Försäkringskassan

Swedish Social Insurance Agency Certificate Policy

Key Information:

Formal title:	Swedish Social Insurance Agency Certificate Policy
OID:	HW CA: 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)] } Sign CA: 1.2.752.146.8.3 [.0.0.1] { iso (1) member (2) sweden (752) swedish social insurance agency (146) ssia Sign CA (8.3) [cpvn-top (0) cpvn-2nd (0) cp (1)] }
Responsible authority:	Försäkringskassan Infrastructure Management Authority
Version:	*1.6.0*
Effective date:	*2019-06-10*
Classification / Distribution	Un-classified / Unlimited distribution
Published at:	http://www.myndighetsca.se/cps/
Author:	IMA
Point-of-Contact:	Försäkringskassan Infrastructure Management Försäkringskassan, SE-851 93 Sundsvall, Sweden email: MCA@forsakringskassan.se

Approval record:

Version	Approval date	Author	Approved (role)	Reason / notes
1.6.0	2019-06-10	SSIA IMA	SSIA PMA Board	Approved
1.5.1	2019-05-20	SSIA IMA		Changes in chapter 4.3.2 and 6.1.5 Move Approval Control to chapter 1.5.4
1.5.0	2019-04-29	SSIA IMA	SSIA PMA Board	Approved
1.4.4	2019-04-29	SSIA IMA		Correction of RFC3647, chapter names
1.4.3	2019-04-26	SSIA IMA		Clarification in chapter 4.9.7
1.4.2	2019-04-18	SSIA IMA		Update in chapter 4.9.7
1.4.1	2019-04-16	SSIA IMA		Update in chapter 5.4.3
1.4.0	2019-02-08	SSIA IMA	SSIA PMA Board	Approved
1.3.1	2019-01-21	SSIA IMA		Small corrections
1.3.0	2018-09-28	SSIA IMA	SSIA PMA Board	Approved
1.2.1	2018-08-28	SSIA IMA		Add/Update chapter 1.6.1 and 1.6.3 and small corrections.
1.2.0	2018-06-15	SSIA IMA	SSIA PMA Board	Approved
1.1.1	2018-06-04	SSIA IMA		Updating chapter name according to RFC3647
1.1.0	2018-05-04	SSIA IMA	SSIA PMA Board	Approved
1.0.2	2018-04-26	SSIA IMA		Small changes/updates in document.
1.0.1	2018-04-18	SSIA IMA		Adding algorithms in chapter 7.1.3 Small changes/updates in document.
1.0.0	2017-12-18	SSIA IMA	SSIA PMA Board	Approved
0.9.0	2017-11-30	SSIA IMA		Merging SSIA_HWCA_v4_CP_Ver420 and SSIA_Sign_CA_v3_CP_Ver320. Change Rôle to Role. Change in chapter 5.4 and 5.5 regarding logs.

CONTENTS

1. INTRODUCTION 10
1.1. Overview 10
1.1.1. Certificate Policy 10
1.1.2. Certification Practice Statement 10
1.1.3. Scope of Applicability 10
1.2. Document name and identification 12
1.3. PKI Participants 13
1.3.1. Certification Authorities 13
1.3.2. Registration authorities 14
1.3.3. Subscribers 14
1.3.4. Relying Parties 15
1.3.5. Other Participants 15
1.4. Certificate Usage 15
1.4.1. Appropriate Certificate Uses 15
1.4.2. Prohibited Certificate Uses 15
1.5. Policy Administration 16
1.5.1. Organization Administering the Document 16
1.5.2. Contact Person 16
1.5.3. Person determining CPS suitability for the policy 16
1.5.4. CP Approval Procedures 16
1.6. Definitions and Acronyms 16
1.6.1. Definitions 17
1.6.2. Acronyms 17
1.6.3. References 17
2. PUBLICATION AND REPOSITORY RESPONSIBILITIES 17
2.1. Repositories 17
2.2. Publication of Certification Information 17
2.3. Time or frequency of publication 17
2.4. Access controls on repositories 18
3. IDENTIFICATION AND AUTHENTICATION 18
3.1. Naming 18
3.1.1. Types of Names 18
3.1.2. Need for Names to be meaningful 18
3.1.3. Anonymity or Pseudonymity of Subscribers 18
3.1.4. Rules for interpreting various name forms 18
3.1.5. Uniqueness of names 18
3.1.6. Recognition, Authentication, and Role of Trademarks 19
3.2. Initial Identity Validation 19
3.2.1. Method to Prove Possession of Private Key 19

3.2.2. Authentication of Organization Identity 19
3.2.3. Authentication of Individual Identity 19
3.2.4. Non-verified Subscriber information 19
3.2.5. Validation of Authority 19
3.2.6. Criteria for inter-operation 19
3.3. Identification and Authentication for Re-Key Requests 19
3.3.1. Identification and authentication for routine re-key 19
3.3.2. Identification and authentication for re-key after revocation 20
3.4. Identification and Authentication for Revocation Request 20
4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS 20
4.1. Certificate Application 20
4.1.1. Who Can Submit a Certificate Application 20
4.1.2. Enrolment Process and Responsibilities 20
4.2. Certificate Application Processing 20
4.2.1. Performing Identification and Authentication Functions 20
4.2.2. Approval or rejection of certificate applications 20
4.2.3. Time to process certificate applications 20
4.3. Certificate Issuance 20
4.3.1. CA Actions during Certificate Issuance 20
4.3.2. Notification to subscriber by the CA of issuance of certificate 20
4.4. Certificate Acceptance 21
4.4.1. Conduct Constituting Certificate Acceptance 21
4.4.2. Publication of the Certificate by the CA 21
4.4.3. Notification of Certificate Issuance by the CA to Other Entities 21
4.5. Key Pair and Certificate Usage 21
4.5.1. Subscriber Private Key and Certificate Usage 21
4.5.2. Relying Party Public Key and Certificate Usage 21
4.6. Certificate Renewal 21
4.6.1. Circumstance for Certificate Renewal 21
4.6.2. Who May Request Renewal 22
4.6.3. Processing Certificate Renewal Requests 22
4.6.4. Notification of New Certificate Issuance to Subscriber 22
4.6.5. Conduct Constituting Acceptance of a Renewal Certificate 22
4.6.6. Publication of the Renewal Certificate by the CA 22
4.6.7. Notification of Certificate Issuance by the CA to Other Entities 22
4.7. Certificate Re-Key 22
4.7.1. Circumstance for Certificate Re-key 22
4.7.2. Who may request certification of a new public key 22
4.7.3. Processing certificate re-keying requests 22
4.7.4. Notification of new certificate issuance to subscriber 22
4.7.5. Conduct Constituting Acceptance of a Re-keyed Certificate 22
4.7.6. Publication of the re-keyed certificate by the CA 22
4.7.7. Notification of Certificate Issuance by the CA to Other Entities 22

4.8. Certificate Modification 22
4.8.1. Circumstance for Certificate Modification 22
4.8.2. Who May Request Certificate Modification 22
4.8.3. Processing Certificate Modification Requests 23
4.8.4. Notification of new certificate issuance to subscriber 23
4.8.5. Conduct Constituting Acceptance of a Modified Certificate 23
4.8.6. Publication of the Modified Certificate by the CA 23
4.8.7. Notification of certificate issuance by the CA to other entities 23
4.9. Certificate Revocation and Suspension 23
4.9.1. Circumstances for Revocation 23
4.9.2. Who Can Request Revocation 24
4.9.3. Procedure for Revocation Request 24
4.9.4. Revocation Request Grace Period 24
4.9.5. Time within which CA Must Process the Revocation Request 24
4.9.6. Revocation Checking Requirement for Relying Parties 24
4.9.7. CRL Issuance Frequency 24
4.9.8. Maximum Latency for CRLs 25
4.9.9. On-line Revocation/Status Checking Availability 25
4.9.10. On-line Revocation Checking Requirements 25
4.9.11. Other Forms of Revocation Advertisements Available 25
4.9.12. Special requirements re key compromise 25
4.9.13. Circumstances for Suspension 25
4.9.14. Who Can Request Suspension 25
4.9.15. Procedure for Suspension Request 25
4.9.16. Limits on Suspension Period 25
4.10. Certificate Status Services 25
4.10.1. Operational Characteristics 25
4.10.2. Service Availability 25
4.10.3. Optional Features 25
4.11. End of Subscription 25
4.12. Key Escrow and Recovery 26
4.12.1. Key Escrow and Recovery Policy Practices 26
4.12.2. Session Key Encapsulation and Recovery Policy and Practices 26
5. MANAGEMENT, OPERATIONAL, AND PHYSICAL CONTROLS 26
5.1. Physical Controls 26
5.1.1. Site Location and Construction 26
5.1.2. Physical Access 26
5.1.3. Power and Air Conditioning 26
5.1.4. Water exposures 26
5.1.5. Fire Prevention and Protection 27
5.1.6. Media Storage 27
5.1.7. Waste Disposal 27

5.1.8. Off-site Back-up 27
5.2. Procedural Controls 27
5.2.1. Trusted Roles 27
5.2.2. Number of Persons Required per Task 27
5.2.3. Identification and Authentication for each Role 28
5.2.4. Roles Requiring Separation of Duties 28
5.3. Personnel Controls 28
5.3.1. Qualifications, Experience, and Clearance Requirements 28
5.3.2. Background Check Procedures 28
5.3.3. Training Requirements 28
5.3.4. Retraining Frequency and Requirements 29
5.3.5. Job Rotation Frequency and Sequence 29
5.3.6. Sanctions for Unauthorized Actions 29
5.3.7. Independent Contractor Requirements 29
5.3.8. Documentation Supplied to Personnel 29
5.4. Audit Logging Procedures 29
5.4.1. Types of Events Recorded 29
5.4.2. Frequency of Processing Log 32
5.4.3. Retention Period for Audit Log 32
5.4.4. Protection of Audit Log 32
5.4.5. Audit Log Back-up Procedures 32
5.4.6. Audit Collection System (internal vs. external) 33
5.4.7. Notification to Event-causing Subject 33
5.4.8. Vulnerability Assessments 33
5.5. Records Archival 33
5.5.1. Types of Records Archived 33
5.5.2. Retention Period for Archive 34
5.5.3. Protection of Archive 34
5.5.4. Archive Back-up Procedures 34
5.5.5. Requirements for Time-stamping of Records 34
5.5.6. Archive Collection System (internal or external) 34
5.5.7. Procedures to Obtain and Verify Archive Information 34
5.6. Key Changeover 34
5.7. Compromise and Disaster Recovery 35
5.7.1. Incident and Compromise Handling Procedures 35
5.7.2. Computing Resources, Software, and/or Data Are Corrupted 35
5.7.3. Entity Private Key Compromise Procedures 35
5.7.4. Business Continuity Capabilities after a Disaster 35
5.8. CA or RA Termination 35
6. TECHNICAL SECURITY CONTROLS 35
6.1. Key Pair Generation and Installation 35
6.1.1. Key Pair Generation 35
6.1.2. Private Key Delivery to Subscriber 36

