Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Swiss Confederation

Federal Department of Justice and Police FDJP

Federal Office of Police fedpol

Certificate Policy (CP) and Certification Practice Statement (CPS) of the Swiss Country Signing CA (Swiss CSCA)

Author	Arnaldo Cremisini, fedpol		
Publication date	24.08.2021		
Version	2.8		
Status	in process	under review	authorised for use
	☐	☐	☑

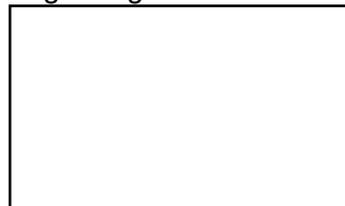| **Roles**	
CSCA Owner / Supervisor	Roman Vanek, Federal Office of Police, fedpol
National PKI Coordinator	Patrick Beer, Federal Office of Police, fedpol
Reviewer	Markus Waldner, Federal Office of Police, fedpol Jürgen Weber, FOITT

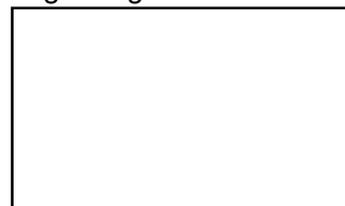| **Authorisation** |
| --- |

Place and date: Berne, 22.07.2021

Signed by:

National PKI Coordinator

Digital signature

CSCA Owner / Supervisor

Digital signature

Version History			
Date	Version	Author	Remarks
30.12.2015	2.0	Arnaldo Cremisini, fedpol	First Release of Version 2
26.01.2016	2.1	Arnaldo Cremisini, fedpol	Revision based on comments from fedpol and FOITT
21.03.2016	2.2	Arnaldo Cremisini, fedpol	Revision based on notes from fedpol
19.04.2016	2.3	Arnaldo Cremisini, fedpol	Editorial revision
11.05.2016	2.4	Arnaldo Cremisini, fedpol	Revision based on reviewer's notes
19.08.2016	2.5	Antonio Alessio, FOITT	Revision of chapter 8
26.09.2018	2.6	Arnaldo Cremisini, fedpol	Revision based on reviewer's notes
01.10.2018	2.7	Arnaldo Cremisini, fedpol	Editorial revision
19.07.2021	2.8	Nicolas Meuwly, Arnaldo Cremisini, fedpol	Revision based on PKI's Life-cycle
20.07.2021	2.8	Jürgen Weber, FOITT	Review
22.07.2021	2.8	Markus Waldner, fedpol	Review
22.07.2021	2.8	Patrick Beer, fedpol	Final version based on reviewer's notes

Table of Contents

1 Introduction

1.1 Overview

This document defines the Certificate Policy (CP) and Certification Practice Statement (CPS) governing the procedural and operational requirements, which the Swiss CSCA and its Subscribers must adhere to, when issuing and managing digitally signed objects.

This CP/CPS is based on the "Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework", [RFC3647] and takes further into account the ICAO Publications and Requirements [Doc9303].

1.2 Definitions and Acronyms

Although the [RFC3647] recommends all components and subcomponents to be included in this CP/CPS, the Swiss CSCA will only address specific and required components and subcomponents.

The statement "no stipulation" is used rarely and only where appropriate for editorial purposes.

All omitted components and subcomponents are all elements, for which "no stipulation" is implicitly declared.

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" are used according to [RFC2119] and are written in capital letters.

Acronym	Definition
CA	Certification Authority is an entity that issues digital certificates.
CP	Certificate Policy is a document, which aims to state, what are the different actors of a public key infrastructure (PKI), their roles and their duties.
CPS	Certification Practice Statement is a document from a Certificate Authority, which describes their practice for issuing and managing public key certificates.
CRL	Certificate Revocation List is a list of certificates (or more specifically, a list of serial numbers for certificates), that have been revoked, and therefore, entities presenting those (revoked) certificates should no longer be trusted.
CSCA	Country Signing Certification Authority as defined in [Doc9303].
DN	Distinguished Name (name of certificate holder (Subject DN) or certificate issuer (Issuer DN).
DS	Document Signer defined according to [Doc9303].
EC	Elliptic Curve is an algebraic structure used for cryptographic purposes.

Acronym	Definition
eMRTD	Electronic Machine Readable Travel Document (e.g. ePassport).
fedpol	Federal Office of Police of the Swiss Federal Department of Justice and Police.
FIPS	Federal Information Processing Standards (publication). Standard published by NIST.
FOITT	Federal Office of Information Technology, Systems and Telecommunication.
HSM	A hardware security module (HSM) is a physical computing device that safeguards and manages digital keys for strong authentication and provides crypto processing.
ICAO	International Civil Aviation Organization.
ICAO PKD Service	A service provided by ICAO to the service participants, to publish subscriber's certificates or generated objects such as CRL, Master-Lists, etc..
Inspection System	An Inspection System is both an organisation as well as an IT-system responsible for the verification of documents. For eMRTDs, it requires the information of the CSCA certificates to verify the digital content stored in the eMRTDs; therefore it is a relying party of the CSCA.
Master-List	A signed binary object, as specified by [Doc9303] and containing a list of CSCA certificates.
ML-Signer	The Master-List Signer is the entity responsible for the issuance and hence the signature of the Master-List.
National PKI Coordinator	The National PKI Coordinator is responsible for all issues related to the Swiss CSCA and coordinates the Swiss CSCA relations with foreign countries and international organisations.
NIST	U.S. Department of Commerce / National Institute of Standards and Technology Is the federal technology agency that works with industry to develop and apply technology, measurements, and standards.
PKI	A public key infrastructure (PKI) is a set of hardware, software, people, policies, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates and manage public-key encryption.
SEM	State Secretariat for Migration of the Swiss Federal Department of Justice and Police.
SPOC	Swiss Single Point of Contact for the eMRTD PKI/PKD.
SPOC TLS	SPOC Transport Layer Security are cryptographic protocols that provide communications security over a computer network.
Swiss eDoc PKD	Swiss National Public-Key Directory. Where, in the context of the adoption of biometric eMRTDs and Residence Permits, all required information will be accessible to

Acronym	Definition
	national participants only. It is also responsible for the international distribution of the Swiss CSCA public objects.
Swiss Government PKI	Is the Swiss Organisation in charge of the Swiss PKI, moreover it is responsible for operating the Swiss CSCA and for the publication of the Swiss CSCA public entities, such as certificates, CRL, etc.
TLS	Transport Layer Security is a cryptographic protocol designed to provide communications security over a computer network.
VDSS	Visa Digital Seal Signer defined according to [Doc9303].

Table 1: Acronyms

1.3 Document Name and Identification

This document is the Certificate Policy (CP) and the Certification Practice Statement (CPS) of the Swiss Country Signing Certificate Authority (Swiss CSCA).

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

1.4 PKI Participants

This chapter defines and describes the Participants to the Swiss Country Signing CA. The following table gives an overview of the participants:

PKI Participants			
Identifier	CA	Subscriber	Relying Party
CSCA	☒	☒	☐
DS	☐	☒	☒
VDSS	☐	☒	☒
ML-Signer	☐	☒	☒
SPOC TLS Server	☐	☒	☒
SPOC TLS Client	☐	☒	☒
Inspection Systems	☐	☐	☒
Organisations, e.g. ICAO, EU, Cantones, etc.	☐	☐	☒

PKI Participants			
Identifier	CA	Subscriber	Relying Party
Swiss Gov PKI, Swiss eDoc PKD	☐	☐	☒

Table 2: PKI Participants

1.4.1 Certification Authority

The Swiss Country Signing CA issues certificates, which are required to sign and verify the content of the Swiss eMRTD, the Swiss Residence Permits, the Visa Digital Seal and the Swiss Master List (ML), further guarantees the secure communication between the Swiss and Foreign SPOC.

