisdiction and authority to request revocation. The SSIA HWCA shall revoke any certification the occurrence of any of the following circumstances:

a) the Subscriber requests revocation of its Certificate;

b) the Subscriber indicates that the original Certificate Request was not authorized and does not retroactively grant authorization;

c) the SSIA HWCA obtains reasonable evidence that the Subject's Private Key (corresponding to the Public Key in the Certificate) has been compromised or is suspected of compromise, or that the Certificate has otherwise been misused;

d) the SSIA HWCA receives notice or otherwise becomes aware that a Subscriber has violated one or more of its material obligations under [IAA];

e) the SSIA HWCA receives notice or otherwise becomes aware that a court or arbitrator has revoked a Subscriber's right to use the Domain Name listed in the Certificate, or that the Subscriber has failed to renew its rights to the Domain Name;

f) the SSIA HWCA receives notice or otherwise becomes aware of a material change in the information contained in the Certificate or that such information is no longer accurate or representative of the facts

(which would include the situation where the role of the Subject changes within the Agency such that they no longer qualify for or need the use of the certificate);

g) a determination, in the SSIA HWCA's sole discretion, that the Certificate was not issued in accordance with the terms and conditions of these Guidelines or the SSIA HWCA's Policies;

h) the SSIA HWCA ceases operations for any reason and has not arranged for another CA to provide revocation support for the Certificate;

i) the SSIA HWCA's right to issue Certificates under these Guidelines expires or is revoked or terminated, unless the SSIA HWCA makes arrangements to continue maintaining the CRL Repository;

j) the Private Key of the SSIA HWCA's Root Certificate used for issuing that Certificate is suspected to have been compromised;

k) the SSIA HWCA receives notice or otherwise becomes aware that a Subject has been added as a denied party or prohibited person to a blacklist, or is operating from a prohibited destination under the laws of the SSIA HWCA's jurisdiction of operation;

l) the subject fails to retrieve the certificate within sixty (60) days of notification of its availability; or

m) such additional events as the SSIA HWCA determines, at its sole discretion, warrant revocation.

The SSIA HWCA shall always revoke a certificate if the binding between the Subject and the Subject's public key in the certificate is no longer valid or if any associated Private Key is compromised.

If an Agency terminates its relationship with the SSIA HWCA, the SSIA HWCA shall revoke all certificates issued in the name of that Agency.

4.9.2. Who Can Request Revocation

The SSIA HWCA or RA shall accept revocation requests from authenticated and authorized parties, such as the certificate Subscriber (see [IAA]) and the Affiliated Organization named in a certificate. The SSIA HWCA or RA may establish procedures that allow other entities to request certificate revocation (see §4.1.2) for fraud or misuse. The SSIA HWCA shall revoke a certificate if it receives sufficient evidence of compromise of loss of the Private Key. The SSIA HWCA may unilaterally revoke a certificate if it finds justifiable cause.

4.9.3. Procedure for Revocation Request

Entities submitting certificate revocation requests shall provide their own identity (from the end user certificate) as well as (if not the Subject) that of the Subject and the identification of the certificate, with their reason for requesting revocation. The SSIA HWCA automatically authenticates and logs each revocation request.

The SSIA HWCA shall revoke a certificate without challenge if the request is authenticated as originating from either the Subscriber or the Subject. If revocation originates from another source then the SSIA HWCA or RA shall investigate the reason for the revocation request and act according to their findings.

The SSIA HWCA shall provide a 24/7 response (see [IAA] for details) to any high-priority certificate problem reports. When required by law or other explicit policy or directive, the SSIA HWCA or the RA may notify law enforcement. Revocation leads to updates in the database, a next update of CRL. A revoked certificate shall continue to be in CRL until the certificate expires HWCA.

4.9.4. Revocation Request Grace Period

The revocation request grace period is the time available to the subscriber within which the subscriber must make a revocation request after reasons for revocation have been identified.

RAs are required to report the suspected compromise of their private keys and request revocation to both the SSIA-IAM and the SSIA HWCA within one hour of discovery. The SSIA HWCA shall report its decision to revoke private keys to the SSIA-IAM within one hour of discovery. All other Subscribers are required to report suspected key compromise and request revocation promptly, but in no case later than 24 hours, after discovery.

4.9.5. Time within which CA Must Process the Revocation Request

This is determined by the CP. Revocation management services are available 24 hours per day, 7 days per week. Upon system failure, service failure or other factors that are not under the control of the SSIA HWCA, SSIA shall make best endeavors to ensure that this service is not unavailable for an unreasonable long period of time.

4.9.6. Revocation Checking Requirement 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. CAs shall provide Relying Parties with information on how to find the appropriate CRL to check for revocation status. This is stated in [IAA].

4.9.7. CRL Issuance Frequency

The CRL issuance frequency is determined by the CP. SSIA HWCA issues a new CRL even if there is no change in the status of end user certificates notice of a key compromise.

4.9.8. Maximum Latency for CRLs

CRLs are posted to the repository within within four hours of generation (and no later than 18 hours after notification of compromise) after generation. This is generally done automatically within minutes of generation.

4.9.9. On-line Revocation/Status Checking Availability

The SSIA HWCA doesn't supports the OCSP protocol for on line revocation checking. Certificate status information are available via a web-based repository.

4.9.10. On-line Revocation Checking Requirements

A relying party must, when working with certificates issued by SSIA HWCA, at all times verify the certificates issued by this CA. The validity of a certificate must be confirmed via CRL in accordance with §4.9.6. The relevant standards are given in section 7.2 and section 7.3 of this CPS.

4.9.11. Other Forms of Revocation Advertisements Available

None shall be permitted

4.9.12. Special Requirements Related to Key Compromise

The SSIA HWCA or any of its RA shall use commercially reasonable methods to notify potential Relying Parties that their private key may have been compromised. This includes cases where new vulnerabilities have been discovered or where SSIA HWCA at its own discretion decides that evidence suggests a possible key compromise has taken place. Where key compromise is not disputed, SSIA HWCA shall revoke Issuing CA Certificates or Subscriber End Entity certificates and shall issue a CRL within 18 hours.

4.9.13. Circumstances for Suspension

Not applicable.

4.9.14. Who Can Request Suspension

Not applicable.

4.9.15. Procedure for Suspension Request

Not applicable.

4.9.16. Limits on Suspension Period

Not applicable.

4.10. Certificate Status Services

4.10.1. Operational Characteristics

SSIA HWCA provides a certificate status service available in the form of a CRL distribution point. These services are presented to relying parties within each certificate.

4.10.2. Service Availability

SSIA HWCA shall provide availability of the certificate status services and online certificate revocation services on a 24/7 basis. Service interruptions for maintenance will be announced thru channels stated in [IAA]. Upon system failure or other factors that are not under the control of the HWCA, SSIA shall make best endeavour's to ensure that this information services are not unavailable for an unreasonable long period of time.

4.10.3. Optional Features

Revocation notices shall not be removed before the certificate's original expiration date.

4.11. End of Subscription

Subscribers or Subjects may end their subscription to certificate services either by requesting that their certificate(s) be revoked or by allowing the certificate(s) or [IAA] to expire without renewal.

4.12. Key Escrow and Recovery

SSIA HWCA Private Keys shall never be escrowed. No other key escrow services shall be offered.

4.12.1. Key Escrow and Recovery Policy Practices

No stipulation.

4.12.2. Session Key Encapsulation and Recovery Policy and Practices

No stipulation.

5. MANAGEMENT, OPERATIONAL AND PHYSCAL CONTROLS

5.1. Physical Controls

5.1.1. Site Location and Construction

The SSIA´s CA equipment are housed in secure facilities that are protected by multiple tiers of physical security, electronic control access systems, alarmed doors and is monitored via a 24/7 security camera and motion detector system.