6.1.3. Public Key Delivery to Certificate Issuer 36
6.1.4. CA Public Key Delivery to Relying Parties 36
6.1.5. Key Sizes 36
6.1.6. Public Key Parameters Generation and Quality Checking 37
6.1.7. Key Usage Purposes (as per X.509 v3 key usage field) 37
6.2. Private Key Protection and Cryptographic Module Engineering Controls 37
6.2.1. Cryptographic Module Standards and Controls 37
6.2.2. Private key (n out of m) multi-person control 37
6.2.3. Private Key Escrow 37
6.2.4. Private Key Back-up 37
6.2.5. Private Key Archival 38
6.2.6. Private Key Transfer into or from a Cryptographic Module 38
6.2.7. Private Key Storage on Cryptographic Module 38
6.2.8. Method of Activating Private Key 38
6.2.9. Method of Deactivating Private Key 38
6.2.10. Method of Destroying Private Key 38
6.2.11. Cryptographic Module Rating 38
6.3. Other Aspects of Key Pair Management 38
6.3.1. Public Key Archival 38
6.3.2. Certificate operational periods and key pair usage periods 38
6.4. Activation Data 39
6.4.1. Activation Data Generation and Installation 39
6.4.2. Activation Data Protection 39
6.4.3. Other Aspects of Activation Data 39
6.5. Computer Security Controls 39
6.5.1. Specific Computer Security Technical Requirements 39
6.5.2. Computer Security Rating 40
6.6. Life Cycle Technical Controls 40
6.6.1. System Development Controls 40
6.6.2. Security Management Controls 40
6.6.3. Life Cycle Security Controls 40
6.7. Network Security Controls 40
6.8. Time-stamping 41
7. CERTIFICATE, CRL, AND OCSP PROFILES 41
7.1. Certificate Profile 41
7.1.1. Version Number 41
7.1.2. Certificate Extensions 41
7.1.3. Algorithm Object Identifiers 41
7.1.4. Name Forms 41
7.1.5. Name Constraints 41
7.1.6. Certificate Policy Object Identifier 42
7.1.7. Usage of Policy Constraints Extension 42
7.1.8. Policy Qualifiers Syntax and Semantics 42

7.1.9. Processing Semantics for the Critical Certificate Policies Extension 42
7.2. CRL Profile 42
7.2.1. Version number(s) 42
7.2.2. CRL and CRL Entry Extensions 42
7.3. OCSP PROFILE 42
7.3.1. Version Number(s) 42
7.3.2. OCSP Extensions 42
8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS 42
8.1. Frequency or Circumstances of Assessment 42
8.2. Identity/Qualifications of Auditors 42
8.3. Assessor's Relationship to Assessed Entity 43
8.4. Topics covered by Assessment 43
8.5. Actions taken as a result of Deficiency 43
8.6. Communication of Results 43
8.7. Self-Audits 43
9. OTHER BUSINESS AND LEGAL MATTERS 43
9.1. Fees 43
9.1.1. Certificate issuance or renewal fees 43
9.1.2. Certificate access fees 43
9.1.3. Revocation or status information access fees 43
9.1.4. Fees for other services 44
9.1.5. Refund policy 44
9.2. Financial Responsibility 44
9.2.1. Insurance Coverage 44
9.2.2. Other Assets 44
9.2.3. Insurance or Warranty Coverage for End-Entities 44
9.3. Confidentiality of Business Information 44
9.3.1. Scope of Confidential Information 44
9.3.2. Information Not Within the Scope of Confidential Information 44
9.3.3. Responsibility to Protect Confidential Information 44
9.4. Privacy of Personal Information 44
9.4.1. Privacy plan 44
9.4.2. Information Treated as Private 44
9.4.3. Information Not Deemed Private 44
9.4.4. Responsibility to Protect Private Information 44
9.4.5. Notice and Consent to Use Private Information 44
9.4.6. Disclosure Pursuant to Judicial or Administrative Process 44
9.4.7. Other Information Disclosure Circumstances 45
9.5. Intellectual Property Rights 45
9.6. Representations and Warranties 45
9.6.1. CA Representations and Warranties 45
9.6.2. RA Representations and Warranties 45
9.6.3. Subscriber Representations and Warranties 45
9.6.4. Relying Party Representations and Warranties 45
9.6.5. Representations and Warranties of Other Participants 45

9.7. Disclaimers of Warranties **45**
9.8. Limitations of Liability **46**
9.9. Indemnities **46**
9.9.1. Indemnification by an Issuer CA 46
9.9.2. Indemnification by Subscribers 46
9.9.3. Indemnification by Relying Parties 46
9.10. Term and Termination **46**
9.10.1. Term 46
9.10.2. Termination 46
9.10.3. Effect of Termination and Survival 46
9.11. Individual Notices and Communications with Participants **46**
9.12. Amendments **46**
9.12.1. Procedure for Amendment 46
9.12.2. Notification Mechanism and Period 46
9.12.3. Circumstances under which OID Must Be Changed 47
9.13. Dispute Resolution Provisions **47**
9.14. Governing Law **47**
9.15. Compliance with Applicable Law **47**
9.16. Miscellaneous Provisions **47**
9.16.1. Entire Agreement 47
9.16.2. Assignment 47
9.16.3. Severability 47
9.16.4. Enforcement (attorneys' fees and waiver of rights) 47
9.16.5. Force Majeure 47
9.17. Other Provisions **47**
9.17.1. Inter-Agency Agreement 47

1. INTRODUCTION

1.1. Overview

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

1.1.1. Certificate Policy

This document sets forth the Certificate Policy (CP) addressing the provision of certificates by Försäkringskassan (SSIA), the Swedish government's Social Insurance Agency (hereafter SSIA) to Swedish government agencies, and for the life-cycle management of those certificates. These certificates shall be issued from the 'HW CA v4' and 'Sign CA v3'. This policy is published under the authority of the SSIA Infrastructure Management Authority (SSIA PMA), whose executive mandate is defined in the SSIA PMA Charter [SSIA PMAcharter].

For public-facing references, the English-language title (and associated abbreviation) of SSIA shall be used.

1.1.2. Certification Practice Statement

This policy may be referenced by any Certification Practice Statement (CPS) fulfilling the obligations herein. Specifically, the SSIA Certification Practice Statement [SSIA CPS] fulfils all the obligations of this policy.

1.1.3. Scope of Applicability

This CP covers SSIA's Public Key Infrastructure (SSIA PKI) which issues Certificates to SSIA subscribers (Swedish government agencies). This CA does not issue EV certificate. Figure 1 offers a schematic representation of the SSIA PKI and its relationship to its subscribers.

Figure 1 - Scope and Domain of the SSIA PKI

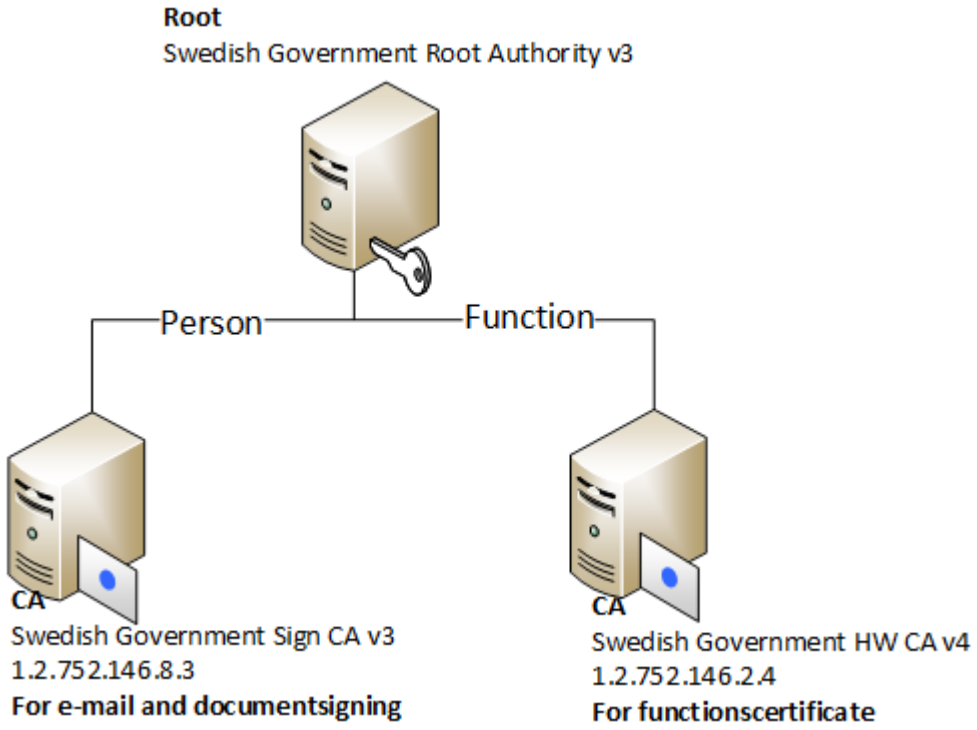

Figure 2 – Issuing CAs of the SSIA PKI

Certificates issued pursuant to this CP are intended for use solely within the Swedish government and its agencies, and their contracted service providers (hereafter assumed to be included within any reference to the government or its agencies), and there are no provisions within this CP for cross-certification or other forms of recognition or usage of certificates issued under this CP by or with certificates issued by other governments, other CAs or under any other PKIs.

Any use of or reference to this CP outside the purview of the SSIA PKI is therefore exercised completely at the using party's own risk. Parties' outwith the scope of this CP shall not assert the OIDs listed in Section 1.2 of this CP in any certificates they may issue.

This CP 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 CP 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). In the event of any inconsistency between this CP and those Guidelines, the latter shall take precedence. SSIA also conforms to ISO/IEC 27001.

This CP presents a single level of identity assurance, that implied by conformity with [CABF]. The CP covers the issuance of these types of Certificate:

a) HW CA - Agency Client HW Certificates (having the purposes described in [CABF] §6.1.1 (1));
b) HW CA - Agency Server HW Certificates (having the purposes described in [CABF] §6.1.1 (1));
c) HW CA - Agency Encryption Certificates (having the purposes described in [CABF] §6.1.1 (2)).
d) Sign CA - Agency Signing Certificates;
e) Sign CA - Agency S/mime Certificates;

1.2. Document name and 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} and the OID for the Swedish Social Insurance Agency's Sign CA v3 (ssia-SignCA) is defined in the applicable CP as {1.2.752.146.8.3}.

Ssia	::= { iso (1) member-body (2) sweden (752) swedish social insurance agency (146) } 1.2.752.146
ssiaRootCA	::= { ssia 1.0 } 1.2.752.146.0
ssia HWCA	::= { ssia 2.2 } 1.2.752.146.2.4
ssia SignCA	::= { ssia 8.3 } 1.2.752.146.8.3

Policy OIDs addressed by this CP are:

ssia-HWclient	::= { ssia- HWCAv4 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
ssia-Signing	::= { ssia- SignCA 100 } 1.2.752.146.8.3.100
ssia-Signing s/mime	::= { ssia- SignCA 200 } 1.2.752.146.8.3.200

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- CP	{ssia- cpvn-top cpvn-2nd } ssia-HWCA - 1.2.752.146.2.4.x.y ssia-SignCA - 1.2.752.146.8.3.x.y
ssia- CPS	{ssia-CPS } ssia-HWCA - 1.2.752.146.2.4.x.y.1 ssia-SignCA - 1.2.752.146.8.3.x.y.1

These OID relationships are shown schematically in Figure 2, in context with other CAs falling under the authority of the SSIA IMA.

This CP shall apply to any entity asserting any of the above-defined policy OIDs.

1.3. PKI Participants

This section describes the roles relevant to the administration and operation of the SSIA PKI.

1.3.1. Certification Authorities

1.3.1.1. SSIA Management Authority

The SSIA IMA shall report to SSIA IT Production Manager and shall be responsible for the following:

a) Management of initial drafting and subsequent amendments to the SSIA CP;
b) Review and approval of top-level versions of the SSIA CP, prior to them becoming operationally effective;
c) Commissioning of audits of the policy management and operations of the SSIA PKI so as to maintain the certifications required by this CP; and
d) Taking action to ensure policy-related audit recommendations are implemented.

