Swedish Police Authority
IT Department

POLISMYNDIGHETEN

National Certificate Policy (CP)

Swedish Country Signing CA

2021-11-19

This document describes the policy for issuing and managing public key certificates at the Swedish Country Signing CA.

Author	Swedish Police Authority		
Publication date	01.12.2021		
Version	2.0		
Status	In Process	Under Review	Authorised for Use
	☐	☐	☒

Authorisation

Place and date:	**Stockholm, 19.11.2021**
Approved by:	**Swedish Police Authority**
Approval number:	**UTS-240/2021**

Version History			
Date	Version	Author	Remarks
01.10.2021	2.0	Swedish Police Authority	Initial Release of version 2
19.11.2021	2.0	Swedish Police Authority	Approved

Definitions and Acronyms 8
1 Introduction 10
1.1 Overview 10
1.1.1 Purpose of this Document 10
1.1.2 Certificate Policy 11
1.1.3 CP vs CPS 11
1.1.4 Relationship with other PKI systems 11
1.2 Document name and identification 11
1.3 PKI participants 11
1.3.1 Certification Authority (CA) 12
1.3.2 Registration Authority (RA) 12
1.3.3 Subscriber 12
1.3.4 Relying Party 13
1.4 Certificate Usage 13
1.4.1 Acceptable uses 13
1.4.2 Prohibited uses 13
1.5 Policy administration 13
1.5.1 Organisation Administering the Document 13
1.5.2 Contact Person 13
2 Publication and repository responsibilities 14
2.1 Repositories 14
2.2 Publication of Certification Information 14
2.3 Time or Frequency of Publication 14
2.4 Access Controls on Repositories 14
3 Identification and Authentication 15
3.1 Naming 15
3.1.1 Type of Names 15
3.1.2 Need for names to be meaningful 15
3.1.3 Anonymity or Pseudonymity of Subscribers 15

3.1.4 Rules for interpreting various name forms 15
3.1.5 Uniqueness of Names 15
3.2 Initial identity validation 16
3.2.1 Method to prove possession of private keys 16
3.3 Identification and Authentication for Re-key request 16
3.3.1 Identification and Authentication for routine re-key 16
3.3.2 Identification and Authentication for Re-key after revocation 16
3.4 Identification and Authentication for Revocation Requests 16
4 Certificate Life Cycle Operational Requirements 17
4.1 Certificate Application 17
4.1.1 Submission of Certificate Application 17
4.1.2 Enrolment Process and Reponsibilities 17
4.2 Certificate Application Processing 17
4.2.1 Performing Identification and Authentication Functions 17
4.2.2 Approval or Rejection of Certificate Applications 17
4.2.3 Time to Process Certificate Applications 17
4.3 Certificate Issuance 17
4.3.1 CA Actions During Certificate Issuance 18
4.3.2 Notification to Subscriber by the CA of Issuance of Certificate 18
4.4 Certificate Acceptance 18
4.4.1 Conduct Constituting Certificate Acceptance 18
4.4.2 Publication of the Certificate by the CA 18
4.5 Key Pair and Certificate Usage 18
4.5.1 Subscriber Private Key and Certificate Usage 18
4.5.2 Relying Party Public Key and Certificate Usage 18
4.6 Certificate Re-key 19
4.6.1 Circumstance for Certificate Re-Key 19
4.6.2 Who may request a re-key 19
4.6.3 Processing Certificate re-keys 19
4.6.4 Notification of New Certificate Issuance to Subscriber 19
4.6.5 Conduct Constituting Acceptance of re-keyed Certificate 20
4.6.6 Publication of the Renewed Certificate by the CA 20
4.6.7 Notification of Certificate Issuance by the CA to other entities 20
4.7 Certificate Renewal 20
4.8 Certificate Modification 20
4.9 Certificate Revocation and Suspension. 20
4.9.1 Circumstance for revocation of a certificate 20

4.9.2 Who can request revocation of a certificate 20
4.9.3 Procedure for Revocation Request 20
4.9.4 Time within which CA MUST Process the Revocation Request 20
4.9.5 Revocation Checking Requirements for Relying Parties 21
4.9.6 CRL Issuance Frequency 21
4.9.7 Maximum Latency of CRLs 21
4.9.8 Online Revocation Checking Availability 21
4.9.9 Special Requirements Related To Key Compromise 21
4.10 End of Subscription 21
5 FACILITY MANAGEMENT & OPERATIONAL CONTROLS 22
5.1 Physical Controls 22
5.1.1 Site Location & Construction 22
5.1.2 Physical Access 22
5.1.3 Power and Air Conditioning 22
5.1.4 Water Exposure 22
5.1.5 Fire Prevention and Protection 23
5.1.6 Media Storage 23
5.1.7 Waste Disposal 23
5.1.8 Off-Site backup 23
5.2 Procedural Controls 23
5.2.1 Trusted Roles 23
5.2.2 Number of Persons Required per Task 24
5.2.3 Identity-proofing for Each Role 24
5.2.4 Separation of Roles 24
5.3 Personnel Controls 24
5.3.1 Background, Qualifications, Experience, & Security Clearance. 24
5.3.2 Background Check Procedures 25
5.3.3 Training Requirements 25
5.3.4 Retraining Frequency & Requirements 25
5.3.5 Sanctions for Unauthorised Actions 25
5.3.6 Contracting Personnel Requirements 25
5.3.7 Documentation Supplied To Personnel 25
5.4 Audit Logging Procedures 25
5.4.1 Types of Events Recorded 25
5.4.2 Frequency of Processing Data 25
5.4.3 Retention Period for Security Audit Data 26
5.4.4 Protection of Security Audit Data 26

5.4.5 Security Audit Data Backup Procedures 26
5.4.6 Security Audit Collection System 26
5.4.7 Notification to Event Causing Subject 26
5.4.8 Vulnerability Assessments 26
5.5 Records Archive 26
5.5.1 Types of Events Archived 26
5.5.2 Retention Period for Archive 26
5.5.3 Protection of Archive 26
5.5.4 Archive Backup Procedures 27
5.5.5 Requirements for Time-Stamping of Records 27
5.5.6 Archive Collection System (Internal or External) 27
5.5.7 Procedures to Obtain & Verify Archive Information 27
5.6 Key Changeover 27
5.7 Compromise & Disaster Recovery 27
5.7.1 Incident and Compromise Handling Procedures 27
5.7.2 Computing Resources, Software, and/or Data Are Corrupted 27
5.7.3 CA Private Key Compromise Recovery Procedures 27
5.7.4 Business Continuity Capabilities after a Disaster 27
6 TECHNICAL SECURITY CONTROLS 28
6.1 Key Pair Generation & Installation 28
6.1.1 Key Pair Generation 28
6.1.2 Private Key Delivery to Subscriber 28
6.1.3 Public Key Delivery to Certificate Issuer 28
6.1.4 CA Public Key Delivery to Subscribers and Relying Parties 28
6.1.5 Key Sizes 28
6.1.6 Public Key Parameters Generation and Quality Checking 28
6.1.7 Key Usage Purposes 28
6.2 Private Key Protection & Crypto Module Engineering Controls 29
6.2.1 Cryptographic Module Standards & Controls 29
6.2.2 CA Private Key Multi-Person Control 29
6.2.3 Private Key escrow 29
6.2.4 Private Key Backup 29
6.2.5 Private Key Archival 29
6.2.6 Private Key Transfer into or from a Cryptographic Module 29
6.2.7 Private Key Storage on Cryptographic Module 29
6.2.8 Method of Activating Private Keys 29
6.2.9 Methods of Deactivating Private Keys 29