The Swiss Country Signing CA complies with the requirements of this CP/CPS.

1.4.2 Subscribers

The Swiss CSCA issues certificates to the following subscribers only:

- DS: the Document Signer digitally signs data to be stored either on a Swiss eMRTD or on a Swiss Residence Permit.

- VDSS: the Visa Digital Seal Signer digitally signs data to be stored in a Swiss Visa 2D-Barcode.

- ML-Signer: the Swiss Master List Signer is the entity that digitally signs a list of CSCA certificates (Domestic and Foreign) generated by the Swiss eDoc PKD according to the rules defined by ICAO [Doc9303].

- SPOC TLS Server (Single Point of Contact – Transport security Layer Server side): authenticates the Swiss SPOC toward a foreign SPOC Client. It is the entity responsible for the secure connection with a foreign SPOC Client.

- SPOC TLS Client (Single Point of Contact – Transport security Layer Client side): it authenticates the Swiss SPOC toward a foreign SPOC Server. It is the entity responsible for the secure connection with a foreign SPOC Server.

1.4.3 Relying Parties

The Relying Parties of the Swiss CSCA are among others (as listed in 1.4), the Domestic and Foreign Inspection Systems, verifying the objects of the Swiss CSCA, as well as the digital content of the Swiss eMRTDs and Swiss Residence Permits.

1.4.4 Other Participants

The Swiss Government PKI and the Swiss eDoc PKD are further participants to the Swiss Country Signing CA.

1.5 Certificate Usage

This section defines the appropriate application and usage of the Swiss Country Signing CA objects (i.e. certificates, CRL, etc.).

1.5.1   Appropriate Certificate Uses

The Swiss CSCA SHALL issue the following objects:

- The Swiss CSCA Self-signed Certificate,
- The Swiss CSCA Link Certificate,
- The Swiss Document Signer Certificate (Swiss DS),
- The Swiss Visa Digital Seal Signer Certificate (Swiss VDSS),
- The Swiss Master-List Signer Certificate (Swiss ML-Signer),
- The SPOC TLS Server Certificate and
- The SPOC TLS Client Certificate.

The Swiss CSCA SHALL further generate and SHALL issue the Swiss CSCA CRL.

The Swiss CSCA MAY verify the signature of its issued objects.

The Swiss Document Signer (DS) SHALL sign the digital content of the Swiss eMRTD and Residence Permit according to [Doc 9303].

The Swiss Document Signer (DS) MAY verify the integrity and authenticity of the digital content as stored in the Swiss eMRTD and Residence Permit.

The Swiss Visa Digital Seal Signer (VDSS) SHALL sign the digital content of the Swiss Visa Seal according to [Doc 9303].

The Swiss Visa Digital Seal Signer (VDSS) MAY verify the integrity and authenticity of the digital seal content as stored in the Swiss Visa.

The Swiss Master-List Signer (ML-Signer) SHALL sign the Swiss Master-List generated by the Swiss eDoc PKD according to the rules defined by ICAO [Doc9303].

The Swiss Master-List Signer (ML-Signer) MAY verify the Swiss Master-List.

The Swiss SPOC TLS Server and Client SHALL authenticate and guarantee the Swiss SPOC toward foreign SPOC according to the rules defined by [EUCCP] and [CSN369791].

1.5.2   Prohibited Certificate Uses

This CP/CPS interdicts all usage of the Swiss CSCA certificates, not explicitly listed in the section 1.5.1 "Appropriate Certificate Uses", of this CP/CPS.

1.6 Policy Administration

1.6.1 Organization Administering the Document

Federal Department of Justice and Police

Federal Office of Police, fedpol

1.6.2 Contact Person

National PKI Coordinator

Federal Office of Police, fedpol

E-mail: eac-spoc.che@fedpol.admin.ch

1.6.3 Person Determining CPS Suitability for the Policy

The National PKI Coordinator determines the CP/CPS suitability.

1.6.4 CPS approval procedures

The National PKI Coordinator SHALL submit the CP/CPS at least to the Reviewers; further non-official reviewers MAY be requested for an opinion.

A verification protocol SHALL be produced allowing for the CP/CPS approval, and further showing, that no major findings were left unaddressed.

Final approval is issued by the National PKI Coordinator together with the CSCA Owner / Supervisor.

2 PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 Repositories

The Swiss Federal Repository: The Swiss Government PKI SHALL store and MAY publish either some or all public objects generated and authenticated by the Swiss CSCA. The Swiss CSCA CRL SHALL be published.

The Swiss eDoc PKD MAY publish but SHALL store and SHALL keep an up-to-date replica of the Swiss CSCA public objects (i.e. CSCA, DS, VDSS and ML certificates, Swiss CSCA CRL, etc.).

The published Swiss CSCA public objects SHALL be accessed through the https protocol on

```
https://www.bit.admin.ch/bit/en/home/subsites/allgemeines-zur-swiss-
government-pki/rootzertifikate/swiss-country-signing-certification-
authority--csca-.html
```

Further the Swiss CSCA CRL SHALL be accessed through the http protocol on

```
https://www.pki.admin.ch/crl/csca-switzerland-2.crl
```

2.2 Publication of Certification Information

The Swiss CSCA SHALL publish this CP/CPS and SHALL guarantee the Swiss CSCA compliance to this CP/CPS.

This CP/CPS MAY be retrieved through the following link:

```
https://www.pki.admin.ch/policy/CPS_2_16_756_1_17_3_62_1.pdf
```

2.3 Time or Frequency of Publication

The Swiss CSCA SHALL publish this CP/CPS if and only if any change occurs to either this CP/CPS or to the entities involved by this CP/CPS.

2.4 Access Controls on Repositories

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

3 Identification and Authentication

This section is dedicated to the identification and authentication of the Swiss CSCA Subscribers.

3.1 Naming

3.1.1 Types of Names

The Swiss CSCA SHALL have following Distinguished Name:

DN:

```
C=CH, O=Admin, OU=Services, OU=Certification Authorities,
CN=csca-switzerland-2
```

The Swiss CSCA SHALL only generate and SHALL sign Subscriber's Certificates and Certificate Requests identified by the following Distinguished Names (DN)

- o DS (Document Signer eMRTD)

   DN :
   ```
    C=CH, O=Admin, OU=Services, OU=DS, OU=PP, CN=<common-name>
   where
   <common-name> :== « PS3 » <2 digit number>, uniquely identifying the
   Document Signer
   ```

- o DS (Document Signer Residence Permit)

   DN :
   ```
   C=CH, O=Admin, OU=Services, OU=DS, OU=RP, CN=<common-name>
   where
   <common-name> :== « PS3 » <2 digit number>, uniquely identifying the
   Document Signer
   ```

- o VDSS (Visual Digital Seal Signer)

   DN :
   ```
   C=CH, CN=VS
   ```

- o ML-Signer (Master-List Signer)

   DN :
   ```
   C=CH, O=Admin, OU=Services, OU=MLS, CN= CSCA-MasterListSigner
   ```

- o SPOC TLS Server

   DN :
   ```
   C=CH, O=Admin, OU=SPOC, CN=SPOC TLS Server
   ```

- o SPOC TLS Client

   DN :
   ```
   C=CH, O=Admin, OU=SPOC, CN=SPOC TLS Client
   ```

3.1.2 Need for Names to be Meaningful

The Swiss CSCA names SHALL be meaningful, human readable and SHALL comply with the requirements of [Doc9303].

3.1.3 Anonymity or Pseudonymity of Subscribers

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

3.1.4 Rules for Interpreting Various Name Forms

No stipulation.

3.1.5 Uniqueness of Names

The Swiss CSCA SHALL enforce the uniqueness of the names used and or applied in the Swiss CSCA PKI.

3.1.6 Recognition, Authentication, and Role of Trademarks

No stipulation.