The SSIA IMA shall be chaired by the SSIA Infrastructure Manager who shall be appointed by the SSIA IT Production Manager. A complete description of SSIA IMA roles and responsibilities is provided in [SSIA PMAcharter].

1.3.1.2. SSIA Policy Working Group

The SSIA Policy Working Group (SSIA PWG) is established to undertake developmental work and analysis, as follows:

a) Identification and drafting of internally-originating proposals for changes to this CP;
b) Review of received proposals for changes to this CP;
c) Recommendations to the SSIA IMA for approval or rejection (by the SSIA IMA) of any such changes; and
d) Compliance analysis and recommendations for approval (by the SSIA IMA) of [SSIA CPS] and any other CPS.

The SSIA PWG shall be chaired by the SSIA Infrastructure Manager.

1.3.1.3. SSIA Operational Authority

The SSIA Operational Authority (SSIA OA) shall be headed by the SSIA OA Manager who shall be appointed by and report to the SSIA IT Production Manager. The SSIA OA is responsible for the operation of the CA. This includes:

a) Drafting, maintenance and submission for approval of the [SSIA CPS];
b) Maintaining the currency of certificates and CRLs recorded in the SSIA PKI Repository (SSIA PKI);
c) Performing back-ups and ensuring the readiness of all back-up facilities;
d) Ensuring the on-going availability of all CA services and facilities in accordance with [SSIA CPS]; and
e) Taking action to ensure that audit recommendations concerning operational practices are implemented.

1.3.1.4. SSIA Portal Administrator

Portal Administrators (SSIA PortAdmin) shall be individuals assigned to the Operational Authority having responsibility for overseeing the proper operation of the SSIA CA including its configuration, the registration of Agency Administrators (see §1.3.2) and the verification of requests for certificate issuance and revocation. They may be assigned Trusted Roles as defined in §5.2.1.

The SSIA PortAdmins shall be appointed by and report to the SSIA OA Manager.

1.3.1.5. Root CA

There is a SSIA Root CA which issues the SSIA CA a certificate. Policy directives for this CA is in the scope of this document.

1.3.1.6. Intermediate CA

There shall be no Intermediate CAs.

1.3.1.7. Signing CA

This is the SSIA CA (see chapter 3.1.2, 'SSIA SignCA' and 'SSIA HWCA') that issues certs to its Subscribers.

1.3.1.8. Certificate Status Authority

This is within the SSIA CA. Certificate responses are provided using CRL/OCSP to provide certificate revocation status.

1.3.2. Registration authorities

Agency Server Administrators shall be individuals assigned to and appointed by their respective Agency Administrator (see §1.3.3). They shall be responsible for creating and submitting certificate applications, solely within their specific agency and in accordance with an Inter-Agency Agreement [IAA] which shall serve the purposes of a 'Subscriber Agreement' and 'Relying Party Agreement' (see §9.17.1).

This function fulfils the 'RA' role and it is they to whom the term 'RA" refers when used further in this CP.

1.3.3. Subscribers

Refer to §1.6 for the definitions of Subscriber and Subject specific to this CP.

Swedish government agencies are the SSIA PKI's Subscribers and the entities within each agency to which certificates are issued are its Subjects.

Each agency requiring the issuance of Certificates shall appoint an Agency Administrator, who shall be responsible for the oversight of certificate issuance within their own agencies, in accordance with an Inter-Agency Agreement [IAA], and for the appointment of Agency Administrators (see §1.3.2). Agency Administrators shall be authorized according to the procedure defined in [IAA].

Any stipulations in this CP affecting Subscribers shall also apply to Subjects unless the context or a specific statement makes it clear that it is applicable only to the Subscriber.

1.3.3.1. Subjects

Entities within each agency to which Certificates are issued are the Subjects of those certificates. Subjects shall be required to acknowledge the terms of [IAA].

Note - In some PKIs no distinction is made between the terms Subscriber and Subject, which may be used synonymously and interchangeably.

1.3.4. Relying Parties

Agencies participating within the SSIA-PKI and the customers of those agencies (e.g. any party having permissible access to agency resources employing certificates issued according to this CP) shall be the Relying Parties recognized by the PKI and shall use certificates according to the stipulations of [IAA].

Relying Parties shall be any persons or entities gaining access to Swedish government agency websites which have been issued with a Certificate under the terms of this CP, by the SSIA CA.

1.3.5. Other Participants

1.3.5.1. Auditors

The SSIA PKI will require the services of other security authorities, such as compliance auditors. Any CPS citing an OID assigned to this document shall identify the parties responsible for providing such services, and the mechanisms used to support them.

1.4. Certificate Usage

1.4.1. Appropriate Certificate Uses

Certificates issued under this CP may be used for the purposes designated in the key usage and extended key usage fields found in the certificate. However, the sensitivity of the information processed or protected by a certificate varies greatly, and each Relying Party must evaluate the application environment and associated risks before deciding on whether to use a certificate issued under this CP.

This CP covers different types of end entity certificates/tokens with varying levels of assurance. The following table provides a brief description of the appropriate uses of each.

Certificate/Token	Appropriate Use
HW CA - HW Certificates	Identify the Swedish Government Agency that controls a Web site: Provide a reasonable assurance to the user of an Internet browser that the Web site the user is accessing is controlled by the Agency identified in the Certificate, identified by its existence in the [IAA].
HW CA - Encryption Certificates	Enable encrypted communications with a Swedish Government Agency Web site: 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 Web site provided by the Agency identified in the Certificate, identified by its existence in the [IAA].
Sign CA – Signing and s/mime Certificates	These certificates are used to sign documents and e-mails.

1.4.2. Prohibited Certificate Uses

Certificates do not attest to the good behaviour of the certificate Subjects and Subscribers. They shall not be taken to guarantee that the Subject is trustworthy, honest, reputable in its business dealings, compliant with any laws, or safe to do business with. Code signing certificates do not indicate that the signed code is safe to install or free from malware, bugs, or other forms of threats and vulnerabilities.

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

a) any application having a direct relationship with any safety- or environmental-critical systems;
b) where prohibited by any laws, be they national, European or international.

1.5. Policy Administration

1.5.1. Organization Administering the Document

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

1.5.2. Contact Person

The 'IMA 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 shall determine the suitability of the [SSIA CPS] after taking into consideration the advice of the SSIA PWG (see §1.3.1.2).

1.5.4. CP Approval Procedures

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 this CP which has a **significant policy change** requiring a change of the policy's OID;
Second-level:	A formal release of this CP which has a **no significant policy change** and therefore does NOT require a change of the policy's OID;
Third-level:	A draft of this CP 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 Infrastructure Management Authority (SSIA IMA) for archival purposes.

On its effective date a formal version of this CP 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 IMA shall preserve records of all past versions.

Approval authorities:

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

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

1.6. Definitions and Acronyms

Unless alternative definitions, meanings or interpretations are assigned in the following parts of this sub-clause, the definitions in [CABF] and [RFC3647] apply. Should there be any conflict between terms defined in both these documents, [CABF] shall take precedence.

1.6.1. Definitions

Administrator: Either an Agency Administrator (see §1.3.3) or an Agency System Administrator (see §1.3.2), where either role may perform the required action.

Public: the community of participating Agencies within the Swedish government.

Relying Party: used subject to the limitations defined in §1.3.4 but otherwise with the meaning ascribed to it in [RFC3647].

SSIA CA: The Swedish Social Insurance Authority Certificate Authority. Usage of this acronym will, depending upon context, refer to the actual CA systems itself or the management of the SSIA CA, i.e. the SSIA OA (defined in §1.3.1.3).

Subject: entity identified in a certificate as the holder of the private key associated with the public key given in the certificate [TS102042].

Subscriber: entity subscribing with a Certification Authority on behalf of one or more Subjects [TS102042].

WHOIS: information retrieved directly from the Domain Name Registrar or registry operator via the protocol defined in RFC 3912, the Registry Data Access Protocol defined in RFC 7482, or an HTTPS website.

1.6.2. Acronyms

1.6.3. References

- RFC3912, Request for Comments: 3912, WHOIS Protocol Specification, Daigle, September 2004.
- RFC7482, Request for Comments: 7482, Registration Data Access Protocol (RDAP) Query Format, Newton, et al, March 2015.

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1. Repositories

The following responsibilities for establishing repositories of, and publishing, information related to the SSIA PKI shall be fulfilled:

Responsible Entity	Information required to be published	Notification of change
SSIA IMA	This CP	Within five business days of approval of any revision
	[IAA]	
SSIA OA	[SSIA CPS]	
	Subscriber Certificates	Within 24 hours of issuance
	Certificate Revocation information	Within 18 hours of any change

2.2. Publication of Certification Information

Each Responsible Entity shall ensure that information for which it has a publishing responsibility shall be available through a publically accessible, on-line, repository.

2.3. Time or frequency of publication

Each Responsible Entity shall ensure that information for which it has a publishing responsibility shall be available 24 hours a day, 7 days a week with a minimum of 99% availability overall per annum, with a scheduled down-time that does not exceed 0.5% per annum.

2.4. Access controls on repositories

Information published in a repository is Public information. The Responsible Entity shall provide unrestricted read access to its repositories and shall implement logical and physical controls to prevent unauthorized modification to such repositories.

3. IDENTIFICATION AND AUTHENTICATION

3.1. Naming

3.1.1. Types of Names

SSIA CA shall issue certificates with a non-null subject Distinguished Name (DN) that complies with ITU X.500 standards. DNs must respect name space uniqueness.

3.1.2. Need for Names to be meaningful

Distinguished Names in certificates shall identify the Subject by giving an accurate description of the Agency (which shall be that used in [StatsRegister] per §3.1.5, which shall be considered a Qualified Government Information Source (QGIS, per [CABF])) and Agency Entity to which they relate.

The Distinguished Name for the issuer 'SSIA HWCA' shall be:

C = SE
O = SSIA
OU = «null»
CN = "Swedish Government HW CA v4"

The Distinguished Name for the issuer 'SSIA SignCA' shall be:

C = SE
O = SSIA
OU = «null»
CN = "Swedish Government Sign CA v3"

Directory information trees shall accurately reflect organizational structures.

3.1.3. Anonymity or Pseudonymity of Subscribers

Neither Subscribers nor Subjects may use anonymous or pseudonymous names.

3.1.4. Rules for interpreting various name forms

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

3.1.5. Uniqueness of names

Name uniqueness in certificates shall be ensured by assigning each participating Agency the name given it in the register maintained by Statistiska centralbyrån (Statistics Sweden) [StatsRegister], available at http://www.myndighetsregistret.scb.se/Myndighet. Where the Subject is an outsourced service provider an additional OU field shall be injected (see below).

Individual Agencies shall be responsible for assigning names to Agency Entities. In the event of any potential name clashes at the Agency Entity level, RAs shall be responsible for resolving these and submitting a unique DN within Certificate Applications. Certificate DNs shall thus have the form:

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

3.1.6. Recognition, Authentication, and Role of Trademarks

RAs may neither accept nor generate requests for certificates with any content that infringes the intellectual property rights of another entity. Explicitly, no certificate application may use any trademark, nor the identifying marks of any agency other than the Subscriber Agency issuing the request.

3.2. Initial Identity Validation

The SSIA CA shall only recognize agencies according to [StatsRegister].