6.2.10 Methods of Destroying Private Keys 30
6.2.11 Cryptographic Module Rating 30
6.3 Other Aspects of Key Management 30
6.3.1 Public Key Archive 30
6.3.2 Certificate Operational Periods and Key Usage Periods 30
6.4 Computer Security Controls 30
6.5 Life Cycle Technical Controls 30
6.5.1 System Development Controls 30
6.5.2 Security Management Controls 30
6.6 Network Security Controls 30
6.7 Time Stamping 31
7 CERTIFICATE, CRL, AND OCSP PROFILES 32
7.1 Certificate Profile 32
7.1.1 Version Number(s) 32
7.1.2 Certificate Extensions 32
7.1.3 Algorithm Object Identifiers 32
7.1.4 Name Forms 32
7.1.5 Name Constraints 32
7.1.6 Certificate Policy Object Identifier 32
7.1.7 Processing Semantics for the Critical Certificate Policies Extension 32
7.2 CRL Profile 32
7.2.1 Version Number(s) 32
7.2.2 CRL and CRL Entry Extensions 32
8 COMPLIANCE AUDIT & OTHER ASSESSMENTS 33
8.1 Frequency and Circumstances of Assessments 33
8.2 Qualifications of Assessor 33
8.3 Topics Covered by Assessment 33
8.4 Actions Taken As A Result Of Deficiency 33
8.5 Communication of Results 33
9 OTHER BUSINESS & LEGAL MATTERS 34
9.1 Fees 34
9.2 Financial Responsibility 34
9.3 Warranties 34
9.3.1 CSCA Warranties 34
9.3.2 RA Warranties 34
9.3.3 Relying Parties Warranties 34

9.3.4 Subscriber Warranties 34
9.4 Term & Termination 35
9.4.1 Term 35
9.4.2 Termination 35
9.4.3 Effect of Termination and Survival 35
9.5 Individual Notices & Communications with Participants 35
9.6 Amendments 35
9.6.1 Procedure for Amendment 35
9.6.2 Notification Mechanism and Period 35
9.6.3 Circumstances under which OID MUST be changed 36
9.7 Governing Law 36
10 References 36

Definitions and Acronyms

Although the [RFC3647] recommends all chapters and sub-chapter to be included in this CP/CPS, the Swedish Country Signing Certificate Authority (CSCA) will only address chapters and sub-chapter that apply to the CSCA. All omitted chapters and sub-chapter are implicitly declared as not applicable.

For the most important activities regarding key management (key generation, re-key, key destruction, etc.) a protocol SHALL be recorded.

The key words "MUST", "MUST NOT", "SHALL", "SHALL NOT", "SHOULD", "**SHOULD** NOT", and "MAY", are used according to [RFC 2119] and are written in capital letters.

Acronym	Definition
BCS	A Bar Code Signer is an entity that digitally signs 2D bar codes used e.g. in Visa stickers.
CA	Certification Authority is an entity that issues digital certificates.
CP	Certificate Policy is a document from a CA that aims to state: what are the different involved actors in a PKI infrastructure and what are their roles and duties.
CPS	Certificate Practice Statement is document from a CA describing the practices of issuing and managing certificates for different actors.
CSP	Certification Service Provider is the unit that operates the CA and performs services in conjunction with electronic signatures within the PKI infrastructure.
CRL	Certificate Revocation List is a list of certificates serial numbers that have been revoked, and therefore, should no longer be trusted
CSCA	Country Signing Certificate Authority is the root certification authority within the scope of the passport and citizens' registration system.
CSCA keys	Cryptographic keys belonging to a CSCA's certificate.
CSCA certificate	Certificate of the CSCA.
CSR	A Certificate Signing Request is a structured message sent from an applicant to a registration authority of a PKI system in order to apply for a digital certificate.
DN	Distinguished Name is a made up technical name for a certificate holder or certificate issuer as defined in [X.501].
DS	Document Signer is a unit authorized to sign the Document Security Objects in eMRTDs. The signing is made either by the Swedish Police Authority or on behalf of the Swedish Po-

	lice Authority by a contracted passport manufacturer.
DS keys	Cryptographic keys belonging to a Document Signer's certificate.
DS certificate	Certificate of the Document Signer.
eMRTD	Electronic Machine Readable Travel Document. This refers both to passports, residence permits and any other eMRTDs which may be developed in the future.
FIPS	Federal Information Processing Standards. Standard published by NIST.
HSM	Hardware Security Module is a physical computing device that safeguards and manages digital keys for strong authentication and provides crypto processing.
ICAO	The International Civil Aviation Organization is a UN specialized agency in charge of the planning and the development of safe international civil air transport by adopting standards and recommended practices.
Link certificate	Certificate created by a CSCA instance to certify its successor. Used to create trust to a new CSCA certificate.
ML	A Master List is a collection of trusted CSCA certificates combined into a secure container file-structure.
ML certificate	Certificate of the Master List.
MLS	A Master List Signer is an entity that digitally signs a Master List of CSCA certificates (domestic and/or foreign).
NIST	The National Institute of Standards and Technology (NIST) is a physical sciences laboratory and a non-regulatory agency of the United States Department of Commerce and in charge of promoting innovation and industrial competitiveness.
NPC	The National PKI Coordinator is the entity responsible for all issues related to the Swedish CSCA and coordinates the Swedish CSCA relations with foreign countries and international organisations.
PKD	Public Key Directory (PKD) is a central repository for exchanging the information required to authenticate ePassports.
PKI	A Public Key Infrastructure is a set of roles, policies, hardware, software and procedures needed to create, manage, distribute, use, store and revoke digital certificates and manage public-key encryption.