5.1.2. Physical Access

SSIAHWCA protect its system components (computers, rooms, services, documentation, records, etc.) from unauthorized access and have physical controls to reduce the risk of equipment being tampered with. SSIAHWCA store all removable media and paper containing sensitive plain-text information related to CA or RA operations, in secure containers. The security mechanisms are in commensurate with the level of threat to the equipment and data.

SSIA HWCA electronically monitor its systems for unauthorized access at all times, maintain an access log that is inspected periodically, and require two-person physical access to the CA hardware and systems. SSIAHWCA shall deactivate, remove, and securely store its CA equipment when not in use. Activation data must either be memorized or recorded and stored in a manner commensurate with the security afforded the cryptographic module and must not be stored with the cryptographic module or removable hardware associated with remote workstations used to administer the CA equipment or private keys.

If the facility housing the SSIA HWCA equipment is ever left unattended, the SSIA OA shall verify that:

a. the CA is left in a mode of operation appropriate to its unattended state;

b. all security containers are properly secured;

c. physical security systems (e.g., door locks, vent covers) are functioning properly and are activated; and

d. the area is secured against unauthorized access.

The SSIA HWCA shall assign to a person or group of persons explicitly responsibility for making security checks. If a group of persons is responsible, the SSIA HWCA shall maintain a log that identifies who performed the security check. Whenever the facility is left un- attended, the last person to depart shall initial a sign-out sheet that indicates the date and time and asserts that all necessary physical protection mechanisms are in place and activated.

During regular business hours, entry to the building where the CA is housed is accessed through a reception area with a security guard on duty at the facility 24 hours a day, 7 days a week, and 365 days a year. After hours, an access card is required to enter the building. Access to all areas beyond the reception area requires the use of an "access" or "pass" card. All access card use is logged. The building is equipped with motion detecting sensors, and the exterior and internal passageways of the building are also under constant video surveillance.

The key to the room where the CA is housed in is held in a safe where only specified person (on a list) could have access to. The guards specify witch user who have borrow that key and when. There needed to be at least 2 people accessing this room.

5.1.3. Power and Air Conditioning

There are primary and secondary power supplies that ensure continuous, uninterrupted access to electric power. Redundant backup power is provided by battery uninterrupted power supplies (UPS) and diesel generators.

The facility is equipped with heating, ventilation, and air conditioning appropriate for a commercial data processing facility.

5.1.4. Water Exposure

SSIA has taken reasonable precautions to minimize the impact of water exposure to the CA system. No liquid, gas, exhaust, etc. pipes traverse the controlled space other than those directly required for the area's HVAC system and for the pre-action fire suppression system.

5.1.5. Fire Prevention and Protection

The secure facility is equipped with fire suppression.

5.1.6. Media Storage

All media containing production software and data, audit, archive, or backup Information is stored within SSIA facilities and in a secure off-site storage facility with appropriate physical and logical access controls.

5.1.7. Waste Disposal

Printed sensitive information is shredded on-site before disposal. All electronic media are zeroized using programs meeting proper standards. Cryptographic devices are physically destroyed or zeroized in accordance the manufacturers' guidance prior to disposal. Other waste is disposed in accordance with SSIA's normal waste disposal requirements.

5.1.8. Off-site Back-up

SSIA performs routine backups of critical system data, audit log data, and other sensitive information. Offsite backup media are stored in a physically secure manner. Access to the site is limited to authorized personnel listed on an access list, which is subject to audit.

There is a separate document that specifies this in detail. Since this document classification is un-classified this information could not be detailed here.

5.1.9. CMS and External RA Systems

All physical control requirements under this Section 5.1 apply equally to any CMS or external RA system.

5.2. Procedural Controls

5.2.1. Trusted Rôles

SSIA HWCA personnel acting in Trusted Rôles 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, renewal requests, or enrollment information;
- the issuance, or revocation of Certificates, including personnel having access to restricted portions of its repository;
- the handling of Subscriber information or requests.

HWCA Trusted Rôles include, but are not limited to:

- SSIA PKI Administrator
- System Administrator/ System Engineer (Operator)
- Agency Registration Agent/ Server Administrator
- Internal Auditor Rôle
- External Auditor Rôle

Persons seeking to acting in Trusted Rôles must successfully complete the screening requirements set out in this CPS (§5.3). All personnel in Trusted Rôles must be free from conflicts of interest that might prejudice the impartiality of CA and RA operations. Senior management of the SSIA HWCA or the Subscribing Agency shall be responsible for appointing individuals to Trusted Rôles (See §1.3). Those in such roles shall be identified through the [IAA].

There is a separate document that specifies Trusted Rôles in detail. Since this documents classification is un-classified this information could not be detailed here.

5.2.1.1. SSIA PKI Administrator

The SSIA PKI Administrator is responsible for the installation and configuration of the SSIA HWCA software, including key generation, User and CA accounts, audit parameters, key back-up, and key management. The SSIA PKI Administrator is responsible for performing and securely storing regular system back-ups of the SSIA HWCA system.

The SSIA PKI Administrator is also responsible for managing the certificate request queue and for issuing credentials to Agency Registration Agents.

5.2.1.2. System Administrator/ System Engineer (Operator)

The System Administrator, System Engineer or CA Operator is responsible for installing and configuring CA system hardware, including servers, routers, firewalls, and network configurations. The System Administrator / Engineer is also responsible for keeping systems updated with software patches and other maintenance needed to ensure system stability and recoverability.

5.2.1.3. Agency Registration Agent/ Server Administrator

The Agency Registration Agent (Server Administrator) rôle is responsible for requesting the issuance and revocation of certificates for Subjects within its Agency, including enrolment, identity verification, and compliance with required issuance and revocation steps such as managing the certificate request queue and completing certificate approval checklists as identity vetting tasks are successfully completed.

Agency Registration Agents shall not have the means to issue certificates to Subscribers, and this is accomplished through security within the portal.

5.2.1.4. Internal Auditor Rôle

The Internal Auditor Rôle is responsible for reviewing, maintaining, and archiving audit logs and performing or overseeing internal compliance audits to determine whether the SSIA HWCA or RAs are operating in accordance with this CPS.

5.2.1.5. External Auditor Rôle

An additional role external to SSIA HWCA is the External Auditor rôle, performed by an external auditor in accordance with Section 8 below.

5.2.2. Number of Persons Required per Task

The number of persons to provide the SSIA HWCA services is at least 2 people per task to perform sensitive tasks. The goal is to guarantee the trust for all services of SSIA HWCA (key generation, certificate generation, revocation) so that any malicious activity would require collusion. Where multiparty control is required, at least one of the participants shall be an Administrator. All participants shall serve in a trusted role as defined in section 5.2.1 above.

5.2.3. Identification and Authentication for each Rôle

SSIA HWCA employees in trusted roles must first authenticate themselves to the certificate management system before they are allowed access to the components of the system necessary to perform their trusted roles. For normal operations systems, access is controlled by user account and password, IP address subnet, and SSL. These mechanisms restrict access to those who are authorized and make actions directly attributable to the individual taking such action while fulfilling the trusted role.

5.2.4. Rôles Requiring Separation of Duties

While the certification process is operated, the entirety of sequential operations made on the same certificate shall be performed by different persons at different process points. Duties have been distributed to separate roles and thereby a single person is prevented from performing the entirety or a large part of the work in the process. Each operation is logged so as to include detailed place and time data based on roles. Specifically, a user that is authorized to assume a Security Officer or Registration and Customer Services Officer role is not authorized to assume a System Auditor role. A user that is authorized to assume a System Administrator role is not authorized to assume a Security Officer or a System Auditor role.

Individual personnel shall be specifically designated to the four rôles defined in Section 5.2.1 above. Individuals may only assume one of the Officer, Administrator, and Auditor rôles, but any individual may assume the Operator rôle.