3.2.1. Method to Prove Possession of Private Key

Key-pairs may be generated by the SSIA CA or be presented by the Applicant. The SSIA CA shall verify that the Applicant possesses the Private Key corresponding to the Public Key.

3.2.2. Authentication of Organization Identity

In the context of this CP, 'Organizations' shall be Swedish government Agencies – all Agencies defined in [StatsRegister] shall be eligible applicants, as Subscribers. On initial application the Agency representative shall sign and submit on behalf of their Agency their acceptance of [IAA] (*the signatory serves as the [CABF] Authorized Representative; the agreement fulfilling [CABF]'s requirements for Terms of Use*).

The SSIA CA shall verify 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 authority of a person to request a certificate on behalf of an Agency shall be verified in accordance with Section 3.2.5.

At the time of submitting their application Administrators shall reference and acknowledge the applicability of [IAA] and date their request.

These checks shall fulfil the requirements of [CABF] §4.2.1 (2) in accordance with [CABF] §4.2.2 (2).

3.2.3. Authentication of Individual Identity

For any certificate type request, the RA or appointed Agency Server Administrator shall verify an entity's identity in accordance with the process established in [SSIA CPS]. This shall include verification through the registrar for that domain of the Applicant Agency's right to use any domain name(s) listed in the request. Additional information required for issuance of Certificates shall be verified in accordance with Guidelines. End-entities may be non-governmental entities to which an Agency has outsourced certain services which need to be the Subjects of an Agency SSL Certificate. They shall be identified per §3.1.5.

3.2.4. Non-verified Subscriber information

No stipulation.

3.2.5. Validation of Authority

The SSIA CA shall validate the authority of an entity requesting any type of certificate by verifying that they are either the requesting Agency's Administrator or one of the requesting Agency's appointed Agency Server Administrators, by reference to a register of established Inter-Agency Agreements [IAARegister] maintained by the SSIA IT Production Manager]. Authentication shall rely upon User certificates issued by "Swedish Government User CA v1" and "Swedish Government Auth CA v2" which shall map to the Agency name and Agency number from [StatsRegister].

A Certificate Application may only be made for a Subject in the same Agency's domain as the requesting RA.

3.2.6. Criteria for inter-operation

No stipulation.

3.3. Identification and Authentication for Re-Key Requests

Re-keying shall not be supported.

3.3.1. Identification and authentication for routine re-key

Re-keying shall not be supported.

3.3.2. Identification and authentication for re-key after revocation

Re-keying shall not be supported.

3.4. Identification and Authentication for Revocation Request

All Revocation Requests shall be authenticated by the SSIA CA or the Administrator that approved certificate issuance. Any Revocation Request may be authenticated by reference to the Certificate's Public Key, regardless of whether the associated Private Key is compromised.

4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1. Certificate Application

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

4.1.1. Who Can Submit a Certificate Application

The SSIA CA shall only accept Certificate Applications from a designated RA, who shall only be permitted to request certificates for their own Agency's (or if other is stipulated in the [IAA]) Subjects.

4.1.2. Enrolment Process and Responsibilities

Validation personnel of the SSIA CA or the RA are responsible for verifying the identity of individuals or entities in accordance with this CP prior to authorizing issuance of a certificate. Each Applicant shall submit sufficient information and documentation for the SSIA CA or the RA to perform the required verification of identity prior to issuing a Certificate. All communication during the Certificate Application process, including delivery of public keys to be included in Certificates, shall be authenticated and protected from modification.

4.2. Certificate Application Processing

Prior to issuing the certificate the SSIA CA or the RA shall verify the information in each Certificate Applications and shall further ensure that the requested certificate contents are accurate.

4.2.1. Performing Identification and Authentication Functions

Validation personnel of the SSIA CA or the RA shall identify and verify each Applicant in accordance with Section 3.2. Applicable Certification Practice Statements and [IAA] must identify who (RA, Trusted Agent, other entity, or individual) performs the identification and authentication steps required to issue a Certificate to the Applicant in each case.

4.2.2. Approval or rejection of certificate applications

Certificate Applications that cannot be verified shall be rejected. The SSIA CA may also reject a Certificate Application 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 applications

All parties involved in Certificate Applications processing shall use reasonable efforts to ensure that Certificate Applicants are processed in a timely manner. Once the SSIA CA receives a request from a RA it shall be processed within 24 business hours.

4.3. Certificate Issuance

4.3.1. CA Actions during Certificate Issuance

During the certificate issuance process, the SSIA CA shall verify that the identified and authenticated Applicant is the source of the certificate application and that the Subject individual or entity exists within the indicated Agency. 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 subscriber by the CA of issuance of certificate

The SSIA CA or Agency Administrator shall notify the Subject within seven business days of a certificate's issuance and may use any reliable mechanism to deliver the certificate to the Subject.

The SSIA CA or other reliable mechanism shall notify the Subject that a certificate requires renewal (see §4.6) not less than thirty calendar days prior to the certificates expiry.

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

All certificates issued by the SSIA CA shall be published in the SSIA CA's repository.

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

ssia-HWCA	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.
ssia-SignCA	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(see §1.4.1). All agencies should have a liaison with key holders where it should be clear that key holders must comply with the following obligations: (a) Certify that the information provided to SSIA when applying for the certificate is correct and complete and in accordance with the requirements of CP/CPS; b) Only use the key pair for the purposes of certificate and in compliance with other restrictions that reiterated key holder; c) Exercise reasonable care to prevent unauthorized persons can use the private key; this includes, among other things the following measures: i. Not to reveal YOUR PIN or other security routine for other, ii. Protect the smart card similarly as a value object, iii. Do not store the note about the PIN or PUK so that someone else receive the information or can understand that the note refers to the PIN or PUK iv. Do not store the note about the PIN or PUK along with the smart card, v. Not leaving a smart card unattended. d) Promptly notify the SSIA by making a notice of revocation, if any of the following occur: i. The private key is lost or stolen is suspected to have been compromised; ii. Certificate contains incorrect or outdated information. e) If the private key has been compromised, it shall immediately cease use.

4.5.2. Relying Party Public Key and Certificate Usage

Relying Party software shall be compliant with X.509 and applicable IETF PKIX standards. The SSIA CA shall specify restrictions on the use of a certificate through certificate extensions and shall specify the mechanism(s) to determine certificate validity (CRLs). Relying Parties must process and comply with this information in accordance with their obligations as Relying Parties.

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 certification of a new public key

No stipulation.

4.7.3. Processing certificate re-keying requests

No stipulation.

4.7.4. Notification of new certificate issuance to subscriber

No stipulation.

4.7.5. Conduct Constituting Acceptance of a Re-keyed Certificate

No stipulation.

4.7.6. Publication of the re-keyed 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

Modifying a certificate means creating a new certificate for the same subject with authenticated information that differs slightly from the old certificate (e.g., changes to email address or non-essential parts of names or attributes) provided that the modification otherwise complies with this CP. The new certificate may have the same or a different subject public key. Additional examples of circumstances when certificate modification may occur include minor name changes (e.g., change CA1 to CA2) as part of key rollover procedures, organizational name change (e.g. as the result of merger, acquisition, or legally documented name change), and the replacement of the certificate where a minor error in certificate information or profile has been discovered.

After modifying a client certificate, the SSIA CA 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 CA may modify certificates at the request of the Subject or at its own discretion.

4.8.3. Processing Certificate Modification Requests

After receiving a request for modification, the SSIA CA shall verify any information that will change in the modified certificate. The SSIA CA 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 section 3.3.1 or 6.3.2.

4.8.4. Notification of new certificate issuance 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 issuance 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 CA shall verify that the revocation request was made by either the Subject or the applicable RA that made the Certificate Application, or by an entity with the legal jurisdiction and authority to request revocation. The SSIA CA 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 Application was not authorized and does not retroactively grant authorization;

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

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

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

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

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

k) the SSIA CA 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 CA'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 CA determines, at its sole discretion, warrant revocation.

The SSIA CA 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 CA, the SSIA CA shall revoke all certificates issued in the name of that Agency.

4.9.2. Who Can Request Revocation

The SSIA CA or RA shall accept revocation requests from authenticated and authorized parties, such as the certificate Subscriber and the Affiliated Organization named in a certificate. The SSIA CA or RA may establish procedures that allow other entities to request certificate revocation for fraud or misuse. The SSIA CA shall revoke a certificate if it receives sufficient evidence of compromise of loss of the Private Key. The SSIA CA 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 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 CA or RA shall authenticate and log each revocation request.

The SSIA CA 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 CA or RA shall investigate the reason for the revocation request and act according to their findings.

The SSIA CA shall provide a 24/7 response to any high-priority certificate problem reports. When required by law or other explicit policy or directive, the SSIA CA or the RA may notify law enforcement. The SSIA CA shall list revoked certificates on an appropriate CRL where they shall be published until one full publication cycle after the end of the certificate's validity.

The SSIA CA shall publish its revocation and problem reporting procedures.

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 CA within one hour of discovery. The SSIA CA 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

The SSIA CA shall revoke a certificate within one hour of receiving an actionable request or making its own decision to revoke.

4.9.6. Revocation Checking Requirement for Relying Parties

Prior to relying on information listed in a certificate, a Relying Party shall confirm the validity of each certificate in the certificate path in accordance with IETF PKIX standards, including checks for certificate validity, issuer-to-subject name chaining, policy and key use constraints, and revocation status through CRLs responders identified in each certificate in the chain. This shall be stated in [IAA].

4.9.7. CRL Issuance Frequency

The SSIA CA shall publish CRLs within 18 hours of notice of a key compromise.

ssia-HWCA	The SSIA CA CRL shall be updated and issued at least once every seven (7) days and record the date and time of the transaction in the CRL's Effective date field. The CRL's *NextUpdate* field value identifies the point in time when the CRL expires and MUST NOT be more than 7 days and 12 hours after the value of the Effective date field.

ssia-SignCA	The SSIA CA CRL shall be updated and issued at least once every 12 hours and record the date and time of the transaction in the CRL's Effective date field. The CRL's *NextUpdate* field value identifies the point in time when the CRL expires and MUST NOT be more than 24 hours after the value of the *Effective date* field.

Upon expiration of certain CAs a final CRL MAY be published that has a *NextUpdate* value that exceeds the time parameters noted elsewhere in this section.

4.9.8. Maximum Latency for CRLs

The SSIA CA shall post an irregular, interim or emergency CRL to its online repository within four hours of generation (and no later than 18 hours after notification of compromise) and shall publish all regularly scheduled CRLs prior to the `nextUpdate` field in the previously issued CRL of the same scope.

4.9.9. On-line Revocation/Status Checking Availability

The SSIA CA shall ensure that the certificate status information distributed by it on-line meets or exceeds the requirements for CRL issuance and latency stated in §4.9.5, §4.9.7 and §4.9.8.

4.9.10. On-line Revocation Checking Requirements

A relying party must confirm the validity of a certificate via CRL in accordance with section §4.9.6, prior to relying on the certificate. This shall be stated in [IAA].

4.9.11. Other Forms of Revocation Advertisements Available

None shall be permitted

4.9.12. Special requirements re key compromise

The SSIA CA or RA shall use reasonable efforts to notify potential Relying Parties if it discovers or suspects that its Private Key has been compromised. If a certificate is revoked because of compromise or suspected compromise, the SSIA CA shall issue a CRL within 18 hours after it receives notice of the compromise or suspected compromise.

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 CA shall make certificate status information available via CRL. CRLs shall be updated at least once every seven (7) days.