RA	Registration Authority is an entity responsible for accepting certificates requests and authenticating/registering the entity making them.
SOD	Document Security Object (SOD) is a special file stored on an ePassport. It stores hash values of all files stored in the chip (picture, fingerprint, etc.) and a digital signature of these hashes.
UPS	An uninterruptible power supply (UPS) is an electrical apparatus that provides backup emergency power when the main power fails.
VDS	A Visible Digital Seal is a cryptographic mechanism for ensuring the authenticity and integrity of non-electronic documents (e.g. visas).

1 Introduction

1.1 Overview

This document defines the Certificate Policy (CP) and Certification Practice Statement (CPS) governing the procedural and operational requirements for the Swedish Country Signing Certification Authority (CSCA) and its Subscribers. All parties MUST adhere to this document when issuing and managing digitally signed objects within the scope of electronic Machine Readable Travel Documents (eMRTD).

The Swedish Police Authority in Sweden (sw. Polismyndigheten) acts as the CSCA, DS for emergency passports and Master List Signer (MLS).

The CSCA was established in 2005 for the purpose of issuing CSCA certificates, MLS certificates and DS certificates. As a trust point, the Certification Authority (CA) is required to be governed by a certificate policy.

This document is owned by the Swedish Police Authority and is administered by the travel documents systems group (sw. Resehandlingssystem).

1.1.1 Purpose of this Document

The purpose of the document it to serve as the grounding foundation upon which trust should be built towards the Swedish CSCA by describing the principles used in certification.

This document also serves the purpose of describing the relationships, responsibilities, and obligations between the entities involved in the PKI infrastructure. Hence, the target groups of this document are the entities that make use of this CP.

1.1.2 Certificate Policy

The content of this document include the principles for issuance, usage, and maintenance of the certificates along with the underlying system. The policy also identifies the entities involved in the infrastructure.

The CSCA publicly discloses and highlights the features of certificates issued by it, considerations governing their use, certification processes, rights and obligations of the parties taking part in the certification process.

1.1.3 CP vs CPS

The CP states what needs to done and the policies around it. The CPS describes the manner in which the CP statements need to be executed.

The CPS MAY contain references to confidential information regarding procedures and policies that need to be executed.

1.1.4 Relationship with other PKI systems

Certificates MAY be published to the International Civil Aviation Organization (ICAO) Public Key Directory (PKD) which is a global repository of certificates originating from various countries CSCA.

As part of the eMRTD life cycle, the CSCA also forms part of the issuance system along with the verification.

1.2 Document name and identification

The name of this document is the “National Certificate Policy (CP) Swedish Country Signing CA”.

This document is uniquely identified according to section 7.1.6 Certificate Policy Object Identifier.

Document Name	Object identifier (OID)
National Certificate Policy (CP) Swedish Country Signing CA	1.2.752.84.101.1

1.3 PKI participants

This section defines and describes the participants of the Swedish CSCA. The table below shows an overview of the PKI participants:

Identifier	CA	RA	Subscriber	Relying Party
Swedish Country Signing CA	☑	☑		
Document Signers*			☑	
Master List Signers**			☑	☑
Swedish Inspection Systems				☑
ICAO (Member States)				☑
2D Barcode Signer***			☑	☑

* Entities that digitally signs Swedish travel documents (e.g. Swedish travel document manufacturers)
** Entities that digitally signs Swedish master lists (e.g. Swedish CSCA)
*** Entities that digitally signs Swedish Visa Stickers (e.g. Swedish Migration Agency)

1.3.1 Certification Authority (CA)

The CSCA is the primary trust point for the entire PKI architecture. The specific duties of the CSCA are to:

- Provide certificate services in accordance with its certificate policy, certification practice statement, and certification revocation services.
- Revoke certificates and publish certificate revocation lists.

1.3.2 Registration Authority (RA)

The RA is responsible for all tasks related to the certificate enrolment. The specific roles of the RA include:

- Process certificate requests in accordance with this CP, applicable RA agreements, and other policies and procedures with regards to the issued certificates.
- Maintain and process all supporting documentation related to the certificate application process,
- Process certificate revocation requests in accordance with this CP and other relevant operational policies and procedures with respect to the issued certificates. Without limitation to the generality of the foregoing, the RA can request the revocation of any certificate that it has approved for issuance according to the conditions described in this document.
- Forwarding approved certificate request to the CA.

For this implementation, the RA accepts certificate requests dispatched manually. It is the responsibility of the personnel performing the RA role to verify the requests and process them. An automatic process for certificate request submission MAY be supported. In this case it is secured by SSL/TLS and client certificates

The Swedish CSCA acts as the RA to manage and approve requests for document signers.

1.3.3 Subscriber

Subscribers are document signers compliant with the ICAO standard [Doc9303].

The Swedish CSCA issues certificates to the following Subscribers:

- DS: the Document Signer that digitally signs data to be stored either on a Swedish eMRTD or on a Swedish residence permit/card.
- MLS: the Swedish Master List Signer is the entity that digitally signs a list of CSCA certificates.
- BCS: A Bar Code Signer that digitally signs data to be stored on VISA stickers.

1.3.4 Relying Party

Relying parties are PKI participants that give trust to signed information created by the Swedish CSCA. The relying party is responsible for deciding whether or how to check the validity of the certificate by checking the appropriate certificate status information.

1.4 Certificate Usage

This section defines the appropriate application and usage of the Swedish CSCA artefacts (Certificates, Master Lists, Certificate Revocation Lists).

1.4.1 Acceptable uses

- The Swedish CSCA certificate SHALL be the trust point for Sweden.
- The Swedish CSCA link certificate SHALL be used for verification of a CSCA chain.
- The private key of the Swedish CSCA certificates SHALL only be used to sign DS certificates, Swedish ML certificates, Swedish BC certificate and CRLs.
- The private key of the DS certificate SHALL be used only for signing the data groups as stipulated in the ICAO 9303 standards.
- The private key of the ML certificate SHALL be used only for signing the Swedish Master List.
- The private key of the 2D bar code certificate SHALL be used only for signing the bar codes used for VISA stickers.

1.4.2 Prohibited uses

Any use that falls outside of this CP is prohibited.

1.5 Policy administration

1.5.1 Organisation Administering the Document

Swedish Police Authority (sw. Polismyndigheten).

1.5.2 Contact Person

Swedish Police Authority
IT Department
Att: National PKI Coordinator
SE-10675 Stockholm
Sweden

Email: emrtd@polisen.se

2 Publication and repository responsibilities

2.1 Repositories

The CSCA SHALL publish CSCA certificates and this CP on the Swedish Police Authority website: https://www.polisen.se

The CSCA MAY publish its certificates and CRLs to the ICAO PKD.