3.2 Initial Identity Validation

3.2.1 Method to Prove Possession of Private Key

- Swiss CSCA, ML-Signer
  The Swiss Government PKI Personnel together with an authorised representative of the National PKI Coordinator SHALL generate a Public Key and a Private Key, together with a Certificate Signing Request (CSR) for the Public Key to be certified. The CSR SHALL be signed by the Private Key.

- DS and VDSS
  The Swiss Government PKI Personnel together with an authorised representative of the respective Certificate owner (as defined in Table 3: Certificate owners) SHALL generate a Public Key and a Private Key, together with a Certificate Signing Request (CSR) for the Public Key to be certified. The CSR SHALL be signed by the Private Key.

- SPOC TLS Server and Client
  The Swiss Government PKI Personnel SHALL generate a Public Key and a Private Key, together with a Certificate Signing Request (CSR) for the Public Key to be certified. The CSR SHALL be signed by the Private Key.

3.2.2 Authentication of Organization Identity

The Organisation Identity SHALL be authenticated against the Distinguished Names as defined in 3.1.1 "Types of Names".

3.2.3 Authentication of Individual Identity

No stipulation.

3.2.4 Non-Verified Subscriber Information

Non-Verified or Non-Verifiable Subscribers MUST NOT be allowed.

3.2.5 Validation of Authority

No stipulation.

3.2.6 Criteria for Interoperation

No stipulation.

3.3 Identification and Authentication for Re-Key Requests

3.3.1 Identification and Authentication for Routine Re-Key

Refer to 3.2.1 "Method to Prove Possession of Private Key".

3.3.2 Identification and Authentication for Re-Key after Revocation

Refer to 3.2.1 "Method to Prove Possession of Private Key".

3.4 Identification and Authentication for Revocation Request

The National PKI Coordinator SHALL identify the Revocation Request for any Swiss CSCA's Subscriber through the Distinguished Name, the Serial Number and the Fingerprint of the Object to be revoked.

4 Certificate Life Cycle Operational requirements

4.1 Certificate Application

4.1.1 Who can submit a Certificate Application

The Swiss Government PKI Personnel authorised for that purpose SHALL submit a request.

The Submission SHALL be carried out under the presence of the "Owner" (as defined in 4.1.2).

4.1.2 Enrolment Process and Responsibilities

The Swiss CSCA Operating Manuals [OPMAN], [OPMAN1], [OPMAN2], [OPMAN3] and [OPMAN4] SHALL describe and define all Processes related to the Swiss CSCA.

The enrolment SHALL be carried out by the Swiss Government PKI Personnel and under the supervision of the certificate owner according to Table 3.

Certificate	Definition	Owner
CSCA Self-signed	Swiss Country Signer, Self-signed Certificate	National PKI-Coordinator
CSCA Link	Swiss Country Signer, Link Certificate	National PKI-Coordinator
ML-Signer	Master List Signer Certificate – Issuer of the Swiss Master List	National PKI-Coordinator
DS	Document Signer Certificate – Signer of the Swiss eMRTDs	fedpol
DS	Document Signer Certificate – Signer of the Swiss Residence Permits	SEM
VDSS	Visible Digital Seal Signer Certificate – Signer of the Swiss Visible Digital Seals for Non-Electronic Documents	SEM
Swiss CSCA CRL	Swiss CSCA Certificate Revocation List	National PKI-Coordinator
SPOC TLS Client	SPOC Communication Certificate, Client side	Swiss Government PKI
SPOC TLS Server	SPOC Communication Certificate, Server side	Swiss Government PKI

Table 3: Certificate owners

4.2 Certificate Application Processing

4.2.1 Performing Identification and Authentication Functions

The Swiss Government PKI Security Officer SHALL verify the identity of the involved representatives and SHALL confirm their role.

The verification SHALL be recorded in a protocol.

4.2.2 Approval or Rejection of Certificate Applications

The Certificate Application SHALL be approved if and only if ALL the following rules are verified:

- The Application SHALL be submitted by an authorised representative (refer to 4.1.1)
- The Possession of the Key Pair SHALL be proved (refer to 3.2.1)
- The Distinguished Names (DN) of the Certificate Application SHALL be defined according to 3.1 "Naming".

4.2.3 Time to Process Certificate Applications

A Certificate application SHALL be processed by the Swiss Government PKI Personnel within 4 days, once the Certificate Request has been approved.

4.3 Certificate Issuance

4.3.1 Swiss CSCA Actions during Certificate Issuance

The Swiss Government PKI Personnel SHALL log and SHALL confirm the issuance of any new Swiss CSCA Subscriber Certificate.

The issuance process SHALL be carried out according to [OPMAN], [OPMAN1].

4.3.2 Notification to Subscriber and Relying Parties by the Swiss CSCA of Issuance of Certificate

The Swiss CSCA Certificate Issuance SHALL be notified to Swiss CSCA Subscribers and the national Relying Parties.

The Swiss CSCA Certificate Issuance SHALL be notified to the EU Commission and the ICAO PKD Service.

The Swiss CSCA Certificate Issuance MAY be notified to non-national Relying Parties according to a non-exhaustive list maintained by the Swiss eDoc PKD.

The Swiss CSCA Subscriber's Certificate Issuance MAY be notified to Relying Parties according to a non-exhaustive list maintained by the Swiss eDoc PKD.

4.4 Certificate Acceptance

4.4.1 Conduct Constituting Certificate Acceptance

4.4.1.1 Swiss CSCA Self-signed and Link Certificates

The National PKI Coordinator SHALL verify the Swiss CSCA Self-signed and Link Certificates after their issuance according to the certificate profile specified in [Doc9303] AND according to the defined certificate parameters.

The National PKI Coordinator SHALL accept the Swiss CSCA Self-signed and Link Certificates after the successful verification.

4.4.1.2 Swiss DS Certificates

The National PKI Coordinator SHALL verify the eMRTD's and RP's DS Certificates after their issuance according to the certificate profile specified in [Doc9303] AND according to the defined certificate parameters.

The National PKI Coordinator SHALL accept the eMRTD's and RP's DS Certificates after the successful verification.

4.4.1.3 Swiss VDSS Certificates

The National PKI Coordinator SHALL verify the VDSS Certificates after their issuance according to the certificate profile specified in [Doc9303] AND according to the defined certificate parameters.

The National PKI Coordinator SHALL accept the VDSS Certificates after the successful verification.

4.4.1.4 Swiss ML-Signer Certificates

The National PKI Coordinator SHALL verify the ML-Signer Certificates after their issuance according to the certificate Profile specified in [Doc9303].

The National PKI Coordinator SHALL accept the ML-Signer Certificates after the successful verification.

4.4.1.5 SPOC TLS Server and Client Certificates

The Swiss Government PKI SHALL verify the SPOC TLS Server and Client Certificates after their issuance according to the certificate Profile specified in [CSN369791] AND according to the defined certificate parameters.

The Swiss Government PKI SHALL accept the SPOC TLS Server and Client Certificates after the successful verification.

4.4.2 Publication of the Certificate by the Swiss CSCA

The Swiss CSCA SHALL publish the Swiss CSCA Self-signed and Link Certificates in the repositories defined in 2.1 "Repositories".

The Swiss eDoc PKD SHALL store and MAY publish a copy of the Swiss Self-signed and Link Certificates according to its own rules.

4.4.3 Notification of Certificate Issuance by the Swiss CSCA to Other Entities

The National PKI Coordinator SHALL notify the International Entities (i.e. EU Commission, ICAO PKD Service), of the Issuance of a Swiss CSCA Self-signed and Link Certificates.

The National PKI Coordinator MAY notify other Entities of the Issuance of a Swiss CSCA Self-signed and Link Certificates.

The National PKI Coordinator MAY notify the other Entities of the Issuance of a Swiss CSCA Subscriber's Certificate.