Separation of duties may be enforced either by the CA equipment, or procedurally, or by both means. The CA and RA software and hardware shall identify and authenticate its users and shall ensure that no user identity can assume both an Administrator and an Officer rôle, assume both the Administrator and Auditor rôles, or assume both the Auditor and Officer rôles. No individual shall have more than one identity.

There shall be the means to audit adherence to these rules.

5.3. Personnel Controls

Persons seeking to acting in Trusted Rôles must present proof of the requisite background, qualifications, and experience needed to perform their prospective job responsibilities competently and satisfactorily, as well as proof of any government clearances, if any, necessary to perform certification services under government contracts. Background checks are repeated at least every 8 years for personnel holding Trusted Rôles.

5.3.1. Qualifications, Experience, and Clearance Requirements

Before starting employment at SSIA, all new employees must sign confidentiality (non-disclosure) agreements. SSIA follows personnel and management practices that provide reasonable assurance of the trustworthiness and competence of their employees and of the satisfactory performance of their duties. The trusted roles and responsibilities, as specified in § 5.2.1, are only assigned to selected and reliable personnel who have proven their suitability for such a position. They must possess the expert knowledge, experience and qualifications necessary for

the trusted roles. SSIA HWCA personnel in trusted roles fulfill the requirement of expert knowledge, experience and qualifications through formal training, credentials or actual experience or a combination of them.

5.3.2. Background Check Procedures

Each person fulfilling a Trusted Rôle must undergo checks and identification prior to acting in the rôle, including verification of the individual's identity, employment history, education, character references, social security number, previous residences, driving records and criminal background. This procedure is made by the recruiting chief and the human resources department. The background (SUA check) investigations are performed by SÄPO (Swedish Secret Police) which is a competent independent authority that has the authority to perform background investigations. The SSIA HWCA shall require each individual to appear in-person before a Trusted Agent whose responsibility it is to verify identity. The Trusted Agent must verify the identity of the individual using at least one form of government-issued photo identification. All checks are for the prior five years.

These checks need not be repeated if the person concerned is already employed by the Swedish government and has been previously been subjected to these checks, but in the case that they have not been subjected to these checks they shall be performed within a period of three (3) months of the publication of this CPS and thereafter prior to appointment for new personnel.

5.3.3. Training Requirements

SSIA provides all personnel with training skills that covers basic Public Key Infrastructure (PKI) knowledge, authentication and verification policies and procedures, common threats to the validation process, including phishing and other social engineering tactics, and the Guidelines. Training of personnel is undertaken via a mentoring process involving senior members of the team to which they are attached. All new personnel must undergo this training process for at least two months. SSIA maintain records of such training and ensures that personnel entrusted with Trusted Rôles meet a minimum skills requirement that enable them to perform such duties satisfactorily. SSIA ensures that its personnel qualify for each skill level required by the corresponding task before granting privilege to perform said task. There is a separate document that specifies the training in detail. Since this document classification is un-classified this information could not be detailed here.

5.3.4. Retraining Frequency and Requirements

Personnel must maintain skill levels that are consistent with industry-relevant training and performance programs in order to continue acting in Trusted Rôles. SSIAHWCA make individuals acting in Trusted Rôles aware of any changes to the SSIA HWCA's and RAs' operations. If such operations change, the SSIAHWCA shall provide documented training, in accordance with an executed training plan, to all Trusted Rôles. SSIA provides 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 stipulation.

5.3.6. Sanctions for Unauthorized Actions

Failure of any SSIA employee (with trusted role) to comply with the provisions of this CPS, whether through negligence or malicious intent, will subject such individual to appropriate administrative and disciplinary actions by HR department. They will be removed from the trusted role pending management review.

5.3.7. Independent Contractor Requirements

In limited circumstances, independent contractors or consultants may be used to fill trusted positions. They are held to the same functional and security criteria that apply to a SSIA employee in a comparable position.

5.3.8. Documentation Supplied to Personnel

Personnel in trusted roles are provided with the documentation necessary to perform the role to which they are assigned, including a copy of this CPS, SSIA's security policy and all technical and operational documentation needed to maintain the integrity of SSIA's HWCA operations.

5.4. Audit Logging Procedures

5.4.1. Types of Events Recorded

Audit log files are generated for all events relating to the security and services of the SSIA CA components. Where possible, the security audit logs shall be automatically collected. Where this is not possible, a logbook, paper form, or other physical mechanism shall be used. All security audit logs, both electronic and nonelectronic, shall be retained and made available during compliance audits. SSIA CA ensures all events relating to the life cycle of certificates are logged in a manner to ensure the imputability to a person in a trusted role of an action required for SSIA CA services.

SSIA manually or automatically logs the following significant events:

- CA key life cycle management events, including:
  - Key generation, backup, storage, recovery, archival, and destruction
  - Cryptographic device life cycle management events.
- CA and Subscriber certificate life cycle management events, including:
  - Certificate Applications, renewal, rekey, and revocation
  - Successful or unsuccessful processing of requests
  - Generation and issuance of Certificates and CRLs.
- Security-related events including:
  - Successful and unsuccessful PKI system access attempts
  - PKI and security system actions performed by SSIA personnel
  - Security sensitive files or records read, written or deleted
  - Security profile changes
  - System crashes, hardware failures and other anomalies
  - Firewall and router activity
  - CA facility visitor entry/exit.

Log entries include the following elements:

- Date and time of the entry
- Serial or sequence number of entry
- Identity of the entity making the entry
- Kind of entry.

SSIA log Certificate Application information including:

- Kind of identification document(s) presented by the Certificate Applicant
- Record of unique identification data, numbers, or a combination thereof (e.g., drivers license number or equal) of identification documents, if applicable
- Storage location of copies of applications and identification documents
- Identity of entity accepting the application
- Method used to validate identification documents, if any
- Name of receiving CA or submitting RA, if applicable.

5.4.2. Frequency of Processing Log

SSIA review HWCA at least every two months, review the audit log to trace and investigate events that occurred. The review includes verification of the audit log for alteration; viewing all items in the log and checking for warnings or anomalies; and explanation of the causes of such events and proposition of preventive actions. Actions taken based on log reviews are also documented. Log files and audit trails are archived for inspection by the authorized personnel of SSIA and designated auditors.

5.4.3. Retention Period for Audit Log

Records concerning SSIA CA certificates are held for a period of time (10 years) as appropriate for providing necessary legal evidence in accordance with the applicable legislation.

5.4.4. Protection of Audit Log

Audit logs are protected by physical and electronic security measures, and kept open for access by authorized personnel only. The data integrity of audit logs is ensured by encryption technologies.

5.4.5. Audit Log Back-up Procedures

Audit logs and audit summaries are backed-up in a secure location, under the control of an authorized trusted role, separated from their component source generation. Audit log backup is protected to the same degree as originals.

5.4.6. Audit Collection System (internal vs. external)

Automated audit data is generated and recorded at the application, network and operating system level. Manually generated audit data is recorded by authorized personnel only.

5.4.7. Notification to Event-causing Subject

No stipulation.

5.4.8. Vulnerability Assessments

Except actions taken in §5.4.2, the following vulnerability assessments should be performed once a year:

- OS vulnerability assessments

- Physical facility vulnerability assessments

- Certificate management system vulnerability assessments

- Network vulnerability assessments.

5.5. Records Archival

SSIA HWCA includes sufficient detail in archived records to show that a certificate was issued in accordance with the CPS.

5.5.1. Types of Records Archived

SSIA retains in a trustworthy manner records of SSIA HWCA digital certificates, audit data, certificate application information, log files and documentation supporting certificate applications.