The CSCA CRL SHALL be accessible on:
http://cert.polisen.se/CSCA/SWE.crl

2.2 Publication of Certification Information

The Swedish CSCA SHALL publish information to the designated repository. The Swedish CSCA SHALL publish the following artefacts:

- CSCA certificates
- CSCA link certificates
- CRL
- CP

2.3 Time or Frequency of Publication

The Swedish CSCA SHALL publish a new CP if and only if any change occurs to it or to the entities involved by this current CP.

The Swedish CSCA SHALL publish certificates and CRL following their generation and issue.

2.4 Access Controls on Repositories

The Swedish CSCA SHALL guarantee the integrity of the published objects.

The Swedish CSCA SHALL protect repository information not intended for public dissemination or modification. Certificate information in the repository SHALL be made available to the PKI participants and other parties as determined by the applicable agreement as described in this document.

For directory search or fetch, access restrictions are implemented to prevent misuse and unauthorised harvesting of information.

For information present in the ICAO PKD, the ICAO PKD repository standards apply.

3 Identification and Authentication

3.1 Naming

3.1.1 Type of Names

The CSCA MUST have a unique and readily identifiable Distinguished Name (DN) according to the X.500 standard. Naming conventions is approved by CSCA.

The Swedish CSCA SHALL have the following DN:

Certificate Type	Distinguished Name
CSCA certificate	CN=Swedish Country Signing CA v2, O=Polismyndigheten, C=SE

The Swedish CSCA SHALL only generate and sign requests for Subscribers identified by the following DNs:

Type	Distinguished Name
DS (Passports)	CN=Swedish Passport Document Signer, O=Polismyndigheten, C=SE
DS (Emergency Passports)	CN=Swedish Emergency Passport Document Signer, O=Polismyndigheten, C=SE
DS (Residence Permit)	CN=Swedish Residence Permit Document Signer, O=Polismyndigheten, C=SE
DS (Residence Card)	CN=Swedish Residence Card Document Signer, O=Polismyndigheten, C=SE
DS (National ID Card)	CN=Swedish National ID Card Document Signer, O=Polismyndigheten, C=SE
Master List	CN= Swedish eMRTD Master List Signer, O=Polismyndigheten, C=SE
Bar Code	CN=[A-Z0-9]{2}, C=SE

3.1.2 Need for names to be meaningful

The Swedish CSCA distinguished name SHALL be meaningful, human readable, and SHALL comply with the requirements of [Doc9303].

3.1.3 Anonymity or Pseudonymity of Subscribers

The Swedish CSCA SHALL forbid the issuance, generation, or signature of anonymous certificates.

3.1.4 Rules for interpreting various name forms

The naming convention used by CSCA and DS SHALL follow ISO/IEC 9595 (X.500) DN.

3.1.5 Uniqueness of Names

The Swedish CSCA SHALL enforce the uniqueness of names used in the Swedish CSCA PKI. The Swedish CSCA SHALL assign names to all DS.

3.2 Initial identity validation

3.2.1 Method to prove possession of private keys

For CSCA root certificate generation, proof of possession of private key is ensured by the witnesses present during the key ceremony.

For signer certificates, proof of possession of private keys is established by manually obtaining the requests from the Subscriber.

Subscriber keys are produced under the control of the Subscriber. With his signature under the application for a certificate, the Subscriber confirms that:

- The key identifier (fingerprint) for a signer certificate in fact identifies the signer key to be certified.
- The keys comply with the specifications given in [Doc9303].
- The keys are newly generated and not previously used.

3.3 Identification and Authentication for Re-key request

3.3.1 Identification and Authentication for routine re-key

As described in 3.2.1 Method to prove possession of private keys.

3.3.2 Identification and Authentication for Re-key after revocation

As described in 3.2.1 Method to prove possession of private keys.

If a certificate is revoked, an authorised representative of the signer entity SHALL provide sufficient information before the Swedish CSCA initiates generation of a new signer certificate.

3.4 Identification and Authentication for Revocation Requests

Revocation requests SHALL be authenticated to verify that the revocation has been requested by an authorised entity. The National PKI Coordinator (NPC) SHALL identify the revocation request for any Swedish CSCA Subscriber through the DN, the serial number and the fingerprint of the object to be re-voked.

4 Certificate Life Cycle Operational Requirements

4.1 Certificate Application

4.1.1 Submission of Certificate Application

Subscribers listed in 3.1.1Type of Names are authorized to apply for certificates.

The Swedish Police Authority appoints the legal entity that will act as authorized representative for each Subscriber.

4.1.2 Enrolment Process and Reponsibilities

The CSCA operating manuals SHALL define and describe all processes related to enrolment.

The enrolment SHALL be carried out by the RA at the Swedish Police Authority who ensures the compliance with the definitions given in this document.

4.2 Certificate Application Processing

Applications received for new Subscriber certificates SHALL be processed by the Swedish CSCA.

4.2.1 Performing Identification and Authentication Functions

The Swedish PKI security officer SHALL verify the identity of the involved representatives and SHALL confirm their role.

For a first Subscriber certificate request, identity proofing functions SHALL be performed manually. Requests are submitted manually via a mass storage device with the custodian entrusted with the task of securing the request during transport. The identity of the custodian SHALL be verified in order to ensure that the request is genuine.

4.2.2 Approval or Rejection of Certificate Applications

If authorization according to section 4.1.1 and 3.2.1 is proven and if the Subscriber was successfully authenticated, a well-formed application is accepted. Failure to meet the above mentioned criteria results in a rejected application.

4.2.3 Time to Process Certificate Applications

A certificate application SHALL be processed within 7 days, once the certificate request has been approved.

4.3 Certificate Issuance

Issuance of certificates that requires the action of the CSCA SHALL take place in the secure area of the CA.

4.3.1 CA Actions During Certificate Issuance

The issuance process SHALL be carried out according to operation manuals.

4.3.2 Notification to Subscriber by the CA of Issuance of Certificate

When a new Swedish CSCA root certificate is issued the following entities SHALL be notified:

- ICAO PKD Service
- The European Commission
- All of its Subscribers

When a new Subscriber certificate is issued, the following entities SHALL be notified:

- The Subscriber of the certificate

4.4 Certificate Acceptance

4.4.1 Conduct Constituting Certificate Acceptance

If the Subscriber does not respond within 5 days after certificate deliverance, the certificate is deemed to be accepted.

4.4.2 Publication of the Certificate by the CA

The Swedish CSCA SHALL publish new root certificates to its repository mentioned in section 2.1.

In the case of DS certificates belonging to eMRTDs, the Swedish CSCA MAY also publish the certificates to ICAO according to [Doc9303].

4.5 Key Pair and Certificate Usage

The CSCA private keys SHALL only be used within the usage period specified for the private key and for the explicit purpose of the certificate specified in 1.4 Certificate Usage.