If the Notification of Certificate Issuance is required, it MAY be carried out through diplomatic channels as defined in [Doc9303].

4.5 Key Pair and Certificate Usage

4.5.1 Subscriber Private Key and Certificate Usage

The Subscriber to the Swiss CSCA SHALL use the private keys and certificates as specified in 1.5 "Certificate Usage".

4.5.2 Relying Party Public Key and Certificate Usage

Relying parties SHALL use public keys, certificates and CRL to verify the authenticity and validity of Swiss CSCA signed objects.

Relying parties MAY use the Public Key and Certificates issued by the Swiss CSCA according to 1.5 "Certificate Usage".

4.6 Certificate Renewal

4.6.1 Circumstance for Certificate Renewal

The Swiss CSCA Certificate Renewal SHALL occur under extreme circumstances only, such as required either by modified security requirements or by compromise of the Swiss CSCA.

The Swiss CSCA Subscriber Certificate renewal MAY occur for impellent organisational or operational requirements.

4.6.2 Who May Request Renewal

The Renewal of the Swiss CSCA Certificate SHALL be requested, in extreme conditions, by the National PKI Coordinator.

Only the Owner of a Swiss CSCA Subscriber Certificate (according to Table 3) SHALL be authorised to request a renewal of its certificate.

4.6.3 Processing Certificate Renewal Requests

Each Renewal Request SHALL be verified and confirmed by the Swiss Government PKI and by the National PKI Coordinator.

The processing of a Swiss CSCA Renewal SHALL be carried out according to 4.3 "Certificate Issuance".

The Renewal Request SHALL be accompanied by an exhaustive document describing the reason.

4.6.4 Notification of New Certificate Issuance to Subscriber

Refer to 4.3.2 "Notification to Subscriber and Relying Parties by the Swiss CSCA of Issuance of Certificate".

4.6.5 Conduct constituting acceptance of a renewal certificate

Refer to 4.2.2 "Approval or Rejection of Certificate Applications".

4.6.6 Publication of the renewal certificate by the Swiss CSCA

Refer to 4.4.2 "Publication of the Certificate by the Swiss CSCA".

4.6.7 Notification of certificate issuance by the Swiss CSCA to Other Entities

Refer to 4.4.3 "Notification of Certificate Issuance by the Swiss CSCA to Other Entities".

4.7 Certificate Re-Key

4.7.1 Circumstance for Certificate Re-Key

The expiration of the validity period of the Swiss CSCA Private Key SHALL trigger the CSCA Re-Key.

The Swiss CSCA Re-Key MAY take place in case the specifications require modifications to the Swiss CSCA's certificate profile.

The Swiss CSCA Re-Key MAY take place to enforce augmented security requirements.

4.7.2 Who May Request Certification of a New Public Key

The Swiss Government PKI and National PKI Coordinator MAY request the certification of a New Swiss CSCA public key.

The Request SHALL be accompanied by an exhaustive document describing the reason.

4.7.3 Processing Certificate Re-Keying Requests

Processing of the Swiss CSCA Re-Keying SHALL be performed according to [OPMAN].

4.7.4 Notification of New Certificate Issuance to Relying Parties

The New Certificate Issuance SHALL be notified to the EU Commission and the ICAO PKD Service according to [Doc9303].

The New Certificate Issuance MAY be notified to Relying Parties according to a non-exhaustive list maintained by the Swiss eDoc PKD.

4.7.5 Conduct Constituting Acceptance of a Re-Keyed Certificate

Refer to 4.4.1 "Conduct Constituting Certificate Acceptance".

4.7.6 Publication of the Re-Keyed Certificate by the Swiss CSCA

The Swiss CSCA SHALL publish the Re-keyed Certificate in the repositories defined in 2.1 "Repositories".

The Swiss eDoc PKD SHALL store and MAY publish a copy of the Re-Keyed Certificate.

4.7.7 Notification of Certificate Issuance by the Swiss CSCA to Other Entities

According to the international rules [Doc9303], the Issuance of a New CSCA Certificate SHALL be notified at least 90 days before the rollover will occur.

4.8 Certificate Modification

4.8.1 Circumstance for Certificate Modification

A Certificate Modification MAY occur in case of

- a change in the international rules [Doc9303] or in case of
- an operational requirement by the Swiss CSCA and its Subscribers.

4.8.2 Who May Request Certificate Modification

Refer to 4.7.2 "Who May Request Certification of a New Public Key".

4.8.3 Processing Certificate Modification Requests

Refer to 4.7.3 "Processing Certificate Re-Keying Requests".

4.8.4 Notification of New Certificate Issuance to Relying-Parties

Refer to 4.7.4 "Notification of New Certificate Issuance to Relying Parties".

4.8.5 Conduct Constituting Acceptance of Modified Certificate

Refer to 4.4.1 "Conduct Constituting Certificate Acceptance".

4.8.6 Publication of the Modified Certificate by the Swiss CSCA

Refer to 4.7.6 "Publication of the Re-Keyed Certificate by the Swiss CSCA".

4.8.7 Notification of Certificate Issuance by the Swiss CSCA to Other Entities

Refer to 4.7.7 "Notification of Certificate Issuance by the Swiss CSCA to Other Entities".

4.9 Certificate Revocation and Suspension

A Swiss CSCA Certificate or Subscriber's Certificate Revocation SHALL occur under extreme circumstances only.

4.9.1 Circumstances for Revocation

The Swiss CSCA MAY revoke ANY Subscriber in case of a major incident like a key compromise.

4.9.2 Who can Request Revocation

The Revocation Request for the Swiss CSCA SHALL be submitted by the National PKI Coordinator.

A Revocation Request for a Swiss CSCA Subscriber MAY be submitted by the Swiss CSCA Subscriber's Certificate Owner or by the National PKI Coordinator.

4.9.3 Procedure for Revocation Request

The Revocation of the Swiss CSCA SHALL be verified and extensively documented.

4.9.4 Revocation Request Grace Period

No stipulation.

4.9.5 Time within which CA Must Process the Revocation Request

The processing of a Revocation Request for a Swiss CSCA Subscriber SHALL not be delayed further than 48 hours after the Revocation Requests has been submitted.

The Swiss CSCA SHALL process a Revocation Request at the latest a maximum of 72 hours after a Revocation Request has been submitted.

4.9.6 Revocation Checking Requirement for Relying Parties

A National Swiss CSCA's Relying Party SHALL check the status of any Swiss CSCA Certificate on which it relies toward the Swiss CSCA CRL.

4.9.7 CRL Issuance Frequency

The Swiss CSCA MUST issue at least one Swiss CSCA CRL every 90 days, even if no certificates have been revoked since the previous Swiss CSCA CRL was issued.

The Swiss CSCA CRL MAY be issued more frequently than every 90 days, but not more frequently than every 48 hours.

4.9.8 Maximum Latency for CRLs (if applicable)

The Swiss CSCA SHALL publish its CRL at the latest a maximum of 24 hours after issuance.

4.9.9 On-Line Revocation/Status Checking Availability

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

4.9.10 On-Line Revocation Checking Requirements

Refer to 4.9.6 "Revocation Checking Requirement for Relying Parties".

4.9.11 Other Forms of Revocation Advertisements Available

Refer to 4.7.4 "Notification of New Certificate Issuance to Relying Parties".

The Swiss CSCA CRL SHALL be further published under the ICAO PKD and according to the ICAO PKD rules. The publication SHALL be carried out under the control of the Swiss eDoc PKD.

4.9.12 Special Requirements Key Compromise

The Revocation of a Swiss CSCA certificate is both extreme and difficult. Upon informing a relying Party that a CSCA certificate has been revoked, all other certificates signed using the corresponding Swiss CSCA private key SHALL also be effectively revoked.