4.10.2. Service Availability

SSIA CA shall provide certificate status services 24x7 without interruption, subject to §2.3.

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 CA 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 PHYSICAL CONTROLS

5.1. Physical Controls

5.1.1. Site Location and Construction

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

5.1.2. Physical Access

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

The SSIA CA shall manually or 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. SSIA CA 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 CA 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 CA shall assign to a person or group of persons explicitly responsibility for making security checks. If a group of persons is responsible, the SSIA CA 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.

5.1.3. Power and Air Conditioning

The SSIA CA shall maintain a back-up power supply and sufficient environmental controls to protect the CA systems such that the CA shall be able to automatically conclude pending operations and record the system state prior to a lack of power or environmental conditioning causes a shutdown.

5.1.4. Water exposures

The SSIA CA shall protect its CA equipment from water exposure.

5.1.5. Fire Prevention and Protection

The SSIA CA shall protect its CA equipment from fire by installing mechanisms which detect fire and act to suppress it.

5.1.6. Media Storage

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

5.1.7. Waste Disposal

The SSIA CA and all RAs shall destroy all data (electronic and paper) in accordance with [DoD5220.22M] procedures for permanently destroying such data.

5.1.8. Off-site Back-up

The SSIA CA or RA shall make weekly system back-ups sufficient to enable recovery from system failure and shall store the back-ups, including at least one full back-up copy, at an offsite location that has procedural and physical controls that are commensurate with its operational location and which satisfy the levels of control implied elsewhere in this CP.

5.2. Procedural Controls

5.2.1. Trusted Roles

SSIA CA and RA personnel acting in Trusted Roles include system administration personnel and personnel involved with customer (Subscriber/Subject) support and vetting. SSIA CA and RAs shall design, document and publish the functions and duties performed by persons in Trusted Roles in a way that prevents one person from circumventing security measures or subverting the security and trustworthiness of the PKI. All personnel in Trusted Roles must be free from conflicts of interest that might prejudice the impartiality of CA and RA operations. Senior management of the SSIA CA or the Subscribing Agency shall be responsible for appointing individuals to Trusted Roles (See §1.3). Those in such roles shall be identified through the [IAA].

5.2.1.1. SSIA PKI Administrator

The SSIA PKI Administrator is responsible for the installation and configuration of the SSIA CA 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 CA system.

The SSIA PKI Administrator is also responsible for managing the Certificate Application 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

The Agency Registration Agent role 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.

5.2.1.4. Internal Auditor Role

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

5.2.2. Number of Persons Required per Task

Each SSIA CA shall require that at least two people acting in a Trusted Role (one the SSIA OA and the other not an Internal Auditor) take action to activate the SSIA CA's Private Keys, generate a CA key pair, or back-up a CA private key. The

Internal Auditor may serve to fulfil the requirement of multi-party control for physical access to the CA system, but logical access shall not be achieved using personnel that serve in the Internal Auditor role.

5.2.3. Identification and Authentication for each Role

SSIA CA personnel are required to present themselves for authentication by the certificate management system before they are allowed access to the systems necessary to perform their Trusted Roles.

5.2.4. Roles Requiring Separation of Duties

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

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 role, assume both the Administrator and Auditor roles, or assume both the Auditor and Officer roles. No individual shall have more than one identity.

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

5.3. Personnel Controls

Note – in this section reference is made frequently to 'the SSIA CA and RAs' with the intention that the SSIA CA shall have primacy insofar as is possible, but that (whilst remaining compliant to this CP) RAs will have latitude for specific implementation where Agency rules or circumstances so require.

5.3.1. Qualifications, Experience, and Clearance Requirements

The SSIA OA is responsible and accountable for the operation of the SSIA PKI and compliance with this CP and the CPS. SSIA CA and RA personnel and management within the SSIA PKI shall be assigned to Trusted Roles on the basis of loyalty, trustworthiness, and integrity. There is no citizenship requirement for SSIA CA or RA personnel performing Trusted Roles.

Managerial personnel involved in time-stamping operations must possess experience with information security and risk assessment and knowledge of time-stamping technology, digital signature technology, mechanisms for calibration of time stamping clocks with UTC, and security procedures.

The SSIA CA and RAs shall define in their CPS the experience, qualifications, and trustworthiness required to perform their duties under this CP and ensure that all individuals assigned to Trusted Roles exhibit these attributes.

5.3.2. Background Check Procedures

Each person fulfilling a Trusted Role must undergo checks and identification prior to acting in the role , including verification of the individual's identity, employment history, education, character references, social security number, previous residences, driving records and criminal background. Background investigations must be performed by a competent independent authority that has the authority to perform background investigations. The SSIA CA and RAs 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. The highest education degree obtained must be verified regardless of the date awarded.

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 CP and thereafter prior to appointment for new personnel.

5.3.3. Training Requirements

The SSIA CA shall provide skills training to all personnel involved in the SSIA CA's PKI operations. The training relates to the person's job functions and covers:

a) basic Public Key Infrastructure (PKI) knowledge;

b) software versions used by the SSIA CA;

c) authentication and verification policies and procedures;

d) disaster recovery and business continuity procedures;

e) common threats to the validation process, including phishing and other social engineering tactics, and [CABF].

The SSIA CA shall maintain records of who received training and what level of training was completed. Validation specialists must have the minimum skills necessary to satisfactorily perform validation duties before they are granted validation privileges.

The SSIA CA and RAs involved with the operation of CMS shall ensure that all personnel who perform duties involving the CMS receive comprehensive training. The SSIA CA and RAs shall create a training (awareness) covering all aspects of SMS operations and certificate issuance, and shall document the execution of the plan, including recording the names and qualifications achieved of personnel trained under this plan.

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 Roles. The SSIA CA and RAs shall make individuals acting in Trusted Roles aware of any changes to the SSIA CA's and RAs' operations. If such operations change, the SSIA CA and RAs shall provide documented training, in accordance with an executed training plan, to all Trusted Roles.

5.3.5. Job Rotation Frequency and Sequence

No stipulation.

5.3.6. Sanctions for Unauthorized Actions

The FKIMA and RAs shall ensure appropriate administrative and disciplinary actions are taken against personnel who violate this policy.

5.3.7. Independent Contractor Requirements

Any SSIA CA or RAs allowing independent contractors to be assigned to perform Trusted Roles shall require that they agree to the obligations under this clause and the sanctions implied above in §5.3.6.

5.3.8. Documentation Supplied to Personnel

The SSIA CA and all RAs shall provide personnel in Trusted Roles with the documentation necessary to perform their duties.

5.4. Audit Logging Procedures

5.4.1. Types of Events Recorded

SSIA CA and RAs systems (including any CMS) shall require identification and authentication at system logon. Important system actions shall be logged to establish the accountability of the operators who initiate such actions.

The SSIA CA and all RAs shall enable all essential event auditing capabilities of its CA or RA applications in order to record all events related to the security of the CA or RA (listed below). A message from any source received by the SSIA CA requesting an action related to the operational state of the CA is an auditable event. If the SSIA CA's applications cannot automatically record an event, the SSIA CA shall implement manual procedures to satisfy the requirements. For each event, the SSIA CA shall record the relevant:

a) date and time;

b) type of event;

c) success or failure; and

d) user or system that caused the event or initiated the action.

All event records shall be made available to auditors as proof of the SSIA CA's and/or RAs' practices.

Auditable Event
SECURITY AUDIT
Any changes to the audit parameters, e.g., audit frequency, type of event audited
Any attempt to delete or modify the audit logs
AUTHENTICATION TO SYSTEMS
Successful and unsuccessful attempts to assume a role
The value of maximum number of authentication attempts is changed
Maximum number of authentication attempts occur during user login
An administrator unlocks an account that has been locked as a result of unsuccessful authentication attempts
An administrator changes the type of authenticator, e.g., from a password to a biometric
LOCAL DATA ENTRY
All security-relevant data that is entered in the system
REMOTE DATA ENTRY
All security-relevant messages that are received by the system
DATA EXPORT AND OUTPUT
All successful and unsuccessful requests for confidential and security-relevant information
KEY GENERATION
Whenever a CA generates a key (not mandatory for single session or one-time use symmetric keys)
PRIVATE KEY LOAD AND STORAGE
The loading of Component Private Keys
All access to certificate subject Private Keys retained within the CA for key recovery purposes
TRUSTED PUBLIC KEY ENTRY, DELETION AND STORAGE
SECRET KEY STORAGE
The manual entry of secret keys used for authentication
PRIVATE AND SECRET KEY EXPORT
The export of private and secret keys (keys used for a single session or message are excluded)
CERTIFICATE REGISTRATION
All certificate applications, including issuance, re-key, renewal, and revocation
Certificate issuance
Verification activities
CERTIFICATE REVOCATION
All certificate revocation requests
CERTIFICATE STATUS CHANGE APPROVAL OR REJECTION
CA CONFIGURATION
Any security-relevant changes to the configuration of a CA system component
ACCOUNT ADMINISTRATION
Roles and users are added or deleted
The access control privileges of a user account or a role are modified

Auditable Event
CERTIFICATE PROFILE MANAGEMENT
All changes to the certificate profile
REVOCATION PROFILE MANAGEMENT
All changes to the revocation profile
CERTIFICATE REVOCATION LIST PROFILE MANAGEMENT
All changes to the certificate revocation list profile
Generation of CRLs entries
TIME STAMPING
Clock synchronization
MISCELLANEOUS
Appointment of an individual to a Trusted Role
Designation of personnel for multiparty control
Installation of an Operating System
Installation of a PKI Application
System Start-up
Logon attempts to PKI Application
Receipt of hardware / software
Attempts to set passwords
Attempts to modify passwords
Back-up of the internal CA database
Restoration from back-up of the internal CA database
File manipulation (e.g., creation, renaming, moving)
Posting of any material to a repository
Access to the internal CA database
All certificate compromise notification requests
CONFIGURATION CHANGES
Hardware
Software
Operating System
Patches
Security Profiles
PHYSICAL ACCESS / SITE SECURITY
Personnel access to secure area housing CA components
Access to a CA component
Known or suspected violations of physical security
Firewall and router activities
ANOMALIES

Auditable Event
System crashes and hardware failures
Software error conditions
Software check integrity failures
Receipt of improper messages and misrouted messages
Network attacks (suspected or confirmed)
Equipment failure
Electrical power outages
Uninterruptible Power Supply (UPS) failure
Obvious and significant network service or access failures
Violations of a CP or CPS
Resetting Operating System clock

5.4.2. Frequency of Processing Log

The SSIA CA and RAs shall, at least every two months, review system logs, make system and file integrity checks, and make a vulnerability assessment. The SSIA CA and RAs may use automated tools to scan for anomalies or specific conditions. During their review, the SSIA CA and RAs shall verify that the logs have not been tampered with, examine any statistically significant set of security audit data generated since the last review, and make a reasonable search for any evidence of malicious activity.

The SSIA CA and RAs shall briefly inspect all log entries and more thoroughly investigate any anomalies or irregularities detected. The SSIA CA and RAs shall make a summary of each review available to its auditors upon request. The SSIA CA and RAs shall document any actions taken as a result of a review.

5.4.3. Retention Period for Audit Log

The SSIA CA and RA shall retain audit logs on-site until after they are reviewed. The individual who removes audit logs from the SSIA CA's or RA's systems must be different than the individuals who control the SSIA CA's signature keys.

Audit logs shall be retained for a minimum period of at least ten (10) years unless a greater retention is required by any other applicable law, standard, policy, etc.