4.5.1 Subscriber Private Key and Certificate Usage

A Subscriber to the Swedish CSCA SHALL use the private keys and certificates within the usage period of the private key and for purposes specified in 1.4 Certificate Usage.

4.5.2 Relying Party Public Key and Certificate Usage

A relying party to the Swedish CSCA SHALL use DS certificate public keys for the verification of the Document Security Object (SOD) on an eMRTD.

The Relying Party to the Swedish CSCA SHALL use ML certificate public keys for the verification of the ML signature.

The Relying Party to the Swedish CSCA SHALL use BC certificate public keys for the verification of the bar code in visa stickers.

4.6 Certificate Re-key

4.6.1 Circumstance for Certificate Re-Key

The expiration of the validity period of the Swedish CSCA private key SHALL trigger a re-key. A Swedish CSCA re-key MAY take place in case of specifications requiring modifications to the Swedish CSCA's certificate profile, enforcing augmented security requirements, or under otherwise unforeseeable special circumstances.

DS certificates SHALL be re-keyed when:

- The certificate is about to expire;
- The DS private key is compromised;
- Under otherwise unforeseeable special circumstances.

ML certificates SHALL be re-keyed when

- The certificate is about to expire;
- The ML private key is compromised;
- Under otherwise unforeseeable special circumstances.

BCS certificates SHALL be re-keyed when

- The certificate is about to expire;
- The BC private key is compromised;
- Under otherwise unforeseeable special circumstances.

4.6.2 Who may request a re-key

For the CSCA root certificates, only the NPC MAY request a re-key.

For DS certificates, the owner of the DS entity MAY request a re-key. In the event this occurs, the owner of the DS entity SHALL inform the NPC about this request.

For ML certificates, the owner of the MLS entity MAY request a re-key. In the event this occurs, the owner of the MLS entity SHALL inform the NPC about this request.

For BC certificates, the owner of the BCS entity MAY request a re-key. In the event this occurs, the owner of the BCS entity SHALL inform the NPC about this request.

4.6.3 Processing Certificate re-keys

The process of re-keying SHALL be performed according to the CSCA operating manuals.

4.6.4 Notification of New Certificate Issuance to Subscriber

An authorised representative of the Subscriber SHALL be informed in writing of the issuance of a new certificate.

4.6.5 Conduct Constituting Acceptance of re-keyed Certificate

If the Subscriber does not respond within 5 days of certificate deliverance, the certificate is deemed to be accepted.

4.6.6 Publication of the Renewed Certificate by the CA

The Swedish CSCA SHALL publish the re-keyed certificate in the repositories defined in section 2.1 Repositories.

4.6.7 Notification of Certificate Issuance by the CA to other entities

The NPC SHALL notify to the EU Commission and the ICAO PKD Service according to [Doc9303].

4.7 Certificate Renewal

Certificate renewal is not offered.

4.8 Certificate Modification

Certificate modification SHALL only be done in conjunction with a certificate re-key and is carried out during the process describe in section 4.6 Certificate Re-key.

4.9 Certificate Revocation and Suspension.

4.9.1 Circumstance for revocation of a certificate

The Swedish CSCA root certificate SHALL be revoked in case of a major incident such as a key compromise.

The Swedish CSCA MAY revoke ANY Subscriber under the following circumstances:

- Compromise of the private key is suspected or discovered.
- Termination of business.
- Certificate was issued on the basis of false statements.
- Identifying data in the certificate are no longer considered valid.
- Any major incident or other event.

4.9.2 Who can request revocation of a certificate

For Swedish CSCA certificates, only the NPC MAY submit a request for revocation.

4.9.3 Procedure for Revocation Request

The process of revocation SHALL be performed according to the CSCA operating manuals

4.9.4 Time within which CA MUST Process the Revocation Request

Authorised certificate revocation requests SHALL be processed as soon as possible.

4.9.5 Revocation Checking Requirements for Relying Parties

The relying parties of the Swedish CSCA SHALL check the status of any Swedish CSCA certificate on which it relies toward the Swedish CSCA CRL defined in section 2.1 Repositories.

4.9.6 CRL Issuance Frequency

The Swedish CSCA SHALL issue CRLs according to [Doc9303].

4.9.7 Maximum Latency of CRLs

The Swedish CSCA SHALL issue CRLs according to [Doc9303].

4.9.8 Online Revocation Checking Availability

The Swedish CSCA CRL SHALL be available at least under the URL as defined in 2.1 Repositories.

4.9.9 Special Requirements Related To Key Compromise

Subscribers and relying parties will be responsible for any losses resulting from the use of a compromised key if they continue to use it with the knowledge that it is compromised.

4.10 End of Subscription

Any Swedish CSCA Subscriber MAY end the subscription by:

- Allowing its own certificate to expire without requesting a new certificate.
- Revoking its certificate prior to the certificate expiration.

The Swedish CSCA MAY end the subscription of any Swedish CSCA Subscriber certificate by:

- Not renewing the certificate after its expiration.
- Revoking the certificate prior to the certificate expiration.

5 FACILITY MANAGEMENT & OPERATIONAL CONTROLS

5.1 Physical Controls

5.1.1 Site Location & Construction

The Swedish CSCA and ANY Subscriber SHALL be operated in a physically protected area.

The Swedish CSCA SHALL be operated in an secure area dedicated exclusively to the eMRTD team under control by the Swedish Police Authority.

ANY Subscriber SHALL be located in a secured area with restricted access in the premises of the Subscriber.

The Swedish CSCA Hardware Security Module MAY be removed from the eMRTD-PKI area if and only if the HSM devices have been wiped and no cryptographic keys or parts of them can be read.

ANY Subscriber HSM is NOT allowed to leave the secure area unless the respective hardware has been wiped and no cryptographic keys or parts of them can be read.

5.1.2 Physical Access

The PKI equipment of the Swedish CSCA or ANY Subscriber SHALL always be protected from unauthorized access. The following physical access control requirements SHALL apply:

- Entry to the premises SHALL be logged and secured.
- Access to the secure areas SHALL be secured using access controlled doors.
- The secure areas SHALL be monitored.

Only persons belonging to the eMRTD team at the Swedish Police Authority MAY have access to the area housing the Swedish CSCA components.

Other personnel (e.g. maintenance staff) MAY have access if and only if accompanied by authorized personnel from the eMRTD team; such access SHALL be logged.

5.1.3 Power and Air Conditioning

The areas housing the Swedish CSCA and the Subscriber PKI-components SHALL be equipped with an air conditioning system to regulate temperature and humidity. All electrical components SHALL be connected to an UPS.

5.1.4 Water Exposure

The area housing the Swedish CSCA and Subscriber PKI-components SHALL be equipped with water sensors. In the event that flooding does occur, the

power supply SHALL automatically be cut off and the appropriate personnel SHALL be alerted.