Refer also to [Doc9303]

4.9.13 Circumstances for Suspension

No stipulation.

4.9.14 Who can Request Suspension

No stipulation.

4.9.15 Procedure for Suspension Request

No stipulation.

4.9.16 Limits on Suspension Period

No stipulation.

4.10 Certificate Status Services

4.10.1 Operational Characteristics

The status of any Swiss CSCA Certificate and of any Swiss CSCA Subscriber's Certificate SHALL be available through the Swiss CSCA CRL.

4.10.2 Service Availability

The Swiss CSCA Certificate Status Service is available 24 x 7.

4.10.3 Optional Features

No stipulation.

4.11 End of Subscription

Any Swiss 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 Swiss CSCA MAY end the subscription of any Swiss CSCA Subscriber Certificate by:

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

4.12 Key Escrow and Recovery

4.12.1 Key Escrow and Recovery Policy and Practices

The Key Escrow for the Swiss CSCA and any Swiss CSCA Subscriber's SHALL be forbidden by this CP/CPS.

If applicable, a recovery SHALL be carried out by restoring a standard backup as defined in 6.2.4 "Private Key Backup".

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

The Key Encapsulation MUST NOT be allowed.

If applicable, the Recovery SHALL be carried out according to [OPMAN].

5 Facility, Management and Operational Controls

5.1 Physical Controls

5.1.1 Site Location and Construction

The Swiss CSCA is operated in the Swiss Government Federal Office of Information Technology, Systems and Telecommunication (FOITT) as well as in the premises or data centres of the producers of eMRTDs and Residence Permits.

The Swiss CSCA main central components SHALL be solely operated in Swiss Government PKI area.

The Swiss CSCA distributed components such as DS and VDSS MAY be operated in the premises or data centres of the producers of eMRTDs and Residence Permits.

The Swiss CSCA main central HSMs MAY be removed from Swiss Government PKI area if and only if the HSM devices have been decommissioned according to [DECO] and no cryptographic keys or parts of them can be read.

The Swiss CSCA distributed HSM components MAY be removed from the premises or data centres of the producers of eMRTDs and Residence Permits if and only if the HSM devices have been decommissioned according to [DECO].

5.1.2 Physical Access

Only persons belonging to the Swiss Government PKI and identifiable by name and bearing special badges MAY have access to the area housing the Swiss CSCA components.

Other persons (e.g. maintenance staff) MAY have access if and only if accompanied by authorised personnel; such access SHALL be logged.

Only a small number of persons identifiable by name SHALL have access to the area housing the distributed DS and VDSS components. An additional key SHALL be kept in a safe, to which a small number of persons have access.

Other persons MAY have access if and only if accompanied by authorised personnel. In addition, the area housing the distributed DS or VDSS components SHALL be under video surveillance.

5.1.3 Power and Air Conditioning

The areas (housing the Swiss CSCA, the DS and VDSS components) SHALL be equipped with an air conditioning system to regulate temperature and humidity.

All electrical components SHALL be connected to an UPS (uninterruptible power supply).

5.1.4 Water Exposures

The areas (housing the Swiss CSCA, the DS and VDSS components) SHALL be equipped with water sensors; latter SHALL be directly linked to the building's security control centre.

In the event of a water alarm, the aforementioned equipment SHALL be automatically shut down and the power supply SHALL be cut off.

5.1.5 Fire Prevention and Protection

The usual fire protection methods SHALL be applied according to the Swiss Fire Protections Rules.

Furthermore, the areas (housing the Swiss CSCA, the DS and VDSS components) shall be equipped with smoke sensors; latter SHALL be directly linked to the building's security control centre.

In the event of a fire alarm, the aforementioned equipment SHALL be automatically shut down and the power supply SHALL be cut off.

5.1.6 Media Storage

Data media containing information relating to the Swiss CSCA, including safety copies SHALL be kept at least in the Swiss Government PKI area in a fireproof safe.

5.1.7 Waste Disposal

The Waste Disposal SHALL be carried out according to [OPMAN].

5.1.8 Off-Site Backup

Sensible Swiss CSCA backup information SHALL be kept in at least two separate locations. The locations SHALL be geographically separated.

5.2 Procedural Controls

5.2.1 Trusted Roles

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

- National PKI Coordinator
  The National PKI Coordinator is responsible for all issues related to the Swiss CSCA and SHALL verify and coordinate all activities of the Swiss CSCA as well as its Subscribers. The National PKI Coordinator is also responsible for the Swiss CSCA notifications and SHALL further keep and manage the international relations to foreign CSCA and their Coordinators, as well as international organisations (i.e. ICAO, EU-Commission, etc.).

- Owner
  The Owner is responsible for generating, use and withdrawal of the objects issued by the Swiss CSCA under its control and for which he is responsible.

- Swiss Government PKI Personnel
  Inside the Swiss Government PKI the following roles SHALL be established:

  - PKI Security Officer
    The PKI Security Officer is responsible for enforcing compliance with all legal requirements, for the adherence to physical and functional security policies by Swiss Government PKI and its environment. He manages the physical access control to the certification platform. The security officer is the only one entitled to access, read archives, and analyse activity logs.

    He conducts reviews, at regular intervals of the compliance of the

services delivered by Swiss CSCA to this CP/CPS as well as to the Swiss Government PKI's detailed manuals and security policies.

- o Operating Team
  The Operating Team is responsible for running all services delivered by the Swiss Government PKI. In particular, its tasks are maintaining support contracts with suppliers; ensuring the availability of the certification infrastructure and co-ordinating Swiss Government PKI operations.
  The Operating Team also maintains the applications and the network supporting registration, issuance and revocation for/of certificates and other services provided by Swiss Government PKI.

5.2.2 Number of Persons Required per Task

With the exception of the standard operating tasks performed by the Operating Team, ALL security critical actions SHALL require two persons having different roles (refer to 5.2.1) to jointly execute the required operations.

These operations include, but are not limited to: generating, activating, deactivating, backing up and recovering, as well as destroying Swiss CSCA and Swiss CSCA Subscribers' keys in hardware security modules HSM, issuing, rekeying and revoking Swiss CSCA and Swiss CSCA Subscribers' certificates.

5.2.3 Identification and Authentication for Each Role

The Swiss CSCA and Swiss Government PKI Personnel SHALL be identified by their own national identity documents and their role SHALL be registered in [OPMAN4].

5.2.4 Roles Requiring Separation of Duties

The Swiss CSCA SHALL ensure the role separation by organisation. Therefore, the separation of duties is achieved by the presence of personnel belonging to different roles and hence organisations for the following tasks: issuance, renewal, rekeying and revoking of the Swiss CSCA.

For the tasks above, the "Separation of duties" inside the same organisation and role SHALL be forbidden by this CP/CPS.

5.3 Personnel Controls

5.3.1 Qualifications, Experience, and Clearance Requirements

The staff operating the Swiss CSCA SHALL belong to the FOITT, SHALL possess the necessary qualifications and experience to provide PKI services, and SHALL be employed full time by the Swiss Government PKI.

The employment contract of each staff member SHALL include a confidentiality clause. All Swiss CSCA members SHALL have undergone a personnel security check according to [PSPV].

Swiss Government PKI Personnel SHALL be familiar with the software, hardware and internal operational workflows of the certificate infrastructure components they work with.

The Swiss Government PKI and Swiss CSCA Personnel SHALL understand the involved processes and MUST understand the effects and implications of all actions taken.

5.3.2 Background Check Procedures

Swiss Government PKI and the Swiss CSCA Personnel SHALL be subject to a security review according to [PSPV] permitting the role assignment inside the Swiss CSCA.

5.3.3 Training Requirements

The Swiss Government PKI and Swiss CSCA Personnel SHALL be trained to fulfil the requirements of section 5.3.1 "Qualifications, Experience, and Clearance Requirements", of this CP/CPS.