5.4.4. Protection of Audit Log

The SSIA CA and RA shall implement procedures that protect archived data from destruction prior to the end of the audit log retention period. The SSIA CA and RA shall configure its systems and establish operational procedures to ensure that:

a) only authorized people have read access to logs;

b) only authorized people may archive audit logs; and

c) audit logs are not modified.

The SSIA CA's and RAs' off- site storage location must be a safe and secure location that is separate from the location where the data was generated.

The SSIA CA and RAs shall make records available if required for the purpose of providing evidence of the correct operation of time-stamping services for the purpose of legal proceedings. Audit logs are made available to auditors upon request.

5.4.5. Audit Log Back-up Procedures

On at least a monthly basis, the SSIA CA and RAs shall make back-ups of audit logs and audit log summaries and store a copy of the audit log off-site.

5.4.6. Audit Collection System (internal vs. external)

The SSIA CA and RAs may use automatic audit processes, provided that they are invoked at system start-up and end only at system shut-down. If an automated audit system fails and the integrity of the system or confidentiality of the information protected by the system is at risk, the SSIA CA or RA shall consider suspending its operations until the problem is remedied.

5.4.7. Notification to Event-causing Subject

No stipulation.

5.4.8. Vulnerability Assessments

The SSIA CA shall perform routine risk (once a year) assessments that identify and assess reasonably foreseeable internal and external threats that could result in unauthorized access, disclosure, misuse, alteration, or destruction of any certificate data or certificate issuance process.

Based on such Risk Assessments, the CA shall develop, implement, and maintain a Security Plan consisting of security procedures and controls designed to achieve the objectives set forth above and to reasonably manage and control the risks identified during the Risk Assessment, commensurate with the sensitivity of the information held, the complexity and scope of the activities of the CA, the cost of implementing the specific measures and the harm that might result from a breach of security. The Security Plan shall include administrative, organizational, technical, and physical safeguards appropriate to the size, complexity, nature, and scope of the CA's business. The Security Plan shall be updated once a year.

The SSIA CA shall also routinely assess the sufficiency of the policies, procedures, information systems, technology, and other arrangements that the SSIA CA and RAs have in place to control such risks. The SSIA CA's auditors should review the security audit data checks for continuity and alert the appropriate personnel of any events, such as repeated failed actions, requests for privileged information, attempted access of system files, and unauthenticated responses.

5.5. Records Archival

The SSIA CA shall comply with any record retention policies that apply by law. The SSIA CA shall include sufficient detail in archived records to show that a certificate was issued in accordance with the CPS.

5.5.1. Types of Records Archived

The SSIA CA shall retain the following information in its archives (as such information pertains to the SSIA CA's CA operations):

a) Any amendment of the SSIA CA, CP and CPS versions;

b) Contractual obligations and other agreements concerning the operation of the CA;

c) System and equipment configurations, modifications; and updates;

d) Certificate and revocation requests;

e) Identity authentication data;

f) Any documentation related to the receipt or acceptance of a certificate or token;

g) Subscriber Agreements;

h) Issued certificates;

i) A record of certificate re-keys; CRLs;

j) Any data or applications necessary to verify an archive's contents;

k) Compliance auditor reports;

l) Any changes to the SSIA CA's audit parameters;

m) Any attempt to delete or modify audit logs;

n) Key generation;

o) Access to Private Keys for key recovery purposes;

p) Changes to trusted Public Keys;

q) Export of Private Keys;

r) Approval or rejection of a certificate status change request;

s) Appointment of an individual to a Trusted Role;

t) Destruction of a cryptographic module;

u) Certificate compromise notifications;

v) Remedial action taken as a result of violations of physical security; and

w) Violations of the CP or CPS.

5.5.2. Retention Period for Archive

The SSIA CA shall retain archived data for at least three (3) years unless a greater retention is required by any other applicable law, standard, policy, etc.

5.5.3. Protection of Archive

The SSIA CA shall store its archived records at a secure off-site location in a manner that prevents unauthorized modification, substitution, or destruction. No unauthorized user may access, write, or delete the archives. The SSIA CA shall not release archives except as requested by the SSIA or as required by law. If the original media cannot retain the data for the required period, the archive site must define a mechanism to periodically transfer the archived data to new media. The SSIA CA shall maintain any software application and a suitable software/hardware host system required to process the archive data until the data is either expired or then destroyed, or it is transferred to a newer medium.

5.5.4. Archive Back-up Procedures

The SSIA CA shall describe how its records are backed up and managed in its CPS or a document referenced therefrom.

5.5.5. Requirements for Time-stamping of Records

The SSIA CA shall automatically time-stamp archive records as they are created, using a time-signal per §6.8. Cryptographic time-stamping of archive records is not required.

5.5.6. Archive Collection System (internal or external)

The SSIA CA shall collect archive information internally.

5.5.7. Procedures to Obtain and Verify Archive Information

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

The SSIA CA may allow Subscribers to obtain a copy of their archived information. Otherwise, the SSIA CA shall restrict access to archive data to authorized personnel in accordance with the SSIA CA's internal security policy and shall not otherwise release any archived information except as allowed by law.

5.6. Key Changeover

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

5.7. Compromise and Disaster Recovery

5.7.1. Incident and Compromise Handling Procedures

The SSIA CA shall implement data back-up and recovery procedures and shall develop a Disaster Recovery and/or Business Continuity Plan (DR/BCP). The SSIA CA'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 CA shall review, test, and update the DR/BCP and supporting procedures annually. If a disaster occurs, the SSIA CA shall re-establish operational capabilities as quickly as possible.

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

The SSIA CA shall make regular back-up copies of its Private Keys and store them in a secure off-site location. The SSIA CA shall also make system back-ups on a daily basis. If a disaster causes the SSIA CA's operations to become inoperative, the SSIA CA shall, after ensuring the integrity of the CA systems, re-initiate its operations on replacement hardware located at a secure facility, using back-up copies of its software, data, and Private Keys. The SSIA CA shall give priority to re-establishing the generation of certificate status information. If the Private Keys are destroyed, the SSIA CA shall re-establish operations as quickly as possible, giving priority to generating new key pairs.

5.7.3. Entity Private Key Compromise Procedures

If the SSIA CA suspects that a CA Private Key is comprised or lost then the SSIA CA shall follow its Incident Response Plan and immediately assess the situation, determine the degree and scope of the incident, and take appropriate action. SSIA CA 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.

If there is a compromise or loss, the SSIA CA shall notify any affiliated entities so that they may issue CRLs revoking cross-certificates issued to the SSIA CA and shall notify interested parties and make information available that can be used to identify which certificates and time-stamp tokens affected, unless doing so would breach the privacy of the Issuer CA's user or the security of the SSIA CA's services.

Following revocation of the SSIA CA's certificate and implementation of the SSIA CA's Incident Response Plan, the SSIA CA will generate a new CA Key Pair and sign a new CA certificate in accordance with its CPS. The SSIA CA shall distribute the new self-signed certificate in accordance with Section 6.1.4. The SSIA CA 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

The SSIA CA shall establish a secure facility in at least one secondary location, to ensure that its directory and on-line status servers, if any, remain operational in the event of a physical disaster at the SSIA CA's main site. The SSIA CA shall provide notice at the earliest feasible time to all interested parties if a disaster physically damages the SSIA CA's equipment or destroys all copies of the SSIA CA's signature keys.

5.8. CA or RA Termination

If the SSIA CA's operations are ever terminated, the SSIA CA shall provide notice to interested parties and shall transfer its responsibilities and records to successor entities. The SSIA CA may allow a successor to re-issue certificates if the successor has all relevant permissions to do so and has operations that are at least as secure the SSIA CA's. If no successor CA exists, all relevant records of the SSIA CA shall be transferred to a government regulatory or legal body.

6. TECHNICAL SECURITY CONTROLS

6.1. Key Pair Generation and Installation

6.1.1. Key Pair Generation

All keys must be generated using a FIPS-approved method or equivalent international standard.

The SSIA CA shall generate cryptographic keying material on a FIPS 140-2 level 3 validated cryptographic module using multiple individuals acting in Trusted Roles. When generating keying material, the SSIA CA shall create auditable evidence to show that the SSIA CA enforced role separation and followed its key generation process. The SSIA CA shall

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

6.1.2. Private Key Delivery to Subscriber

If the SSIA CA, a CMS, or a RA generates keys on behalf of the Subscriber, then the entity generating the key shall deliver the Private Key securely to the Subscriber. The entity may deliver Private Keys to Subscribers electronically or on a hardware cryptographic module / SSCD. In all cases:

a) The key generator may not retain a copy of the Subscriber's Private Key after delivery;

b) The key generator shall protect the private key from activation, compromise, or modification during the delivery process;

c) The Subscriber shall acknowledge receipt of the private key(s); and

d) The key generator shall deliver the Private Key in a way that ensures that the correct tokens and activation data are provided to the correct Subscribers, including:

e) For hardware modules, the key generator maintaining accountability for the location and state of the module until the Subscriber accepts possession of it; and,

f) For electronic delivery of private keys, the key generator encrypting key material using a cryptographic algorithm and key size at least as strong as the private key. The key generator shall deliver activation data using a separate secure channel.

The entity assisting with Subscriber key generation shall maintain a record of the Subscriber's acknowledgement of receipt of the device containing the Subscriber's Key Pair. A CMS or RA providing key delivery services shall provide a copy of this record to the SSIA CA.

6.1.3. Public Key Delivery to Certificate Issuer

Subscribers shall deliver their Public Keys to the SSIA CA in a secure fashion and in a manner that binds the Subscriber's verified identity to the Public Key. The certificate application process shall ensure that the Applicant possesses the Private Key associated with the Public Key presented for certification. If cryptography is used to achieve the binding, the cryptography must be at least as strong as the CA keys used to sign the Certificate.

6.1.4. CA Public Key Delivery to Relying Parties

The SSIA CA shall provide its public keys to Relying Parties in a secure fashion and in a manner that precludes substitution attacks. The SSIA CA may deliver its CA Public Keys to Relying Parties as:

a) specified in a certificate validation or path discovery policy file;

b) trust anchors in commercial browsers and operating system root store; and/or

c) roots signed by other CAs

The SSIA CA may distribute Public Keys that are part of an updated signature key pair as a self-signed certificate, as a new CA certificate, or in a key roll-over certificate.

6.1.5. Key Sizes

The SSIA CA shall follow the NIST timelines in using and retiring signature algorithms and key sizes. The SSIA CA shall generate and use the following keys, signature algorithms, and hash algorithms for signing certificates, CRLs, and certificate status server responses:

a) 2048-bit RSA Key with Secure Hash Algorithm version 2 (SHA-256);

b) 2048-bit RSA Key with Secure Hash Algorithm version 2 (SHA-512).

The SSIA CA may issue Subject certificates that contain the following:

c) For certificates that expire on or after 2013-12-31 and that include a `keyUsage` extension that only asserts the `digitalSignature` bit, at least 2048 bits for RSA or DSA, or 224 bits for elliptic curve algorithms;

d) For certificates expiring after 2010-12-31, at least 2048 bits for RSA, DSA, or Diffie-Hellman, or 224 bits for elliptic curve algorithms.

The SSIA CA may require higher bit keys in its sole discretion.

Any certificates (whether CA or Subject) expiring after 2030-12-31 must be at least 3072 bit for RSA and 256 bit for ECDSA. Signatures on certificates and CRLs that are issued after 2010-12-31 shall be generated using, at a minimum, SHA-224. Signatures on certificates and CRLs that are issued after 2030-12-31 shall be generated using, at a minimum, SHA-256.