5.1.5 Fire Prevention and Protection

The area housing the Swedish CSCA and Subscriber PKI-components SHALL be equipped with fire and smoke sensors. Fire extinguishing mechanisms SHALL also be installed.

In the event of a fire, the power supply SHALL automatically be cut off and the appropriate personnel SHALL be alerted.

5.1.6 Media Storage

ANY media containing confidential information relating to the Swedish CSCA or a Subscriber, including safety copies, SHALL be kept in a fireproof safe.

5.1.7 Waste Disposal

The waste disposal SHALL be carried out in secure manner such that, any information cannot be read, re-produced, or used for any purpose.

5.1.8 Off-Site backup

Backup SHOULD be taken to an off-site location in order to facilities disaster recovery and business continuity.

5.2 Procedural Controls

5.2.1 Trusted Roles

To allow for a secure operation the Swedish CSCA SHALL define and administer the following roles:

- NPC;
  The NPC is responsible for all issues related to the Swedish CSCA and SHALL verify and coordinate all activities of the Swedish CSCA as well as its Subscribers. The NPC is also responsible for the Swedish CSCA notifications and SHALL further keep and manage the international relations to other states and their coordinators as well as international organisations (i.e. ICAO, EU-Commission, etc.).
- PKI security officer;
  The PKI security officer is responsible for RA functionality, i.e. authenticating certificates request, certificate deliverance, certificate issuance notification, and delivering certificate requests to the CA operator.
- CA operator;
  The CA operator are responsible for running all services delivered by the Swedish CSCA. They are also responsible for maintaining and ensuring the availability of the certification infrastructure.
- Owner;
  The owner is responsible for the use and withdrawal of the objects issued by the Swedish CSCA.

- Auditor;
  The auditor is responsible for enforcing compliance with all legal requirements and for the adherence to physical and functional security policies by Swedish CSCA and its environment.

5.2.2 Number of Persons Required per Task

ALL security critical operations SHALL require the presence of two authorised persons. These operations include, but are not limited to, creation; activation; de-activation; backup and recovery of the Swedish CSCA private keys. The revocation of Swedish CSCA private keys is possible only under the supervision of two authorised persons. A two person principle is also applied when carrying out maintenance on the (e.g. when the cryptographic module is initialised) CSCA infrastructure.

5.2.3 Identity-proofing for Each Role

ANY individual SHALL identify and authenticate himself before being permitted to perform any actions set forth above for that role or identity. Identification and authentication are done on the basis of the Swedish Police Authority standard procedure (i.e. personal access cards with PIN).
CA operator carrying out the most critical CA tasks SHALL also use additional personal access cards, specific to their roles.

5.2.4 Separation of Roles

The Swedish CSCA and ANY Subscriber SHALL ensure that no individual have more than one trusted role. Separation of duty SHALL be enforced for tasks described in section 5.2.2.

5.3 Personnel Controls

5.3.1 Background, Qualifications, Experience, & Security Clearance

ALL personnel occupying a trusted role MUST possess the necessary qualifications and experience to provide PKI services. ALL personnel occupying a trusted role at the Swedish CSCA MUST be employed by the Swedish Police Authority.

ALL personnel occupying a trusted role at the Swedish CSCA or ANY Subscriber SHALL understand the involved processes and MUST understand the effects and implications of all actions taken.

ALL personnel of the Swedish CSCA MUST have security clearance in accordance with the regulations of the Swedish Police Authority.

ALL personnel occupying a trusted role of ANY Subscriber MUST have security clearance.

5.3.2 Background Check Procedures

At the Swedish CSCA background checks are carried out for all personnel and in accordance with Swedish law.

5.3.3 Training Requirements

The Swedish CSCA and ANY Subscriber SHALL ensure that all personnel receive appropriate training in order to fulfil the requirements laid out in section 5.3.1.

5.3.4 Retraining Frequency & Requirements

Individuals responsible for any eMRTD PKI role SHALL be made aware of changes in the CA operation. ANY significant change to the operations SHALL have a re-training plan. The CSCA SHALL review and update its training program regularly to accommodate changes in the CA system.

5.3.5 Sanctions for Unauthorised Actions

Unauthorized actions by Swedish CSCA Personnel MUST be sanctioned as regulated by Swedish Law.

5.3.6 Contracting Personnel Requirements

Independent contractors SHALL undergo the procedures and adhere to the requirements defined by the Swedish Police Authority.

5.3.7 Documentation Supplied To Personnel

The Swedish CSCA SHALL make any relevant documents available to its personnel to perform their duties.

5.4 Audit Logging Procedures

5.4.1 Types of Events Recorded

Audit log files MUST be generated for all events relating to the security, issuance, and maintenance of the Swedish CSCA and its RA. At a minimum, the following events SHALL be logged:

- Creation, use, and destruction of keys and certificates;
- Creation and modification of registration entries;
- All request and reports relating to incident notification and suspension of registrations, as well as the resulting actions.

Audit logs for each auditable event SHALL be stored and maintained according to the requirements of the Swedish Police Authority.

5.4.2 Frequency of Processing Data

Audit logs SHALL be processed in accordance with the regulation of the Swedish Police Authority.

5.4.3 Retention Period for Security Audit Data

Retention of the Swedish CSCA audit log data SHALL be processed in accordance with the regulation of the Swedish Police Authority.

5.4.4 Protection of Security Audit Data

The protection of Swedish CSCA audit log data SHALL be done in accordance with the regulation of the Swedish Police Authority.

5.4.5 Security Audit Data Backup Procedures

The Swedish CSCA audit log SHALL be backed up in accordance with the regulation of the Swedish Police Authority.

5.4.6 Security Audit Collection System

The Swedish CSCA SHALL implement an external log collection system within the Swedish Police Authority.

5.4.7 Notification to Event Causing Subject

The event causing subject SHALL be notified according to the procedures declared by the Swedish Police Authority.

5.4.8 Vulnerability Assessments

Automatic security check of ALL components involved in the Swedish CSCA SHALL be carried out according to the procedures declared by the Swedish Police Authority.

5.5 Records Archive

5.5.1 Types of Events Archived

The Swedish CSCA archive records SHALL be sufficiently detailed to establish the proper operation of the CA, or the validity of any certificate (including those revoked or expired) issued by the CA.

The Swedish CSCA SHALL archive all relevant data relating to the issuance and maintenance of the Swedish CSCA objects and in particular SHALL archive:

- ALL incident reports and;
- ALL vulnerability analysis reports.

5.5.2 Retention Period for Archive

ALL archives SHALL be retained in accordance with the regulations of the Swedish Police Authority.

5.5.3 Protection of Archive

Archive records SHALL be stored in a secure storage facility separate from the component itself.