CA and RA archive records shall be detailed enough to establish the validity of a signature and of the proper operation of the PKI. At a minimum, the following data shall be archived:

- All logs in §5.4.1 (CP);
- SSIA HWCA audit documentation;
- SSIA HWCA CP documents (all versions);
- SSIA HWCA CPS documents (all versions);
- [IAA] (all versions);

5.5.2. Retention Period for Archive

SSIA HWCA retain archived data for at least ten (10) years unless a greater retention is required by any other applicable law, standard, policy, etc.

5.5.3. Protection of Archive

Archive records are stored at a secure off-site location and are protected by physical and electronic security measures, and kept open for access by authorized personnel only. Electronic archives are protected against unauthorized viewing, modification or deletion. Archives on paper are retained in special units to which only authorized personnel can access.

5.5.4. Archive Back-up Procedures

According to the SSIA backup and disaster recovery operating procedures, key, certificate and transaction data should be archived and backed up daily, weekly and monthly. Copies of paper-based records shall be maintained in an off-site secure facility.

5.5.5. Requirements for Time-stamping of Records

All records in the database and in log files are time-stamped using the system time of the system where the event is recorded. The system time of all servers is synchronized with the time source of WHAT using the Network Time Protocol (NTP).

5.5.6. Archive Collection System (internal or external)

The SSIA HWCA collects archive information internally. SSIA assists its 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.

5.6. Key Changeover

SSIA HWCA key pairs are retired from service at the end of their respective maximum lifetimes as defined in this CPS. SSIA HWCA certificates may be renewed as long as the cumulative certified lifetime of the CA key pair does not exceed the maximum CA key pair lifetime. New CA key pairs can be generated for example to replace CA key pairs that are being retired, to supplement existing, active key pairs and to support new services.

Key changeover procedures enable the transition from expiring CA certificates to new CA certificates. Towards the end of the CA private key's lifetime, SSIA HWCA ceases using its expiring CA private key to sign certificates no later than 60 days before the point in time where the remaining lifetime of the expiring CA key pair equals the approved certificate validity period for the specific type(s) of certificates issued. The old private key is only used to sign CRLs until the expiration date of the last certificate issued using the original key pair has been reached.

A new CA signing key pair is commissioned and all subsequently issued certificates and CRL's are signed with the new private signing key. Both the old and the new key pairs may be concurrently active. This key changeover process helps minimize any adverse effects from CA certificate expiration. The corresponding new CA public key certificate is provided to subscribers and relying parties through the delivery methods detailed in § 6.1.4.

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, and database records for all Certificates issued. Back-ups of CA private keys shall be generated and maintained in accordance with CP §6.2.3. SSIA maintains backups of the foregoing CA information for their own CAs.

SSIA establishes business continuity procedures that outline the steps to be taken in the event of the corruption or loss of computing resources, software and/or data that could disturb or compromise the SSIA CA services. SSIA CA carries out risk assessments to evaluate business risk and determine the necessary security requirements and operational procedures to be taken as a consequence of its disaster recovery plan. This risk analysis is regularly reviewed and revised if necessary (threat evolution, vulnerability evolution etc). This business continuity is in the scope of the audit process as described in section 8 to validate what are the operations that are first maintained after a disaster and the recovery plan. SSIA personnel that own a trusted role and operational role are specially trained to operate according to procedures defined in the Disaster Recovery plan for the most sensitive activities. If SSIA detects a potential hacking attempt or another form of compromise, it should perform an investigation in order to determine the nature and the degree of damage. Otherwise, the SSIA CA assesses the scope of potential damage in order to determine whether the CA or RA system needs to be rebuilt, whether only some certificates

need to be revoked, and/or whether a CA hierarchy needs to be declared as compromised. The CA disaster recovery plan highlights which services should be maintained (for example revocation and certificate status information).

There is a separate document that specifies this in detailed. Since this document classification is un-classified this information could not be detailed here.

The SSIA HWCA has implemented a data back-up and recovery procedures and have developed a Disaster Recovery (DR) and/or Business Continuity Plan (BCP). The SSIA HWCA's shall have redundant CA systems that are located at a separate, geographically diverse location and that are configured for automatic failover in the event of a disaster (Disaster Recovery/Mirror Site). The SSIA HWCA shall review, test, and update the DR/BCP and supporting procedures annually. If a disaster occurs, the SSIA HWCA shall re-establish operational capabilities as quickly as possible.

5.7.2. Computing Resources, Software, and/or Data Are Corrupted

SSIA HWCA performs system back-ups on a daily basis. Back-up copies are made of SSIA HWCA:s Private Keys and are stored off-site in a secure location. In the event of a disaster whereby the primary and disaster recovery CA operations become inoperative at SSIA primary facility and the Disaster Recovery / Mirror Site, SSIA will re-initiate its operations on replacement hardware (on-site) using backup copies of its software, data and CA private keys at a secured facility.

If it cannot be made fully operational or some of the records cannot be recreated, all subscribers and relying people that may be affected shall be urgently notified. Where necessary, certain certificates shall be revoked and new certificates shall be issued.

5.7.3. Entity Private Key Compromise Procedures

If the SSIA HWCA suspects that a CA Private Key is comprised or lost then the SSIA HWCA shall follow its Incident Response Plan and immediately assess the situation, determine the degree and scope of the incident, and take appropriate action. SSIA HWCA personnel shall report the results of the investigation. The report must detail the cause of the compromise or loss and the measures that should be taken to prevent a re-occurrence.

- Collect all information related to the incident (and if the event is on-going, ensure that all data are being captured and recorded);
- Begin investigating incident and determine degree and scope;
- Incident Response Team determines the course of action or strategy that should be taken, (and in the case of Key Compromise, determining the scope of HWCA certificates that must be revoked);
- Contact government agencies (in the [IAARegister]), law enforcement, and other HWCA interested parties and activate any other appropriate additional security measures;
- Monitor system, continue investigation, ensure that data is still being recorded as evidence, and make a forensic copy of data collected;
- Isolate, contain and stabilize the system, applying any short-term fixes needed to return the system to a normal operating state (contact browser software providers to discuss revocation/damage mitigation mechanisms if trust anchors may be affected);
- Prepare an incident report that analyses the cause of the incident and documents the lessons learned, and circulate the report; and
- Incorporate lessons learned into the implementation of long term solutions and also into the Incident Response Plan for future use HWCA.

Following revocation of the SSIA HWCA's certificate and implementation of the SSIA HWCA's Incident Response Plan, the SSIA HWCA will generate a new CA Key Pair and sign a new CA certificate. The SSIA HWCA shall distribute the new self-signed certificate in accordance with Section 6.1.4. The SSIA HWCA shall cease its CA operations until appropriate steps are taken to recover from the compromise and restore security.

5.7.4. Business Continuity Capabilities after a Disaster

See 5.7.1-5.7.3

5.8. CA or RA Termination

This CPS and any amendments remain in effect until deleted or replaced by a newer version. Prior to termination by deletion SSIA shall publish a notification to this effect to SSIA's online repository no less than one (1) year (365 days) in advance.

In case of termination of CA operations for any reason whatsoever, SSIA will provide timely notice and transfer of responsibilities to succeeding entities, maintenance of records, and remedies. Before terminating its own CA activities, SSIA will where possible take the following steps:

- Provide subscribers of valid certificates with one (1) year (365 days) notice of its intention to cease acting as a CA.

- Revoke all certificates that are still un-revoked or un-expired at the end of one (1) year (365 days) notice period without seeking Subscriber's consent.

- Give timely notice of revocation to each affected Subscriber.

- Make reasonable arrangements to preserve its records according to this CPS.

- Reserve its right to provide succession arrangements for the re-issuance of certificates by a successor CA that has all relevant permissions to do so and complies with all necessary rules, while its operation is at least as secure as SSIA's.