5.3.4 Retraining Frequency and Requirements

The Swiss Government PKI Personnel SHALL at least retrain, either after a major system enhancement or after modifications in the organisation, methods or applied tools.

5.3.5 Job Rotation Frequency and Sequence

No Job Rotation SHALL be established.

5.3.6 Sanctions for Unauthorized Actions

Unauthorized actions by Swiss Government PKI Personnel MUST be sanctioned as regulated by the "Federal Act on the Responsibility of the Swiss Confederation, the Members of its Official Bodies and their Officers" [SR17232].

5.3.7 Independent Contractor Requirements

The Independent Contractors SHALL undergo the same requirements valid for the Swiss Federal Personnel.

5.3.8 Documentation Supplied to Personnel

This CP/CPS SHALL be supplied to ALL Personnel involved within the Swiss CSCA.

The Documents listed in section 10 "References", MAY be supplied to the Personnel involved with the Swiss CSCA.

5.4 Audit Logging Procedures

5.4.1 Types of Events Recorded

All relevant events related to the issuance and maintenance of Swiss CSCA entities MUST be logged either automatically or manually (journals, e.g. for recording entries to/exits from a protected room) for checking purposes, together with date/time, type, reason for and result of action, name of requester, name(s) of person(s) approving (where applicable).

5.4.2 Frequency of Processing Log

Log files are checked as part of a daily verification as per Swiss Government PKI's operating manual 'periodic monitoring of functions and activities'.

The Swiss Government PKI Personnel SHALL daily check and verify the logs and events recorded as specified in [OPMAN2].

5.4.3 Retention Period for Audit Log

ALL logs SHALL be retained for a period of at least ten years.

5.4.4 Protection of Audit Log

Audit Logs SHALL be secured on dedicated systems and if required MAY be signed by the Swiss Government PKI Personnel to guarantee their integrity.

5.4.5 Audit Log Backup Procedures

The Logs SHALL be backed up on a daily basis according to [OPMAN2].

5.4.6 Audit Collection System (Internal vs. External)

No stipulation.

5.4.7 Notification to Event-Causing Subject

The Event-Causing Subject SHALL be notified about all security relevant Events caused by his or her actions.

5.4.8 Vulnerability Assessments

The Swiss Government PKI SHALL at least guarantee to undertake, by appropriate means, a daily automatic security check of ALL components involved in the Swiss CSCA.

The results of the Vulnerability Assessment SHALL be documented.

5.5 Records Archival

5.5.1 Types of Records Archived

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

- the contractual agreements with providers,
- Swiss CSCA Self-signed and Link Certificates, DS, VDSS and ML-Signer Certificates issued by the Swiss CSCA,
- ALL CRLs issued by the Swiss CSCA,
- ALL Logs,
- ALL incident reports and
- ALL vulnerability analysis reports.

5.5.2 Retention Period for Archive

ALL Archives SHALL be retained for a period of at least ten years.

5.5.3 Protection of Archive

ALL Archives SHALL be encrypted.

5.5.4 Archive Backup Procedures

ALL Information to be backuped SHALL be copied to all backup system instances (refer also to 5.5.6).

5.5.5 Requirements for Time-Stamping of Records

ALL archived Records SHALL be provided of a Time Stamp. The Time Stamp SHALL be generated according to 6.8 "Time-Stamping".

5.5.6 Archive Collection System (Internal or External)

The Archive System SHALL be operated on a dedicated infrastructure.

The System SHALL be available in at least two geographically separated locations.

5.5.7 Procedures to Obtain and Verify Archive Information

The Swiss CSCA archived Information MAY be only retrieved by Swiss Government PKI Personnel and under the supervision of Swiss Federal Personnel authorised by the National PKI Coordinator.

5.6 Key Changeover

No stipulation.

5.7 Compromise and Disaster Recovery

5.7.1 Incident and Compromise Handling Procedures

The Swiss Government PKI SHALL notify all incidents to the National PKI Coordinator and MAY notify all, or some incidents to some Swiss CSCA Subscribers and Relying Parties.

The Swiss CSCA SHALL handle all incidents according to [OPMAN3].

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 Swiss Government PKI SHALL rely on the backup archives to recover the information.

In case of a major or critical incident or disaster, related to Computing Resources or Software the Swiss Government PKI SHALL recover the problem within a 72 hour period.

5.7.3   Entity Private Key Compromise Procedures

Swiss CSCA Compromise IS an extreme event. In case of a Swiss CSCA Key Compromise, following actions SHALL be undertaken:

- Revocation of ALL Swiss CSCA Subscriber's Certificates, through the generation of the Swiss CSCA CRL. The CRL SHALL include also ALL valid Swiss CSCA Self-signed and Link Certificates according to [Doc9303],

- Inform ALL Swiss CSCA Subscribers,

- Notify the Compromise according to 4.3.2 "Notification to Subscriber and Relying Parties by the Swiss CSCA of Issuance of Certificate",

- Generate and certify a new key pair for the Swiss CSCA,

- Issue new Swiss CSCA certificates to ALL Swiss CSCA Subscribers,

- Issue a new Swiss CSCA CRL.

In case of a Swiss CSCA Subscriber Key Compromise, the Swiss CSCA SHALL undertake following actions:

- Revoke the concerned Swiss CSCA Subscriber's Certificate and immediately issue a new Swiss CSCA CRL,

- Issue a new Swiss CSCA Subscriber Certificate and

- Notify ALL Swiss CSCA Subscribers and National Relying Parties of the Compromise and Issuance of the new certificate.

5.7.4   Business Continuity Capabilities after a Disaster

The Swiss Government PKI SHALL guarantee the disaster recovery of the Swiss CSCA within a 30 days' period at most.

5.8   Swiss CSCA Termination

No stipulation.

6 Technical Security Controls

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

The Swiss CSCA key pairs MUST be generated on a dedicated component complying with [FIPS140-2] Level 3.

The Subscribers Swiss CSCA Key pairs SHALL be generated on a dedicated component complying with [FIPS140-2] Level 3.

6.1.2 Private Key Delivery to Subscriber

The Private Key to be certified by the Swiss CSCA SHALL be generated at the Subscriber's premises.

Private Keys of the Swiss CSCA Subscribers MUST NOT be transferred.

6.1.3 Public Key Delivery to Certificate Issuer

The Public Key to be certified by the Swiss CSCA SHALL be submitted to the Swiss CSCA by the Subscriber through a standard Certificate Signing Request (CSR); the Request SHALL be generated at the Subscriber's premises according to [Doc9303].

6.1.4 Swiss CSCA Public Key Delivery to Relying Parties

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

The Swiss eDoc PKD SHALL distribute the Swiss CSCA certificates to National and International Instances according to its own rules.

6.1.5 Key Sizes

- CSCA:
  The CSCA key SHALL be based on brainpoolp384r1 and comply with [FIPS186-4].
  The EC parameters SHALL be given explicitly in the CA certificate, including the cofactor, as specified in [Doc9303].

- DS:
  The DS keys SHALL be based on elliptic curve brainpoolp256r1 and comply with [FIPS186-4].
  The EC parameters SHALL be given explicitly in the DS certificate, including the cofactor, as specified in [Doc9303].

- VDSS:
  The VDSS keys SHALL be based on elliptic curve brainpoolp256r1 and comply with [FIPS186-4].
  The EC parameters SHALL be given explicitly in the CA certificate, including the cofactor, as specified in [Doc9303].

- ML-Signer:
  The ML-Signer keys SHALL be based on elliptic curve brainpoolp256r1 and comply with [FIPS186-4].
  The EC parameters SHALL be given explicitly in the ML-Signer certificate, including the cofactor, as specified in [Doc9303].

- SPOC TLS Server and Client:
The SPOC TLS Server and Client keys SHALL be based on elliptic curve secp256r1.
The EC parameters MAY be given explicitly in the document signer certificate, including the cofactor, as specified in [Doc9303].