5.5.4 Archive Backup Procedures

Archive records SHALL be backed-up in accordance with the regulations of the Swedish Police Authority.

5.5.5 Requirements for Time-Stamping of Records

ALL archived records SHALL be provided with a time stamp in accordance with the regulations of the Swedish Police Authority.

5.5.6 Archive Collection System (Internal or External)

An archive collection system SHALL be external to the Swedish CSCA and implemented in accordance with the regulation of the Swedish Police Authority.

5.5.7 Procedures to Obtain & Verify Archive Information

Procedures to obtain and verify archive information SHALL be done in accordance with the regulations of the Swedish Police Authority.

5.6 Key Changeover

See section 4.6 Certificate Re-key.

5.7 Compromise & Disaster Recovery

5.7.1 Incident and Compromise Handling Procedures

The Swedish eMRTD PKI SHALL notify all incidents to the NPC and MAY notify all or some incidents to some Swedish CSCA Subscribers and relying parties.

The Swedish CSCA SHALL handle all incidents according to the operation manual.

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

In case of a major or critical incident or disaster, related to data corruption, the Swedish eMRTD PKI SHALL rely on the backup archives to recover the information.

5.7.3 CA Private Key Compromise Recovery Procedures

The Swedish CSCA key compromise recovery procedure SHALL be carried out according to the operating manuals.

5.7.4 Business Continuity Capabilities after a Disaster

In the case of a disaster whereby Swedish CSCA installation is physically damaged and all copies of the CA signing key are destroyed as a result, the Swedish CSCA SHALL continue to remain valid. A new CSCA SHALL be created using a new infrastructure, re-using information whenever possible.

6 TECHNICAL SECURITY CONTROLS

6.1 Key Pair Generation & Installation

6.1.1 Key Pair Generation

The Swedish CSCA key generation process SHALL be documented, recorded, and witnessed and attested by a party separate from the CA trusted roles as part of a key ceremony. Key generation MUST be performed using trustworthy systems and processes that provide the required cryptographic strength of the generated keys. These systems and processes SHALL prevent the loss, disclosure, modification, or unauthorized use of such keys. The Swedish CSCA SHALL use an HSM for CA key generation and storage.

ANY Swedish CSCA Subscriber SHOULD adhere to the above mentioned requirements.

6.1.2 Private Key Delivery to Subscriber

A Swedish CSCA Subscriber private key MUST be generated at the Subscriber's premises and MUST NOT be transferred.

6.1.3 Public Key Delivery to Certificate Issuer

The public key to be certified by the Swedish CSCA SHALL be submitted to the Swedish CSCA by the Subscriber through a standard CSR. The CSR SHALL be generated at the Subscriber's premises according to [Doc9303] and be handed over in person on a storage medium.
An automated process MAY be established between the Subscriber and the CSCA for automatic public key delivery.

6.1.4 CA Public Key Delivery to Subscribers and Relying Parties

The Swedish CSCA SHALL publish the Swedish CSCA certificates as described in 2.1 Repositories.

6.1.5 Key Sizes

Key sizes SHALL comply with [Doc9303].

6.1.6 Public Key Parameters Generation and Quality Checking

Key parameters SHALL comply with [Doc9303].

6.1.7 Key Usage Purposes

The key usage purposes SHALL comply with [Doc9303].

6.2 Private Key Protection & Crypto Module Engineering Controls

6.2.1 Cryptographic Module Standards & Controls

The Swedish CSCA and the Swedish CSCA Subscribers SHALL use security modules compliant with [Doc9303].

6.2.2 CA Private Key Multi-Person Control

The use of CSCA private key SHALL require action by multiple persons.

6.2.3 Private Key escrow

The Swedish CSCA MUST NOT escrow any private keys.
Subscribers of the Swedish CSCA MUST NOT escrow their respective private keys.

6.2.4 Private Key Backup

The Swedish CSCA private keys MUST be secured through a standard backup procedure as defined for the underlying HSM.
Subscribers of the Swedish CSCA MUST NOT backup their private keys.

6.2.5 Private Key Archival

The Swedish CSCA private keys SHALL NOT be archived.
Subscribers of the Swedish CSCA SHALL NOT archive their respective private keys.

6.2.6 Private Key Transfer into or from a Cryptographic Module

For the Swedish CSCA, private keys are only allowed transfer into or from the cryptographic module under the following circumstances:

- In case of a backup.
- In case of a hardware replacement following a restore from a backup.

For the Subscriber private keys:

- The Subscriber private keys SHALL be generated in and remain in the same hardware cryptographic module.
- The Subscriber private key SHALL NOT be temporarily or permanently saved in software for any purpose.

6.2.7 Private Key Storage on Cryptographic Module

The cryptographic module SHALL comply with [Doc9303].

6.2.8 Method of Activating Private Keys

The private key of the Swedish CSCA and ANY Subscriber SHALL be activated in accordance with the specification from the manufacturer of the HSM.

6.2.9 Methods of Deactivating Private Keys

The private key of the Swedish CSCA and ANY Subscriber MAY be deactivated by authorized personnel when not in use.

6.2.10 Methods of Destroying Private Keys

All Swedish CSCA private keys SHALL be destroyed in such a way that they cannot be recreated or reused, when they are no longer needed or when the certificates to which they correspond expire or are revoked.

6.2.11 Cryptographic Module Rating

See Chapter 6.2.1 Cryptographic Module Standards & Controls

6.3 Other Aspects of Key Management

6.3.1 Public Key Archive

The Swedish CSCA and Swedish CSCA Subscribers' public keys MAY be archived.

6.3.2 Certificate Operational Periods and Key Usage Periods

The operational period of the Swedish CSCA key usage period SHALL comply with [Doc9303]. .

6.4 Computer Security Controls

The Swedish CSCA and all of its subcomponents SHALL implement security controls in accordance with the regulations of the Swedish Police Authority.

ANY Subscriber of the Swedish CSCA SHALL implement security controls.

6.5 Life Cycle Technical Controls

6.5.1 System Development Controls

The Swedish CSCA and all of its subcomponents SHALL implement controls for detection of changes to configuration in accordance with the regulations of the Swedish Police Authority.

6.5.2 Security Management Controls

The entire Swedish CSCA infrastructure SHALL operate under an existing security management system within at Swedish Police Authority.

6.6 Network Security Controls

The Swedish CSCA infrastructure SHALL be operated in a dedicated network segment. The network MUST be protected with firewalls and only accessible to authorized personnel.

All unauthorized access MUST be logged and the appropriate personnel SHALL be notified.

6.7 Time Stamping

The Swedish CSCA PKI SHALL use an reliable time server provided by the Swedish Police Authority.