6. TECHNICAL SECURITY CONTROLS

6.1. Key Pair Generation and Installation

6.1.1. Key Pair Generation

SSIA Key Pairs are generated in a HSM device (with FIPS 140-2 level 3). Documentation supporting the integrity of the key generation ceremony and other sensitive key operations is stored in a locked safe in SSIA business offices (and a copy of this is in our backup facility) and is made available to its auditors for review.

This is embedded in the automated process for certificate life cycle management.

6.1.2. Private Key Delivery to Subscriber

When end-user Subscriber key pairs are generated by the end-user Subscriber, private key delivery to a Subscriber is not applicable. Subscribers are solely responsible for the generation of the private keys used in their certificate requests (CSR). If there isn't a CSR the SSIA HWCA creates the certificate from user input and generates a password for that certificate with a random module. That password is not kept in the system after the certificate is generated. The end-user must collect it and store it safely.

6.1.3. Private Key Delivery to Certificate Issuer

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

6.1.4. CA Public Key Delivery to Relying Parties

SSIA Root Public Keys are distributed by Microsoft Root program, downloadable from our website (http://www.myndighetsca.se/) or available by e-mail.

6.1.5. Key Sizes

SSIA SSL Certificate key sizes will be a minimum RSA 2048 bits, with Secure Hash Algorithm version 2 (SHA-256) to sign the certificates.

6.1.6. Public Key Parameters Generation and Quality Checking

No stipulation.

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

SSIA certificates include key usage extension fields to specify the purposes (see appendix 1) for which the CA-Certificate may be used and also to technically limit the functionality of the certificate when used with X.509v3 compliant software. Reliance on key usage extension fields is dependent on correct software implementations of the X.509v3 standard and is outside of the control of SSIA.

6.2. Private Key Protection and Cryptographic Module Engineering Control

6.2.1. Cryptographic Module Standards and Controls

SSIA use HSM, certified to FIPS 140-2 level 3, to protect the Certification Authorities' Private Keys.

6.2.2. Private Key ('n' from 'm') Multi-person Control

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

6.2.3. Private Key Escrow

SSIA ensures that subject private signing keys are not stored on-line anywhere outside the HSM. This means that there is no backup decryption capability whatsoever, and that no entity under any condition can ever decrypt data.

6.2.4. Private Key Back-up

The backup tokens are held in secure facilities (and a copy of this is in our backup facility) under two-person control. Back-up is a part off the standard procedure.

6.2.5. Private Key Archival

SSIA HWCA does not archive Private Keys.

6.2.6. Private Key Transfer into or from a Cryptographic Module

The Private Keys are generated and stored inside the HSM, which has been evaluated to at least FIPS 140-2 level 3 and EAL 4+. Where such keys must be transferred to other media for backup and disaster recovery purposes, they are transferred and stored in an encrypted form protected by the USB authentication tokens (which have been imprinted with secret keys) using the manufacturer's specified PCMCIA token cloning processes. This is the standard procedure how a HSM is used and that we follow.

There is a separate document that specifies this in detailed. Since this document classification is un-classified this information could not be detailed here.

6.2.7. Private Key Storage on Cryptographic Module

SSIA uses HSM with the right FIPS level to meet these criteria. There is a separate document that specifies this in detailed. Since this document classification is un-classified this information could not be detailed here.

6.2.8. Method of Activating Private Key

The CAs private keys are activated by a set of USB authentication tokens. Subscribers are responsible for protecting the Private Key associated with the Public Key in the Subscriber's Certificate. SSIA maintains no involvement in the protection of such keys. SSIA suggests that its subscribers use a strong password or equivalent authentication method to prevent unauthorized access and usage of the subscriber private key.

6.2.9. Method of Deactivating Private Key

The private key stored on the HSM is deactivated via logout procedures when it is not in use. Root private keys are further deactivated by removing them entirely from the storage partition on the HSM device. The device is never left in an unlocked, unattended state or otherwise left active to unauthorized access. When unattended and active, the HSM are kept locked inside steel cabinets in a locked room with multiperson control.

Subscribers should also deactivate their private keys via logout and removal procedures when they are not in use.

6.2.10. Method of Destroying Private Key

The CA private key can be destroyed by deleting it from all known storage partitions. HSM and backup tokens are also zeroized by performing ten (10) consecutive failed login attempts. This reinitializes the device and overwrites all of the data on it with binary zeros. In cases when this zeroization or re-initialization procedure fails, SSIA will incinerate the device in a manner that destroys the ability to extract any private key.

To meet these criteria we use the HSM manufacturer's standard procedures.

6.2.11. Cryptographic Module Rating

See §6.2.1.

6.3. Other Aspects of Key Pair Management

6.3.1. Public Key Archival

SSIA retains copies of all Public Keys for archival and it is embedded in the automated process for certificate life cycle management.

6.3.2. Certificate Operational Validity Periods and Key Pair Usage Validity Periods

The operational period of a certificate ends upon its expiration or revocation. The operational period for key pairs is the same as the operational period for the associated certificates, except that private keys may continue to be used for decryption and public keys may continue to be used for signature verification. The maximum operational periods for SSIA HWCA certificates for certificates issued on or after the effective date of this CPS are set forth in table below.

Type	Private Key Use	Certificate Term
Root CA	20 years	25 years
Sub CA	12 years	15 years
Subscriber	No stipulation	39 months

PKI Participants shall cease all use of their key pairs after their usage periods have expired.

SSIA retires its CA Private Keys from signing subordinate certificates before the listed periods, to accommodate the key changeover process, see § 5.6. The CA Private Key is still used to sign CRLs to provide validation services for certificates issued with that retiring CA Private Key.

6.4. Activation Data

6.4.1. Activation Data Generation and Installation

SSIA uses a set of USB-based two-factor authentication tokens to activate the HSM cryptographic module containing its CA private keys. The HSM is held under two-person control. All SSIA personnel are instructed to use strong passwords and to protect PINs and passwords according to SSIA information security guidelines. There is a separate document that specifies this in detail. Since this document is at SSIA, this information could not be detailed here.

6.4.2. Activation Data Protection

Activation data for HSM are protected by keeping the USB authentication tokens under separate, role-based physical control with backups in separate safe deposit boxes under the same separate, role-based control. Access to additional administrative passwords and keys to access the HSM are similarly protected.

6.4.3. Other Aspects of Activation Data

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 lapse, SSIA shall decommission activation data by overwriting and/or physical destruction.

6.5. Computer Security Controls

6.5.1. Specific Computer Security Technical Requirements

The workstations on which the SSIA Certification Authorities operate are physically secured as described in chapter 5. The operating systems on the workstations enforce identification and authentication of users. All operational personnel that are authorized to have access are required to use hardware tokens in conjunction with a PIN to gain access to the physical room that contains the SSIA Certificate Authority.

SSIA ensures that the systems maintaining CA software and data files are Trustworthy Systems secure from unauthorized access. In addition, SSIA limits access to production servers to those individuals with a valid business reason for such access. General application users do not have accounts on production servers.

6.5.2. Computer Security Rating

No stipulation.

6.6. Life Cycle Technical Controls

6.6.1. System Development Controls

SSIA has mechanisms in place to control and monitor the acquisition and development of its CA systems. Change control processes consist of change control data entries that are processed, logged and tracked for any non-security-related changes to CA systems, equipment and software. Change requests require the approval of at least one Senior Administrator (e.g. the Operations Manager, PKI Administrator or System Administrator/ System Engineer) who may not be the same person who submitted the request. In this manner, SSIA can verify whether a change to the system has been properly evaluated for risk mitigation and authorized by management. Vendors are selected based on their reputation in the market, ability to deliver quality product, and likelihood of remaining viable in the future. Management is involved in the vendor selection and purchase decision process. Non-PKI hardware and software is purchased generically without identifying the purpose for which the component will be used. All hardware and software are shipped under standard conditions with controls in place to ensure delivery of the component directly to a trusted employee who ensures that the equipment is installed without opportunity for tampering. Some of the PKI software components used by SSIA to provide CA services are developed in-house or by consultants using standard software development methodologies, other software is purchased commercial off-the-shelf (COTS). Quality assurance is maintained throughout the process through testing and documentation or by purchasing from trusted vendors, discussed above. Updates of equipment or software are purchased or developed in the same manner as the original equipment or software and are installed and tested by trusted and trained personnel.