6.1.6 Public Key Parameters Generation and Quality Checking

The Public Keys and Parameters SHALL be verified by the National Security Authorities.

6.1.7 Key Usage Purposes (as per [Doc9303] key usage field)

The Key Usage Purposes of the CSCA Self-signed and Link Certificates, DS Certificate, VDSS Certificate and ML-Signer Certificate SHALL comply with [Doc9303].

The Key Usage Purposes of the SPOC TLS Server and Client Certificates SHALL comply with [CSN369791].

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic Module Standards and Controls

The Swiss CSCA and the Swiss CSCA Subscribers SHALL use security modules compliant with [FIPS 140-2] at least Level 3.

6.2.2 Private Key (n out of m) Multi-Person Control

The Swiss CSCA SHALL enforce a "3 out of 3" credentials requirement to generate the Swiss CSCA Private Key and sign the Swiss CSCA Subscribers' Certificates.

The Swiss CSCA SHALL enforce a "2 out of 3" credentials requirement to carry out a Swiss CSCA Backup.

6.2.3 Private Key Escrow

The Swiss CSCA MUST NOT escrow any Private Keys.

The Swiss CSCA's Subscribers MUST NOT escrow their respective Private Keys.

6.2.4 Private Key Backup

The Swiss CSCA Private Keys MUST be secured through a standard backup procedure as defined for the underlying HSM for the full HSM.

No Backup of any Subscribers' Private Keys SHALL be permitted.

6.2.5 Private Key Archival

The Swiss CSCA SHALL NOT archive its Private Keys.

The Swiss CSCA Subscribers SHALL NOT archive their respective Private Keys.

6.2.6 Private Key Transfer into or from a Cryptographic Module

The Swiss CSCA keys MAY be transferred between Cryptographic Modules for backup purposes only.

The conditions set in the sections 6.2.2 "Private Key (n out of m) Multi-Person Control" and 6.2.4 "Private Key Backup" MUST be applied.

6.2.7 Private Key Storage on Cryptographic Module

The Swiss CSCA SHALL enforce the storage of Private Keys on a HSM evaluated to at least [FIPS140-2] Level 3.

6.2.8 Method of Activating Private Key

The Swiss CSCA SHALL activate its Private Keys in accordance with the specifications of the HSM manufacturer.

Swiss CSCA Subscribers SHALL protect their Private Keys only.

6.2.9 Method of Deactivating Private Key

The Swiss CSCA Private Keys SHALL NOT be deactivated.

6.2.10 Method of Destroying Private Key

The Swiss CSCA Private Key SHALL either be deleted upon expiration or the Backup Tokens and the HSM SHALL be re-initialised according to the instructions of the HSM and tokens.

6.2.11 Cryptographic Module Rating

Refer to 6.2.1 "Cryptographic Module Standards and Controls".

6.3 Other Aspects of Key Pair Management

6.3.1 Public Key Archival

The Swiss CSCA and Swiss CSCA Subscribers' Public Keys SHALL NOT be archived.

Only the Swiss CSCA and Swiss CSCA Subscribers' Certificates MAY be archived.

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

6.3.2.1 Definitions

- Validity Period (Tval):
  for the Swiss CSCA and for the Swiss CSCA Subscribers, the validity period of the public and private keys, as well as of the CRL SHALL be expressed in days and MUST be positive.

- Lead-in Time:
  the Lead-in is the time between the beginning of the Validity Period of the Public Keys or Certificate and the beginning of the Validity Period of the Private keys and SHALL be expressed in days.

- Swiss CSCA Lead-in time (Tcal):
  the Lead-in Time of the Swiss CSCA MUST be zero days. Tcal = 0.

- Swiss CSCA Subscribers Lead-in time: (Tsbl)
  the Lead-in Time of the Swiss CSCA Subscribers MAY differ from zero days
  (if it differs from zero, it SHALL be positive).

- Document Validity (Tdval):
  is the Validity Period of a Swiss eMRTD or a Swiss Residence Permit and for
  the purpose of this CP/CPS MUST be expressed in days.

6.3.2.2 Private Key Validity Period

- The Private Key Validity period for the Swiss CSCA Self-signed is set to: 1'098 days

- The Private Key Validity period for the Swiss CSCA Link is set to: 1'098 days

- The Private Key Validity period for the DS is set to: 93 days

- The Private Key Usage Time for the VDSS is set: 366 days

- The Private Key Validity period for the ML-Signer is set to: 366 days

- The Private Key Validity period for the SPOC TLS Client is set to: 365 days

- The Private Key Validity period for the SPOC TLS Server is set to: 365 days

6.3.2.3 Certificate Validity Period

List of the abbreviations used in this section

Abbreviations	Description
Tval(CSCA-S)	Swiss CSCA Self-signed Certificate Validity Period in days
Tval(CSCA-L)	Swiss CSCA Link Certificate Validity Period in days
Tval(DS)	DS Certificate Validity Period in days
Tval(VDSS)	VDSS Certificate Validity Period in days
Tval(ML)	ML-Signer Certificate Validity Period in days
Tval(SPOC-TLS)	SPOC TLS Server and Client Certificate Validity Period in days
Tval(eMRTD)	Validity Period of the eMRTD Document
Tkpri(CSCA-S)	Swiss CSCA Self-signed Private Key Validity Period in days
Tkpri(CSCA-L)	Swiss CSCA Link Private Key Validity Period in days
Tkpri(DS)	DS Private Key Validity Period in days
Tkpri(ML)	ML-Signer Private Key Validity Period in days
Tsbl(DS)	Maximum allowed value for DS Lead-in time
Tkpri(VDSS)	VDSS Private Key Usage Time

Table 4: Abbreviations related to the validity period

The following values SHALL apply according to 6.3.2.2 "Private Key Validity Period":

- Tval(eMRTD) = 3'660 days

- Tkpri(CSCA-S) = 1'098 days

- Tkpri(CSCA-L) = 1'098 days

- Tkpri(DS) = 93 days

- Tkpri(ML) = 366 days

- Tsbl(DS) = 50 days

- Tkpri(VDSS) = 366 days

The Validity Period of the Swiss CSCA certificates is defined hereafter:

- **CSCA Self-signed**:
  The Validity Period of the Swiss CSCA Self-signed Certificate SHALL be computed through the following formula:

  Tval(CSCA-S) = Tkpri(CSCA-S) + Tkpri(DS) + Tsbl(DS) + Tval(eMRTD)

  Tval(CSCA-S) = 4'901 days

- **CSCA Link**:
  The Validity Period of the Swiss CSCA Link Certificate SHALL be by the following formula:

  Tval(CSCA-L) = Tkpri(CSCA-L)

  Tval(CSCA-L) = 1'098 days

- **DS**:
  The Validity Period of all the Swiss DS Certificate SHALL be computed through the following formula:

  Tval(DS) = Tsbl(DS) + Tkpri(DS) + Tval(eMRTD)

  Tval(DS) = 3'803 days

- **VDSS**:
  The Validity Period of all the Swiss VDSS Certificate SHALL be computed through the following formula:

  Tval(VDSS) = Tval(Visa) + 366 days

  Tval(VDSS) = 2'196 days

  NOTE: the VDSS will be used to sign the Visa during 365 days, then it SHALL be renewed. This rule allows for an overlap of at most 366 days between two VDSS certificates.

- **ML-Signer**:
  The Validity Period of the Swiss ML-Signer Certificate SHALL be computed through the following formula:

  Tval(ML) = Tsbl(DS) + Tkpri(ML) + Tval(eMRTD)

  Tval(ML) = 3'803 days

- **SPOC TLS Server and Client**
  The Validity Period of the Swiss SPOC TLS Server and Client Certificate SHALL be computed through the following formula

  Tval(SPOC-TLS) = Tkpri(SPOC-TLS)

  Tval(SPOC-TLS) = 365 days

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

The Swiss CSCA Activation Data SHALL be generated according to [OPMAN4].