This time server SHALL be applied for ALL activities related to the Swedish CSCA PKI activities, e.g. issuing of certificates and CRLs, logs entries, etc.

7 CERTIFICATE, CRL, AND OCSP PROFILES

The Swedish CSCA self-signed and link certificates SHALL be generated according to the profile specified in [Doc 9303].

The Subscriber certificates SHALL be generated according to the profile specified in [Doc9303].

7.1 Certificate Profile

7.1.1 Version Number(s)

The version number SHALL be set according to [Doc9303]

7.1.2 Certificate Extensions

The certificate extensions SHALL comply with [Doc9303]

7.1.3 Algorithm Object Identifiers

The algorithm object identifiers for the CSCA self-signed and link certificate, and Subscriber certificates SHALL comply with [Doc9303].

7.1.4 Name Forms

The name forms SHALL comply with [Doc9303].

7.1.5 Name Constraints

The name constraints SHALL comply with [Doc9303].

7.1.6 Certificate Policy Object Identifier

The Swedish CSCA certificate policy and certification practice statement is uniquely identified by the following OID: 1.2.752.84.101.1

7.1.7 Processing Semantics for the Critical Certificate Policies Extension

The processing semantics for the critical certificate policies extension SHALL comply with [Doc9303].

7.2 CRL Profile

The Swedish CSCA CRL SHALL be generated according to the profile specified in [Doc 9303] and SHALL be signed by the current Swedish CSCA for ALL revoked Swedish CSCA objects.

7.2.1 Version Number(s)

The version number SHALL be set according to [Doc9303].

7.2.2 CRL and CRL Entry Extensions

The CRL SHALL be set according to [Doc9303].

8 COMPLIANCE AUDIT & OTHER ASSESSMENTS

8.1 Frequency and Circumstances of Assessments

The Swedish CSCA SHALL conduct a compliance audit which is no less frequent than once every 3 years.

Moreover, the Swedish Police Authority MAY at any time require an audit of the Swedish CSCA to validate that it is operating in accordance with this document.

8.2 Qualifications of Assessor

The auditor SHALL be appointed by the NPC and SHALL be member of the IT-Security group at the Swedish Police Authority.

8.3 Topics Covered by Assessment

The audit SHALL verify the compliance of the Swedish CSCA to this document.

8.4 Actions Taken As A Result Of Deficiency

In case deficiencies are found during the assessment, the Swedish CSCA SHALL undertake the necessary corrections to comply with this document.

The NPC, together with input from the auditor, is responsible for approving a corrective action plan in case deficiencies are found during the assessment.

8.5 Communication of Results

An audit compliance report, including identification of corrective measures taken or being taken by the audited party, SHALL be provided to the Department of Justice at the Swedish Police Authority.

9 OTHER BUSINESS & LEGAL MATTERS

9.1 Fees

Certificate issuance by the Swedish CSCA is free of charge.

9.2 Financial Responsibility

No entities involved in this system are required to meet any financial responsibility.

9.3 Warranties

9.3.1 CSCA Warranties

The Swedish CSCA will warrant and agree to:

- Provide the operational infrastructure and certification services;
- Provide certification and repository services consistent with this CP, CPS and operating policies and procedures;
- Use its private signing key only to sign certificates and CRLs and for no other purpose;
- Perform authentication and identification procedures in accordance with applicable agreement and operational policies and procedures.

9.3.2 RA Warranties

The RA will warrant and agree to:

- Provide the operational infrastructure and registration services;
- Comply with the stipulations of this CP;
- Be subject to revocation of RA responsibilities if acted in a manner inconsistent with the CP.

9.3.3 Relying Parties Warranties

Relying Parties who rely upon the certificates issued by the Swedish CSCA SHALL:

- Use the certificate for the purpose for which it was issued, as indicated in the certificate information;
- Verify the validity Swedish CSCA certificates by ensuring that the certificate has not expired;
- Establish trust in the CA who issued a certificate by verifying the certificate path in accordance with the guidelines set by [Doc9303].

9.3.4 Subscriber Warranties

Subscribers to the Swedish CSCA agree to:

- Secure their private keys and take reasonable and necessary precautions to prevent loss, disclosure, modification, or unauthorized use of the private key.
- Use Subscriber certificates only for its intended uses as specified by the Swedish CSCA.

- Notify the Swedish CSCA in the event of a key compromise immediately whenever the Subscriber has reason to believe that the private key has been lost, accessed by another individual, or compromised in any other manner.
- Immediately cease the use of the Subscriber certificate upon termination of the Subscriber agreement, revocation or expiration of the Subscriber certificate.

9.4 Term & Termination

9.4.1 Term

The Swedish CSCA CP and CPS SHALL become effective at the time of publication to the repository. Amendments to this policy or practice statement SHALL become effective upon publication to the same repository.

9.4.2 Termination

The Swedish CSCA CP and CPS SHALL be valid until:

- it is either replaced by a newer revision or;
- the Swedish CSCA is forced to end its certification services.

In case of the Swedish CSCA ending its certification services, this CP and CPS SHALL remain valid at least until the last certificate issued by the Swedish CSCA is valid.

9.4.3 Effect of Termination and Survival

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

9.5 Individual Notices & Communications with Participants

Changes to this CP/CPS SHALL be communicated to the Swedish CSCA Subscribers by established channels for communications.

9.6 Amendments

9.6.1 Procedure for Amendment

The Legal Department at the Swedish Police Authority SHALL review this CP regularly in case of system changes. Errors, updates, or suggested changes to this CP SHALL be communicated to the PKI participants and Subscribers. Such communication SHALL include a description of the change, a change justification, and contact information for the person requesting the change.

9.6.2 Notification Mechanism and Period

This CP and any subsequent changes SHALL be made available to the PKI participants within one week of approval. The Legal Department at the Swe-

dish Police Authority reserves the right to amend this CP without notification for amendments that are not material, including without limitation corrections of typographical errors, changes to URLs, and changes to contact information.

9.6.3 Circumstances under which OID MUST be changed

The Swedish CSCA CP/CPS OIDs SHALL be changed if the NPC determines that a change in the CP/CPS modifies the level of trust provided by the CP/CPS.

9.7 Governing Law

The Swedish CSCA CP and CPS is governed by Swedish law.

10 References

Identifier	Title
CPS	Certification Practice Statement of the Swedish Country Signer CA
Doc9303	Doc9303, Machine Readable Travel Documents, Seventh Edition, 2015, Part 12: Public Key Infrastructure for MRTDs
FIPS140-2	NIST, SECURITY REQUIREMENTS FOR CRYPTOGRAPHIC MODULES, May 25, 2001
RFC3647	Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework
RFC 2119	Key word for use in RFCs to indicate requirement levels