6.6.2. Security Management Controls

SSIA has mechanisms in place to control and monitor the security-related configurations of its CA systems. Change control processes consist of change control data entries that are processed, logged and tracked for any security-related changes to CA systems, firewalls, routers, software and other access controls. In this manner, SSIA can verify whether a change to the system has been properly evaluated for risk mitigation and authorized by management.

6.6.3. Life Cycle Security Controls

No stipulation.

6.7. Network Security Controls

SSIA's CA system is connected to one internal network and is protected by firewalls, a Demilitarized Zone (DMZ) and Network Address Translation for all internal IP addresses. SSIA's customer support and vetting workstations are also protected by firewalls and only use internal IP addresses. Root Keys are kept offline and brought online

only when necessary to sign certificate-issuing subordinate CAs or periodic CRLs. Firewalls and boundary control devices are configured to allow access only by the addresses, ports, protocols and commands required for the trustworthy provision of PKI services by such systems. SSIA block all ports and protocols and open only necessary ports to enable CA functions. All CA equipment is configured with a minimum number of services and all unused network ports and services are disabled. All firewall configurations and changes thereto are documented, authorized, tested and implemented in accordance with change management policies and procedures. SSIAs network configuration is available for review on-site by its auditors and consultants under an appropriate non-disclosure agreement

6.8. Time-stamping

System time for SSIA computers is updated from The Swedish national time scale, UTC (by SP Technical Research Institute of Sweden) is a national realisation of the Coordinated Universal Time, using the Network Time Protocol (NTP) to synchronize time.

7. CERTIFICATE AND CRL PROFILES

The profile for the SSIA Certificates and Certificate Revocation List (CRL) issued by SSIA Certification Authority conform to the specifications contained in the Guidelines published by the CA/Browser Forum, which themselves conform to IETF RFC 5280 Internet X.509 PKI Certificate and Certificate Revocation List (CRL) Profile.

7.1. Certificate Profile

7.1.1. Version Number

SSIA Certification Authorities issue certificates in accordance with the X.509 version 3.

7.1.2. Certificate Extensions

Certificate profiles for end entity certificates are described in Appendix 1.

7.1.3. Algorithm Object Identifiers

See Appendix 1

7.1.4. Name Forms

See Appendix 1

7.1.5. Name Constraints

See Appendix 1

7.1.6. Certificate Policy Object Identifier

Object identifier (OID) is a number unique within a specific domain that allows for the unambiguous identification of a policy, including a Certificate Policy and/or Certification Practice Statement, such as this CPS. The CP OIDs that incorporate this CPS into a given certificate by reference (which identify that this CPS applies to a given digital certificate containing the OID) are listed in chapter 1.2.

7.1.7. Usage of Policy Constraints Extension

No stipulation.

7.1.8. Policy Qualifiers Syntax and Semantics

No stipulation.

7.1.9. Processing Semantics for the Critical Certificate Policies Extension

No stipulation.

7.2. CRL Profile

7.2.1. Version number(s)

SSIA issues version two (2) CRLs. CRLs conform to RFC 5280 and contain the basic fields listed below:

- Version
- Issuer Signature Algorithm
- Issuer Distinguished Name
- thisUpdate
- nextUpdate
- Revoked certificates list
    - Serial Number
    - Revocation Date
- Issuer's Signature.

7.2.2. CRL and CRL Entry Extensions

CRL Number (monotonically increasing integer - never repeated). Authority Key Identifier (same as Authority Key Identifier in certificates issued by CA).

CRL Entry Extensions

Invalidity Date (UTC - optional)

Reason Code (optional).

7.3. OCSP PROFILE

The profile for the Online Certificate Status Protocol (OCSP) messages issued by an SSIA conform to the specifications contained in the IETF RFC 2560 Internet X.509 PKI Online Certificate Status Protocol (OCSP) Profile.

7.3.1. Version Number(s)

The SSIA HWCA shall support version 1 OCSP requests and responses.

7.3.2. OCSP Extensions

No stipulation.

8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS

The practices in this CPS are designed to meet or exceed the requirements of generally accepted and developing industry standards, including [CABF] and the AICPA/CICA WebTrust Program for Certification Authorities, ANS X9.79/ISO 21188 PKI Practices and Policy Framework ("CA WebTrust/ISO 21188").

8.1. Frequency or Circumstances of Assessment

An annual audit is performed by an independent external auditor to assess SSIA compliance with WebTrust Program for CAs criteria.

8.2. Identity/Qualifications of Auditors

(a) Qualifications and experience. Auditing must be the individual's or group's primary business function. The individual or at least one member of the audit group must be qualified as a Certified Information Systems Auditor (CISA), an AICPA Certified Information Technology Professional (CPA.CITP), a Certified Internal Auditor (CIA), or have another recognized information security auditing credential.

(b) Expertise: The individual or group must be trained and skilled in the auditing of secure information systems and be familiar with public key infrastructures, certification systems, and the like, as well as Internet security

issues (such as management of a security perimeter), operations of secure data centres, personnel controls, and operational risk management.

(c) Rules and standards: The individual or group must conform to applicable standards, rules, and best practices promulgated by the American Institute of Certified Public Accountants (AICPA), the Canadian Institute of Chartered Accountants (CICA), the Institute of Chartered Accountants of England & Wales (ICAEW), the International Accounting Standards adopted by the European Commission (IAS), Information Systems Audit and Control Association (ISACA), the Institute of Internal Auditors (IIA), or another qualified auditing standards body.

(d) Reputation: The firm must have a reputation for conducting its auditing business competently and correctly.

(e) Insurance: auditors must have Insurance, with policy limits of at least $1 million in coverage

The firm must have no financial interest, business relationship, or course of dealing that could foreseeably create a significant bias for or against SSIA.

8.3. Assessor's Relationship to Assessed Entity

In addition to the foregoing prohibition on conflicts of interest, the assessor shall have a contractual relationship with SSIA for the performance of the audit, but otherwise, shall be independent. The assessor shall maintain a high standard of ethics designed to ensure impartiality and the exercise of independent professional judgment, subject to disciplinary action by its licensing body.

8.4. Topics covered by Assessment

Topics covered by the annual WebTrust Program for CAs audit include but are not limited to SSIA CA business practices disclosure (i.e., this CPS), the service integrity of SSIA CA operations, the environmental controls that SSIA implements to ensure a trustworthy system and SSIA compliance with the Guidelines.

8.5. Actions taken as a result of Deficiency

If an audit reports any material noncompliance with applicable law, this CPS, or any other contractual obligations related to the CA services described herein, SSIA shall develop a plan to cure such noncompliance, subject to the approval of the SSIA Policy Authority and any third party to whom SSIA is legally obligated to satisfy. In the event SSIA fails to take appropriate action in response to the report, then the SSIA Policy Authority may instruct SSIA Operations Manager to revoke the certificates affected by such non-compliance.

8.6. Communication of Results

The results of any inspection or audit are reported to SSIA management, acting as the SSIA Policy Authority, and any appropriate entities, as may be required by law, regulation or agreement. At its option, SSIA will provide interested parties with the letter containing the attestation of management and its auditor’s letter concerning the effectiveness of controls. Otherwise, all audit information will be considered confidential business information in accordance with section 9.3.