The SSIA CA and Subscribers may fulfil their requirements under the CP and CPS using TLS or another protocol that provides similar security, provided the protocol requires at least:

a) AES (128 bits) or equivalent for the symmetric key and at least 2048 bit RSA or equivalent for the asymmetric keys after 2010-12-31; and

b) AES (128 bits) or equivalent for the symmetric key, and at least 3072 bit RSA or equivalent for the asymmetric keys after 2030-12-31.

6.1.6. Public Key Parameters Generation and Quality Checking

The SSIA CA shall generate Public Key parameters for signature algorithms and perform parameter quality checking in accordance with FIPS 140-2 level 3.

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

The SSIA CA shall include key usage extension fields that specify the intended use of the certificate and technically limit the certificate's functionality in X.509v3 compliant software. The SSIA CA shall set key usage bits or assert extended key usage OIDs for each certificate type in accordance with the SSIA Certificate Profiles document.

The SSIA CA shall not issue Level 3 and Level 4 certificates that are certified for both signing and encryption. Level 1 and Level 2 certificates may include a single key for use with encryption and signature in support of legacy applications. Such dual-use certificates must:

a) be generated and managed in accordance with their respective signature certificate requirements, except where otherwise noted in this CP,

b) never assert the non-repudiation key usage bit, and

c) not be used for authenticating data that will be verified on the basis of the dual-use certificate at a future time.

6.2. Private Key Protection and Cryptographic Module Engineering Controls

6.2.1. Cryptographic Module Standards and Controls

The SSIA CA shall use cryptographic modules validated to FIPS 140-2 level 3 (Hardware or Software) or equivalent. Subjects which generate their own keys shall use cryptographic modules validated to FIPS 140-2 level 3 (Hardware or Software) or equivalent.

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

The SSIA CA shall ensure that multiple trusted personnel are required to act in order to access and use the SSIA CA's Private Keys, including any Private Key back-ups.

6.2.3. Private Key Escrow

The SSIA CA shall not escrow its signature keys. Subscribers may not escrow their private signature keys or dual-use keys. The SSIA CA may escrow Subscriber Private Keys used for encryption.

6.2.4. Private Key Back-up

The SSIA CA shall back-up its CA, CRL, and certificate status Private Keys under multi-person control and shall store at least one back-up off site. The SSIA CA shall protect all copies of its CA, CRL, and certificate status Private Keys in the same manner as the originals.

The SSIA CA may back-up (1) Level 1, Level 2, and Level 3 subscriber private signature keys, provided that the back-up copies are held under the Subscriber's control, and (2) Subscriber key management keys. Backed-up keys are never stored in plain text form outside of the cryptographic module. Storage that contains back-up keys shall provide security controls that are consistent with the protection provided by the Subscriber's cryptographic module.

6.2.5. Private Key Archival

The SSIA CA shall not archive Private Keys.

6.2.6. Private Key Transfer into or from a Cryptographic Module

All keys must be generated by and in a cryptographic module. The SSIA CA and RA shall never allow their Private Keys to exist in plain text outside of the cryptographic module. The SSIA CA shall only export its Private Keys from the cryptographic module to perform CA key back-up procedures. When transported between cryptographic modules, the SSIA CA shall encrypt the private key and protect the keys used for encryption from disclosure.

6.2.7. Private Key Storage on Cryptographic Module

The SSIA CA shall store its CA Private Keys on a cryptographic module which has been evaluated to at least FIPS 140-2 level 3 and EAL 4+.

6.2.8. Method of Activating Private Key

The SSIA CA shall activate its Private Keys in accordance with the specifications of the cryptographic module manufacturer. Subscribers are solely responsible for protecting their Private Keys. At a minimum, Subscribers must authenticate themselves to the cryptographic module before activating their private keys. Entry of activation data shall be protected from disclosure.

6.2.9. Method of Deactivating Private Key

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

6.2.10. Method of Destroying Private Key

The SSIA CA shall use individuals in Trusted Roles to destroy CA, RA, and Status Server Private Keys when they are no longer needed. Subscribers shall destroy their Private Keys when the corresponding certificate is revoked or expired or if the Private Key is no longer needed

For software cryptographic modules, the SSIA CA may destroy the Private Keys by overwriting the data.

For hardware cryptographic modules, the SSIA CA may destroy the Private Keys by executing a "zeroize" command. Physical destruction of hardware is not required.

6.2.11. Cryptographic Module Rating

See §6.2.1.

6.3. Other Aspects of Key Pair Management

6.3.1. Public Key Archival

The SSIA CA shall archive a copy of each Public Key.

6.3.2. Certificate operational periods and key pair usage periods

The SSIA CA certificates, including renewed certificates, have maximum validity periods of:

Type	Private Key Use	Certificate Term
Root CA	20 years	25 years
Sub CA	12 years	15 years
SSL (HWCA)	No stipulation	825 days
Subscriber Certificate (SignCA)	5 years	5 years

Relying Parties may still validate signatures generated with these keys after expiration of the certificate.

The SSIA CA may retire its CA Private Keys before the periods listed above to accommodate key changeover processes. The SSIA CA shall not issue a Subscriber certificate with an expiration date that is past the signing root's expiration date or that exceeds the routine re-key identification requirements specified in §3.1.1.

6.4. Activation Data

6.4.1. Activation Data Generation and Installation

The SSIA CA shall generate activation data that has sufficient strength to protect its Private Keys. If the SSIA CA uses passwords as activation data for a signing key, the SSIA CA shall change the activation data upon rekey of the CA certificate. The SSIA CA may only transmit activation data via an appropriately protected channel and at a time and place that is distinct the associated cryptographic module.

6.4.2. Activation Data Protection

The SSIA CA shall protect data used to unlock private keys from disclosure using a combination of cryptographic and physical access control mechanisms. Activation data shall be:

a) memorized;

b) biometric in nature; or

c) recorded and secured at the level of assurance associated with the activation of the cryptographic module, and shall not be stored with the cryptographic module.

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

6.4.3. Other Aspects of Activation Data

No stipulation.

6.5. Computer Security Controls

6.5.1. Specific Computer Security Technical Requirements

The SSIA CA shall configure its systems, including any remote workstations, to:

a) authenticate the identity of users before permitting access to the system or applications;

b) manage privileges of users to limit users to their assigned roles;

c) generate and archive audit records for all transactions;

d) enforce domain integrity boundaries for security critical processes; and

e) support recovery from key or system failure.

The SSIA CA shall authenticate and protect all communications between a Trusted Role and its CA system. All Certificate Status Servers must:

f) authenticate the identity of users before permitting access to the system or applications;

g) manage privileges to limit users to their assigned roles;

h) enforce domain integrity boundaries for security critical processes; and

i) support recovery from key or system failure.

A CMS must be able to execute the following computer security functions:

j) authenticate the identity of users before permitting access to the system or applications,

k) manage privileges of users to limit users to their assigned roles,

l) generate and archive audit records for all transactions, (see Section 5.4)

m) enforce domain integrity boundaries for security critical processes, and

n) support recovery from key or system failure.

6.5.2. Computer Security Rating

No stipulation.

6.6. Life Cycle Technical Controls

6.6.1. System Development Controls

In operating its CA, the SSIA CA shall use only:

a) Commercial off-the-shelf software that was designed and developed under a formal and documented development methodology,

b) Hardware and software developed specifically for the SSIA CA by verified personnel, using structured development approach and a controlled development environment,

c) Open source software that meets security requirements through software verification & validation and structured development/life-cycle management,

d) Hardware and software purchased and shipped in a fashion that reduces the likelihood of tampering, and

e) For CA operations, hardware and software that is dedicated only to performing the CA functions.

The SSIA CA shall take proper care to prevent malicious software from being loaded onto the CA equipment. Hardware and software must be scanned for malicious code on first use and periodically thereafter. The SSIA CA shall purchase or develop updates in the same manner as original equipment, and shall use trusted trained personnel to install the software and equipment. The SSIA CA shall not install any software on its CA systems that are not part of the CA's operations.

The SSIA CA shall use a formal configuration management methodology for installation and on-going maintenance of any CMS. Any modifications and upgrades to a CMS shall be documented and controlled. The SSIA CA shall implement a mechanism for detecting unauthorized modification to a CMS.

6.6.2. Security Management Controls

The SSIA CA shall establish formal mechanisms to document, control, monitor, and maintain the installation and configuration of its CA systems, including any modifications or upgrades. The Issuer CA's change control processes shall include procedures to detect unauthorized modification to the SSIA CA's systems and data entries that are processed, logged and tracked for any security-related changes to CA systems, firewalls, routers, software and other access controls. When loading software onto a CA system, the SSIA CA shall verify that the software is the correct version and is supplied by the vendor free of any modifications. The SSIA CA shall verify the integrity of software used with its CA processes at least once a week.

6.6.3. Life Cycle Security Controls

No stipulation.

6.7. Network Security Controls

The SSIA CA shall document and control the configurations of its systems, including any upgrades or modifications made. The SSIA CA shall implement a process for detecting unauthorized modifications to its hardware or software and for installing and maintaining its systems. The SSIA CA shall verify all software, when first loaded, as the unmodified software.

The SSIA CA and its RAs shall implement appropriate network security controls, including turning off any unused network ports and services and only using network software that is necessary for the proper functioning of the CA systems. The SSIA CA shall implement the same network security controls to protect a CMS as used to protect its other CA equipment.

6.8. Time-stamping

SSIA CA shall ensure that the accuracy of clocks used for time-stamping are within three minutes.
Electronic of manual procedures may be used to maintain system time. Clock adjustments are auditable events.

7. CERTIFICATE, CRL, AND OCSP PROFILES

7.1. Certificate Profile

7.1.1. Version Number

The SSIA CA shall issue X.509 version 3 certificates.

7.1.2. Certificate Extensions

The SSIA CA shall use certificate extensions in accordance with applicable industry standards, including RFC 3280/5280.
The SSIA CA shall not issue certificates with a critical private extension.

7.1.3. Algorithm Object Identifiers

The SSIA CA shall sign certificates using one of the following algorithms:

SHA1WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi (113549) pkcs(1) pkcs-1(1) 5}
SHA256WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi (113549) pkcs(1) pkcs-1(1) 11}
ecdsa-with-SHA1	{iso(1) member-body(2) us(840) ansi-x962(10045) signatures(4) ecdsa-with-SHA1(1)}
ecdsa-with-SHA256	{ iso(1) member-body(2) us(840) ansi-X9-62 (10045) signatures(4) ecdsa-with-SHA2 (3) 2 }

If the SSIA CA signs certificates using RSA with PSS padding, the SSIA CA may use a RSA signature with PSS padding with the following algorithms and OIDs:

id-sha256	{ joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101) csor(3) nistalgorithm(4) hashalgs(2) 1 }
id-sha512	{ joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101) csor(3) nistalgorithm(4) hashalgs(2) 3 }

The SSIA CA and Subscribers may generate Key Pairs using the following:

id-dsa	{iso(1) member-body(2) us(840) x9-57(10040) x9cm(4) 1}
RsaEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 1}
Dhpublicnumber	{iso(1) member-body(2) us(840) ansi-x942(10046) number-type(2) 1}
id-ecPublicKey	{ iso(1) member-body(2) us(840) ansi-X9-62(10045) id-publicKeyType(2) 1 }
id-keyExchangeAlgorithm	{ joint-iso-ccitt(2) country(16) us(840) organization(1) gov(101) dod(2) infosec(1) algorithms(1) 22 }

7.1.4. Name Forms

The SSIA CA shall use distinguished names that are composed of standard attribute types, such as those identified in RFC 3280/5280. The SSIA CA shall include a unique serial number in each certificate.