8.7. Self-Audits

During the period in which it issues certificates, SSIA will control its service quality by performing on going self-audits against a randomly selected sample of at least three percent (3%) of the certificates it has issued in the period beginning immediately after the last sample was taken.

9. OTHER BUSINESS AND LEGAL MATTERS

9.1. Fees

In the [IAA] should it stipulate the fee for each Agency joining the SSIA and the annual fee for participate in the SSIA.

9.2. Financial Responsibility

9.2.1. Insurance Coverage

The SSIA shall maintain sufficient insurances in respect of its performance under this CPS through Kammarkollegiet.

9.2.2. Other Assets

No stipulation.

9.2.3. Insurance or Warranty Coverage for End-Entities

SSIA do not have insurance or warranty coverage for End-Entities for subscriber or relying parties.

9.3. Confidentiality of Business Information

9.3.1. Scope of Confidential Information

The SSIA keeps the following types of information confidential and maintains reasonable controls to prevent the exposure of such records to non-trusted personnel:

- All private keys
- Any activation data used to access private keys or gain access to the CA system
- Any business continuity, incident response, contingency, and disaster recovery plans
- Any other security practices, measures, mechanisms, plans, or procedures used to protect the confidentiality, integrity or availability of information
- Any transactional, audit log and archive record identified in Section 5.4 or 5.5, including certificate application records and documentation submitted in support of certificate applications whether successful or rejected.

9.3.2. Information Not Within the Scope of Confidential Information

Issuer CAs may treat any information not listed as confidential in the CPS as public information.

Subscriber application data identified herein as being published in a digital certificate is considered public and not within the scope of confidential information. Subscribers acknowledge that revocation data of all certificates issued by the SSIA CA is public information and is periodically published at the SSIA repository.

9.3.3. Responsibility to Protect Confidential Information

The following records of Subscribers shall be kept confidential and private:

- CA application records, whether approved or disapproved,
- Certificate Application records,
- Private keys held by SSIA,
- Transactional records (both full records and the audit trail of transactions),
- Audit trail records created or retained by SSIA or a Customer,
- Audit reports created by SSIA or a Customer (to the extent such reports are maintained), or their respective auditors (whether internal or public),
- Contingency planning and disaster recovery plans, and
- Security measures controlling the operations of SSIA hardware and software and the administration of Certificate services and designated enrollment services.

9.4. Privacy of Personal Information

9.4.1. Privacy Plan

The SSIA shall follow a privacy policy that specifies how personal information handles. Regardless of the source, SSIA protects personal information as confidential information except where the information is embedded in an issued digital certificate. This information is necessary for the digital certificate's operation and is considered public information

9.4.2. Information Treated as Private

The SSIA HWCA treats all personal information about an individual that is not publicly available in the contents of a certificate or CRL as private information. The SSIA HWCA protects private information in its possession using a reasonable degree of care and appropriate safeguards. The SSIA HWCA does not distribute certificates that contain the UUID in the subject alternative name extension via publicly accessible repositories (e.g., LDAP, HTTP).

9.4.3. Information Not Deemed Private

Certificates, CRLs, and the personal or corporate information appearing in them are not considered private information.

9.4.4. Responsibility to Protect Private Information

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

9.4.5. Notice and Consent to Use Private Information

Personal data provided during the application, registration, and identity verification process that is not contained in Certificates is considered private information. SSIA may only use private information with the subject's express written consent or as required by applicable law or regulation.

9.4.6. Disclosure Pursuant to Judicial or Administrative Process

SSIA may disclose private information, without notice, when required to do so by law or regulation.

9.4.7. Other Information Disclosure Circumstances

No stipulation.

9.5. Intellectual Property Rights

The SSIA HWCA shall not knowingly violate the intellectual property rights of any third party. The SSIA HWCA shall retain ownership over certificates but shall grant permission to reproduce and distribute certificates on a non-exclusive, royalty-free basis, provided that they are reproduced and distributed in full. Private Keys and Public Keys are the property of the Subscribers who rightfully issue and hold them.

9.6. Representations and Warranties

9.6.1. CA Representations and Warranties

SSIA warrants 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 CPS, and
- Revocation services and use of a repository conform to the applicable CPS in all material aspects.

9.6.2. RA Representations and Warranties

SSIA 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 CPS, and

- Revocation services (when applicable) and use of a repository conform to the applicable CPS in all material aspects.

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 this CPS, and
- The Subscriber is an end-user 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.

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 CPS.

9.6.5. Representations and Warranties of Other Participants

No stipulation.

9.7. Disclaimers of Warranties

SSIA disclaims all warranties and obligations of any type, including any warranty of fitness for a particular purpose, and any warranty of the accuracy of unverified information provided, save as contained herein and as cannot be excluded at law. In no event and under no circumstances (except for fraud or wilful misconduct) shall SSIA be liable for any or all of the following and the results thereof:

- Any indirect, incidental or consequential damages.
- Any costs, expenses, or loss of profits.
- Any death or personal injury.
- Any loss of data.
- Any other indirect, consequential or punitive damages arising from or in connection with the use, delivery, license, performance or non-performance of certificates or digital signatures.
- Any other transactions or services offered within the framework of this CPS.
- Any other damages except for those due to reliance, on the information featured on a certificate, or on the verified information in a certificate.
- Any liability incurred in this case or any other case if the fault in this verified information is due to fraud or willful misconduct of the applicant.
- Any liability that arises from the usage of a certificate that has not been issued or used in conformance with this CPS.
- Any liability that arises from the usage of a certificate that is not valid.
- Any liability that arises from usage of a certificate that exceeds the limitations in usage and value and transactions stated upon it or in this CPS.
- Any liability that arises from security, usability, integrity of products, including hardware and software a Subscriber uses.
- Any liability that arises from compromise of a Subscriber's private key.

9.8. Limitations of Liability

SSIA exclude all liability for any certificate issued and managed in accordance with this CPS.

9.9. Indemnities

9.9.1. Indemnification by an SSIA HWCA

Any indemnification obligations should stipulate in the [IAA].

9.9.2. Indemnification by Subscribers

Any indemnification requirements should stipulate in the [IAA].

9.9.3. Indemnification by Relying Parties

Any indemnification requirements should stipulate in the [IAA].

9.10. Term and Termination

9.10.1. Term

The CPS becomes effective upon publication in the SSIA repository. Amendments to this CPS become effective upon publication in the SSIA repository.

9.10.2. Termination

This CPS 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 CPS, all participating Agencies 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 in the [IAA] between the parties, 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 CPS may be made by the SSIA PMA. Amendments shall either be in the form of a document containing an amended form of the CPS or an update. Amended versions or updates shall be at Repository located at: https://www.myndighetsca.se.

Updates supersede any designated or conflicting provisions of the referenced version of the CPS.

The SSIA PMA shall determine whether changes to the CPS require a change in the Certificate policy object identifiers of the Certificate policies corresponding to each Class of Certificate

9.12.2. Notification Mechanism and Period

SSIA PMA reserve the right to amend the CPS without notification for amendments that are not material, including without limitation corrections of typographical errors, changes to URLs, and changes to contact information. The IMA´s decision to designate amendments as material or non-material shall be within the IMA's sole discretion. Proposed amendments to the CPS shall appear in the Repository, which is located at: https://www.myndighetsca.se.

If the IMA considers such an amendment desirable and proposes to implement the amendment, the IMA shall provide notice of such amendment in accordance with this section.

Notwithstanding anything in the CPS to the contrary, if the IMA believes that material amendments to the CPS are necessary immediately to stop or prevent a breach of the security or any portion of it, SSIA and the IMA shall be

entitled to make such amendments by publication in the Repository. Such amendments will be effective immediately upon publication. Within a reasonable time after publication, SSIA shall provide notice to Affiliates of such amendments.

9.12.3. Circumstances under which OID Must Be Changed

If the IMA 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 policies corresponding to each Class of Certificate. Otherwise, amendments shall not require a change in Certificate policy object identifier

9.13. Dispute Resolution Provisions

Disputes among SSIA participants shall be resolved pursuant to provisions in the applicable agreements among the parties.

9.14. Governing Law

The laws of Sweden shall govern the interpretation, construction, and enforcement of this CPS and all proceedings related hereunder, including tort claims, without regard to any conflicts of law principles.

9.15. Compliance with Applicable Law

This CPS is subject to all laws and regulations within the jurisdiction within which the SSIA HWCA operates.

9.16. Miscellaneous Provisions

9.16.1. Entire Agreement

The agreement should be specified in the [IAA] between the parties.

9.16.2. Assignment

Entities operating under this CPS may not assign their obligations without the prior written consent of SSIA.

9.16.3. Severability

If any provision of this CPS is held invalid or unenforceable by a competent court or tribunal, the remainder of the CPS will remain valid and enforceable.

9.16.4. Enforcement (attorneys' fees and waiver of rights)

SSIA reserves the right to seek indemnification and attorneys' fees from any party related to that party's conduct.

9.16.5. Force Majeure

To the extent permitted by applicable law, Subscriber Agreements and [IAA] shall include a force majeure clause protecting SSIA.

9.17. Other Provisions

9.17.1. Inter-Agency Agreement

Eligible Agencies wishing to participate in the SSIA PKI shall signify their acceptance of the terms of an [IAA], which shall, as a minimum, meet the requirements of [CABF] §9.3. This agreement shall be signed by each participating Agency's authorized representative, per [StatsRegister]. Once signed, the Agreement shall apply to all Certificate Requests which are submitted by and signed by any Administrator, acting in an RA capacity, representing that Agency (that Agency being effectively the Subscriber).

The scope of [IAA] shall be all topics in this CPS where there is reference to [IAA] as being the applicable agreement on which operations shall be based and any other topics as deemed necessary according to the CPS, of which [IAA] shall be a subordinate document, notwithstanding its status as given by this CPS.

Acknowledgement of [IAA] shall be required by reference from each Certificate Request, thus enforcing both the Administrators (Subscribers) and individual Subjects (Sponsors) to acknowledge the existence of [IAA] and their entitlements and obligations thereunder.

After the initial signing of [IAA] each Agency Administrator shall be required, on the anniversary of that initial signing, to reaffirm their commitment to [IAA] within twenty-eight (28) days.

APPENDIX 1

BASIC CONCEPT OF THE SERVER CERTIFICATE

1. Purpose of Certificates.

Certificates are intended for use in establishing web-based data communication conduits via TLS/SSL protocols.

(a) Primary Purposes

Per the guidelines, the primary purposes of a certificate are to:

- Identify the legal entity that controls a website: Provide a reasonable assurance to the user of an Internet browser that the website the user is accessing is controlled by a specific legal entity identified in the certificate by name, address of Place of Business, Jurisdiction of Incorporation, and Registration Number; and
- Enable/encrypted communications with a website: Facilitate the exchange of encryption keys in order to enable the encrypted communication of information over the Internet between the user of an Internet browser and a website.

(b) Secondary purposes

The secondary purpose of an server certificate are to help establish the legitimacy of a business claiming to operate a website by confirming its legal and physical existence, and to provide a vehicle that can be used to assist in addressing problems related to phishing and other forms of online identity fraud. By providing more reliable third-party verified identity and address information regarding the owner of a website, server certificates may help to:

- Make it more difficult to mount phishing and other online identity fraud attacks using SSL certificates;
- Assist companies that may be the target of phishing attacks or online identity fraud by providing them with a tool to better identify themselves and their legitimate websites to users; and
- Assist law enforcement in investigations of phishing and other online identity fraud, including where appropriate, contacting, investigating, or taking legal action against the Subject.

CERTIFICATE CONTENT AND PROFILE

2. Certificate Content Requirements

SSIA HW End Entity Certificates

Field	Value	Comments
Version	V3 (2)	
Serial Number	Unique number	
Issuer Signature Algorithm	sha256 WithRSAEncryption (1.2.840.113549.1.1.11)	
Issuer Distinguished Name	Unique X.500 CA DN. CN = Swedish Government HW CA v4 O = Swedish Social Insurance Agency C = SE	
Validity Period	Up to 36 months expressed in UTC	

	format	
Subject Distinguished Name		
Common Name	subject:commonName (2.5.4.3) cn = Common name	SubjectAlternativeName:dNSName is found below in this table. This field **MUST** contain one or more host domain name(s) owned or controlled by the Subject and to be associated with Subject's publicly accessible server. Such server may be owned and operated by the Subject or another entity (e.g., a hosting service). Wildcard certificates are not allowed for EV certificates.
OrganizationUnit	subject:orgUnit (2.5.4.11)	This field **MUST** contain the Subject's full legal organization number as listed in the official records of the Government Agency in the following format: XXXXXXXXXX
Organization	subject:organizationName (2.5.4.10)	This field **MUST** contain the Subject's full legal organization name as listed in the official records of the Government Agency
SerialNumber	Subject:serialNumber (2.5.4.5)	This field **MUST** contain the Subject's full legal organization Number (OrganizationUnit) as listed in the official records of the Government Agency WITH beginning 16 in the following format: 16XXXXXXXXXX
Locality	subject:localityName (2.5.4.7)	This field **MUST** contain the City of the Subject's headoffice of the Government Agency
EMail	Subject:EMail (1.2.840.113549.1.9.1)	This field CAN contain the email of the Subject's responsible of the Government Agency
Country	subject:countryName (2.5.4.6)	This field **MUST** contain the field country where the official records of the Government Agency are. e.g. C = SE

Subject Public Key Information	2048-bit RSA key modulus, rsaEncryption (1.2.840.113549.1.1.1)	
Issuer's Signature	sha256 WithRSAEncryption (1.2.840.113549.1.1.11)	
Extension	**Value**	
Authority Key Identifier	c=no; Octet String – Same as Issuer's	Contains 20 byte SHA-2 hash of the CA Public Key
Subject Key Identifier	c=no; Octet String – Same as calculated by CA from PKCS#10	Contains 20 byte SHA-2 hash of the subjectPublicKey in this certificate
Certificate Policies	[1]Certificate Policy: Policy Identifier=1.2.752.146.2.4 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.myndighetsca.se/cps/	
Key Usage	c=yes; Digital Signature, Key Encipherment (a0)	**Critical**
Extended Key Usage	c=no; Server Authentication (1.3.6.1.5.5.7.3.1) Client Authentication (1.3.6.1.5.5.7.3.2)	
Subject Alternative Name	c=no; DNS = FQDN of Device (e.g., domain.com)	SAN name can be the same as the CN or any other FQDN, can contain multiple SAN name
Authority Information Access	c = no; CRL HTTP URL = http://pki.myndighetsca.se/crl/SwedishGovernmentHWCAv4.crl URL= http://pki.forsakringskassan.se/crl/SwedishGovernmentHWCAv4.crl URL= http://ocsp.myndighetsca.se	
Information about the certificate template	Information about used template	

Programs principle	[1] Program Certificate Policy: Principidentifierare = Server Authentication [2] Program Certificate Policy: Principidentifierare = Client Authentication	
Access to issuers information	[1] Access to issuers information Access Method = Publisher of CA (1.3.6.1.5.5.7.48.2) Alternative Names: URL=http://pki.myndighetsca.se/crl/SwedishGovernmentHWCAv4.crt [2]Åtkomst till information om utfärdare Access Method = Publisher of CA (1.3.6.1.5.5.7.48.2) Alternative Names: URL=http://pki.forsakringskassan.se/crl/SwedishGovernmentHWCAv4.crt	