7.1.5. Name Constraints

The SSIA CA may include name constraints in the `nameConstraints` field when appropriate.

7.1.6. Certificate Policy Object Identifier

An object identifier (OID) is a unique number that identifies an object or policy. The SSIA CA shall use the OIDs listed in §1.2 to identify its certificates and policies in the `certificatePolicies` extension.

7.1.7. Usage of Policy Constraints Extension

Not applicable.

7.1.8. Policy Qualifiers Syntax and Semantics

The SSIA CA may include brief statements in the Policy Qualifier field of the `certificatePolicies` extension.

7.1.9. Processing Semantics for the Critical Certificate Policies Extension

No stipulation.

7.2. CRL Profile

7.2.1. Version number(s)

The SSIA CA shall issue version 2 CRLs that conform to [RFC3280/5280].

7.2.2. CRL and CRL Entry Extensions

The SSIA CA CRL extensions shall conform to the Federal PKI X.509 CRL Extensions Profile.

7.3. OCSP PROFILE

The SSIA CA shall operate an OCSP service in accordance with [RFC2560].

7.3.1. Version Number(s)

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

7.3.2. OCSP Extensions

No stipulation.

8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS

The policies in this CP 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

On at least an annual basis, the SSIA CA shall appoint an independent (third-party) auditor who shall assess its conformity with this CP and its CPS. This audit shall cover the SSIA CA, CMSs, RAs, and each Status Server that is specified in a certificate issued by the SSIA CA.

8.2. Identity/Qualifications of Auditors

The appointed auditor shall fulfil the following criteria

a) ***Qualifications and experience:*** *Auditing must be the auditor'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 Internet security issues;

c) ***Rules and standards:*** *The auditor 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 maintain Professional Liability/Errors and Omissions Insurance, with policy limits of at least $1 million in coverage.

8.3. Assessor's Relationship to Assessed Entity

The SSIA CA shall utilize an independent (third-party) auditor that has no financial interest, business relationship, or course of dealing that could foreseeably create a significant bias for or against SSIA or the SSIA CA.

8.4. Topics covered by Assessment

The audit must conform to industry standards, cover the SSIA CA's compliance with its business practices disclosure, and evaluate the integrity of the SSIA CA's PKI operations, commencing from the Root Key generation and signing ceremony.

8.5. Actions taken as a result of Deficiency

If an audit reports any material non-conformity with applicable law, this CP, the CPS, or any other contractual obligations related to the SSIA CA's services, then

a) the auditor shall document the non-conformity;

b) the auditor shall promptly notify the SSIA CA and the SSIA IMA of the non-conformity, and;

c) the SSIA CA and the SSIA IMA shall develop a plan to remedy the non-conformity.

The SSIA CA shall submit the remedial plan to the SSIA IMA for approval and to any third party that the SSIA CA is legally obligated to satisfy. The SSIA IMA may require additional action if necessary to rectify any significant issues created by the non-conformity, including requiring revocation of affected certificates.

8.6. Communication of Results

The results of each audit shall be reported to the SSIA IMA for review and approval. The results shall also be communicated to any third party entities entitled by law, regulation, or agreement to receive a copy of the audit results.

8.7. Self-Audits

The SSIA CA shall conduct at planned intervals internal (first-party) quality audits against a randomly-selected sample of certificates issued, encompassing a minimum of 3% of the issuances since the last internal audit for HW CA.

9. OTHER BUSINESS AND LEGAL MATTERS

9.1. Fees

The SSIA CA shall levy Subscriber Agencies an annual charge for each Agency, depending how many employees they have.

9.1.1. Certificate issuance or renewal fees

No extra fee for Subscriber Agencies.

9.1.2. Certificate access fees

No extra fee for Subscriber Agencies.

9.1.3. Revocation or status information access fees

No extra fee for Subscriber Agencies.

9.1.4. Fees for other services

No extra fee for Subscriber Agencies.

9.1.5. Refund policy

Refund is not applicable.

9.2. Financial Responsibility

9.2.1. Insurance Coverage

The SSIA CA shall maintain sufficient insurances in respect of its performance under this CP through Kammarkollegiet (The Legal, Financial and Administrative Services Agency) in accordance with ordinance on governmental agencies´ risk management (förordningen (1995:1300) om statliga myndigheters riskhantering).

9.2.2. Other Assets

No stipulation.

9.2.3. Insurance or Warranty Coverage for End-Entities

No stipulation.

9.3. Confidentiality of Business Information

9.3.1. Scope of Confidential Information

Issuer CAs shall specify what constitutes confidential information in its CPS.

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.

9.3.3. Responsibility to Protect Confidential Information

The SSIA CA's employees, agents, and contractors are responsible for protecting confidential information in accordance with the Public Access to Information Act (2009:400).

9.4. Privacy of Personal Information

9.4.1. Privacy plan

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 CA shall securely store and protect sensitive against accidental disclosure.

9.4.2. Information Treated as Private

The SSIA CA treats all personal information about an individual that is not publicly available in the contents of a certificate or CRL as private information.

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.

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 CA shall not knowingly violate the intellectual property rights of any third party. The SSIA CA 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

The SSIA CA represents that it complies, in all material aspects, with this CP, the CPS, its internal and published policies and procedures, and all applicable laws and regulations. The SSIA CA expressly disclaims all other representations except as otherwise stated in the CPS or in any separate agreements.

9.6.2. RA Representations and Warranties

At a minimum, the SSIA CA shall require all Agencies (in their role as RAs) to represent that they have followed this CP and the CPS when participating in the issuance and management of certificates. The SSIA CA may include additional representations and obligations in its CPS or in its agreement with the RA.

9.6.3. Subscriber Representations and Warranties

The SSIA CA shall, through the [IAA], make Subscribers solely responsible for any misrepresentations they make to third parties and for all transactions that use Subscriber's Private Key, regardless of whether such use was authorized. Prior to being issued a certificate, Subscribers shall contractually agree to:

a) Securely protect their Private Keys from compromise;

b) Provide accurate and complete information and communication to the SSIA CA at all times;

c) Confirm the accuracy of certificate data prior to using the certificate;

d) Promptly cease using a certificate and notify the SSIA CA if:

   i) any information that was submitted to the SSIA CA or is included in a certificate changes or becomes misleading or;

   ii) there is any actual or suspected misuse or compromise of the Private Key associated with the certificate;

e) Use the certificate only for authorized and legal purposes, consistent with this CPS and the [IAA], including only installing SSL certificates on servers accessible at the domain listed in the certificate;

f) Abide by the [IAA] and the CPS when requesting or using a Certificate; and

g) Promptly cease using the certificate and related Private Key after the certificate's expiration.

9.6.4. Relying Party Representations and Warranties

Relying Parties must follow the procedures and make the representations provided for herein and in the applicable Relying Party Agreement prior to relying on or using a certificate.

9.6.5. Representations and Warranties of Other Participants

No stipulation.

9.7. Disclaimers of Warranties

Except as expressly stated otherwise herein or as limited by law, SSIA disclaims all warranties and obligations related to this CP. A fiduciary duty is not created simply because an entity uses services offered within the SSIA PKI.

9.8. Limitations of Liability

SSIA CA may limit its liability for each certificate type as set forth in its CPS. A CPS may exclude all liability for any certificate issued and managed in accordance with this CP and the CPS or in instances where a Subscriber or Relying Party has not complied with the terms and conditions of use for the Certificate.

9.9. Indemnities

9.9.1. Indemnification by an Issuer CA

The SSIA CA's indemnification obligations are set forth in [IAA].

9.9.2. Indemnification by Subscribers

The SSIA CA shall include its indemnification requirements for Subscribers in the CPS and in [IAA].

9.9.3. Indemnification by Relying Parties

The SSIA CA shall include its indemnification requirements for Relying Parties in [IAA].

9.10. Term and Termination

9.10.1. Term

This CP and any amendments are effective when published to SSIA's online repository and remain in effect until deleted or replaced with a newer version.

9.10.2. Termination

This CP 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.

9.10.3. Effect of Termination and Survival

SSIA will communicate the conditions and effect of this CP's termination via the SSIA Repository. The communication will specify which provisions survive termination. At a minimum, responsibilities related to protecting confidential information will survive termination.

9.11. Individual Notices and Communications with Participants

SSIA accepts digitally signed or paper notices related to this CP that are addressed to the locations specified in Section 2.2 of this CP. Notices are deemed effective after the sender receives a valid, digitally signed acknowledgment of receipt from SSIA. If an acknowledgement of receipt is not received within five days, the sender must resend the notice in paper form to the street address specified in Section 2.2 using either a courier service that confirms delivery or via certified or registered mail with postage prepaid and return receipt requested.

9.12. Amendments

9.12.1. Procedure for Amendment

The SSIA IMA determines what amendments should be made to this CP or the CPS. Amendments are made by posting an updated version of the CP or CPS to the online repository. Controls are in place to reasonably ensure that this CP and the CPS is not amended and published without the prior authorization of the SSIA IMA. The SSIA IMA reviews this CP and the CPS annually.

9.12.2. Notification Mechanism and Period

The SSIA CA will post notice on its website of any proposed significant revisions to this CP. The notice will include a final date for receipt of comments and the proposed effective date. The Issuer CA does not have a fixed notice and comment period. The SSIA CA may make editorial and typographical corrections, changes to contact details, and other changes that do not materially impact the parties without notice and without changing the version of this CP.

9.12.3. Circumstances under which OID Must Be Changed

If the SSIA IMA determines an amendment necessitates a change in an OID, then the revised version of this CP will also contain a revised OID. Otherwise, amendments do not require an OID change.

9.13. Dispute Resolution Provisions

Before resorting to any dispute resolution mechanism, including adjudication or any type of alternative dispute resolution, a party must notify SSIA of the dispute with a view to seek dispute resolution.

9.14. Governing Law

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

9.15. Compliance with Applicable Law

This CP is subject to all laws and regulations within the jurisdiction within which the SSIA CA operates.

Subject to §9.4.5's Notice and Consent to Use Private Information contained in Certificates, each SSIA CA shall meet the requirements of European Data Protection Directive 95/46/EC and shall establish and maintain appropriate technical and organizational measures against unauthorized or unlawful processing of personal data and against the loss, damage, or destruction of personal data.

9.16. Miscellaneous Provisions

9.16.1. Entire Agreement

The SSIA CA shall, through the [IAA], contractually obligate every RA involved in Certificate issuance to comply with this CP and applicable industry Guidelines. The SSIA CA will also require parties using its products and services, such as Subscribers and Relying Parties, to accept agreements. No third party may rely on or bring action to enforce any such agreement.

9.16.2. Assignment

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

9.16.3. Severability

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

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

SSIA may seek indemnification and attorneys' fees from any party for damages, losses, and expenses related to that party's conduct. SSIA's failure to enforce a provision of this CP does not waive SSIA's right to enforce the same provision later or right to enforce any other provision of this CP. To be effective, waivers must be in writing and signed by SSIA.

9.16.5. Force Majeure

SSIA is not liable for a delay or failure to perform an obligation under this CP to the extent that the delay or failure is caused by an occurrence beyond SSIA's reasonable control. The operation of the Internet is beyond SSIA's reasonable control.

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 Inter-Agency Agreement [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 Applications 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 CP 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 CP.

Acknowledgement of [IAA] shall be required by reference from each Certificate Application, 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.

No further stipulations beyond §9.17.1.