6.4.2 Activation Data Protection

The Swiss CSCA Owners possessing parts of one or more HSMs' activation data SHALL keep this data locked at all times unless there is a HSM to be activated or deactivated.

ALL Swiss CSCA Subscribers SHALL NOT write down or copy certificate token PINs.

6.4.3 Other Aspects of Activation Data

No stipulation.

6.5 Computer Security Controls

6.5.1 Specific Computer Security Technical Requirements

The Swiss CSCA PKI SHALL use mandatory access control with all applications constituting the Swiss CSCA PKI services.

The Swiss CSCA SHALL enforce segregation of duties for ALL critical processes and system handling.

6.5.2 Computer Security Rating

No stipulation.

6.6 Life Cycle Technical Controls

6.6.1 System Development Controls

The Swiss Government PKI SHALL perform a risk analysis for each hardware or software component, which MAY be modified and/or added during the lifecycle of the Swiss CSCA.

The Swiss Government PKI SHALL operate a configuration management, which MUST ensure, that ONLY approved hardware and software MAY be deployed.

6.6.2 Security Management Controls

The Swiss Government PKI Personnel SHALL regularly verify the integrity of ALL the Swiss CSCA components.

6.6.3 Life Cycle Security Controls

No stipulation.

6.7   Network Security Controls

The Swiss CSCA Infrastructure SHALL be operated in a dedicated network-segment.

The Network segment of the Swiss CSCA SHALL be separated from ALL Swiss Federal internal and external connections.

6.8   Time-Stamping

The Swiss Government PKI SHALL provide an independent and reliable Time-Server. This Time-Server SHALL be applied for ALL activities related to the Swiss CSCA (i.e. issuing of certificates and CRLs, logs entries, etc.).

7   Certificate and CRL Profiles

7.1   Certificate Profile

The Swiss CSCA Self-signed and Link Certificates SHALL be generated according to the profile specified in [Doc9303].

The DS Certificates SHALL be generated according to the profile specified in [Doc9303].

The VDSS Certificates SHALL be generated according to the profile specified in [Doc9303].

The ML-Signer Certificates SHALL be generated according to the ML-Signer profile specified in [Doc9303].

The TLS Client Certificates SHALL be generated according to the SPOC TLS Client Certificate profile specified in [CSN369791].

The TLS Server Certificates SHALL be generated according to the SPOC TLS Server Certificate profile specified in [CSN369791].

7.1.1   Version Number(s)

The Version Number SHALL be set according to [Doc9303] or [CSN369791] according to 7.1.

7.1.2   Certificate Extensions

The Certificate Extensions SHALL comply with [Doc9303] or [CSN369791] according to 7.1.

7.1.3   Algorithm Object Identifiers

The Algorithm Object Identifiers for the CSCA Self-signed and Link Certificate, DS certificate, VDSS certificate and ML-Signer Certificate SHALL comply with [Doc9303].

The Algorithm Object Identifiers for the SPOC TLS Server and Client Certificates SHALL comply with [CSN369791].

The following list SHALL identify all Algorithms OIDs used under the Swiss CSCA responsibility:

- CSCA   ecdsa-with-SHA384
- DS   ecdsa-with-SHA384
- VDSS   ecdsa-with-SHA384
- ML-Signer   ecdsa-with-SHA384
- SPOC TLS Client   ecdsa-with-SHA384
- SPOC TLS Server   ecdsa-with-SHA384

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 Swiss CSCA Certificate Policy and Certification Practice Statement is uniquely identified by the following OID:

```
2.16.756.1.17.3.62.1
```

7.1.7 Usage of Policy Constraints Extension

No stipulation.

7.1.8 Policy Qualifiers Syntax and Semantics

No stipulation.

7.1.9 Processing Semantics for the Critical Certificate Policies Extension

The Processing Semantics for the Critical Certificate Policies Extension SHALL comply with [Doc9303].

7.2 CRL Profile

The Swiss CSCA Certificate Revocation List (CRL) SHALL be generated according to the profile specified in [Doc9303] and SHALL be signed by the Current Swiss CSCA for ALL revoked Swiss 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 and Other Assessments

8.1 Frequency or Circumstances of Assessment

The Swiss CSCA and the Swiss CSCA Subscribers SHALL be subject to a verification of their compliance with the requirements of this CP/CPS at least all 3 years.

8.2 Identity/Qualifications of Assessor

Auditors SHALL belong to the PKI Security Officers (refer to 5.2.1)
The National PKI Coordinator SHALL determine the Auditor.

8.3 Assessor's Relationship to Assessed Entity

The audits SHALL be conducted by the PKI Security Officers (refer to 5.2.1) mandated by the National PKI Coordinator.

The Auditor SHALL maintain a high standard of ethics required to ensure impartiality and the exercise of independent professional judgment.

8.4 Topics Covered by Assessment

The Swiss CSCA Assessment SHALL prove the adherence of the Swiss CSCA to this CP/CPS.

8.5 Actions Taken as a Result of Deficiency

The Swiss Government PKI and the Swiss CSCA SHALL undertake the necessary corrections to comply with this CP/CPS.

8.6 Communication of Results

The results MAY be communicated to the subscribers and relying parties by the National PKI Coordinator. No other entity SHALL communicate the results.

9 Other Business and Legal Matters

9.1 Term and Termination

9.1.1 Term

The Swiss CSCA Certificate Policy and Certification Practice Statement (i.e. this document), SHALL enter into force at the time of its publication.

9.1.2 Termination

The Swiss CSCA Certificate Policy and Certification Practice Statement (i.e. this document), SHALL be valid until

- it is either replaced by a newer revised version or
- the Swiss CSCA is forced to perform a Swiss CSCA renewal.

In case of a Swiss CSCA renewal, this CP/CPS SHALL remain valid at least until the last certificate issued by the Swiss CSCA is valid.

9.1.3 Effect of Termination and Survival

After expiration of this CP/CPS all regulations and data protection laws MUST still be observed.

9.2 Individual Notices and Communications with Participants

Changes to this CP/CPS SHALL be communicated to the Swiss CSCA Subscribers by e.g. email, but MAY be communicated to further Relying Parties.

The communication to Relying parties MAY be carried out as specified in 4.7.4 "Notification of New Certificate Issuance to Relying Parties".

9.3 Amendments

The National PKI Coordinator MAY revise this CP/CPS. Minor modifications, reviews, amendments or changes MAY be enacted at ANY time at the discretion of the National PKI Coordinator.

9.3.1 Notification Mechanism and Period

Amendments or changes to this CP/CPS SHALL be notified to the Swiss CSCA Subscribers at least 3 months before publication and MAY be notified to further Participants according to 4.7.4 "Notification of New Certificate Issuance to Relying Parties".

Spelling errors, typographical corrections, etc., which do not change the meaning of this CP/CPS SHALL be allowed without notification, but MAY be notified to all or some Participants according to 4.7.4 "Notification of New Certificate Issuance to Relying Parties".

9.3.2 Circumstances under Which OID Must be Changed

CP/CPS OIDs SHALL be changed if the National PKI Coordinator determines that a change in the CP/CPS modifies the level of trust provided by the CP/CPS.

9.4 Governing Law

This CP/CPS is subject to the applicable Swiss federal laws, in particular Article 6b(f) letter f of [SR1431] and implementing regulations.

10 References

References	
Identifier	**Title**
Doc9303	Doc 9303, Machine Readable Travel Documents, 8th Edition, 2021, Part 12: Public Key Infrastructure for MRTDs.
Doc9303VDS	Doc 9303, Machine Readable Travel Documents, 8th Edition, 2021, Part 13: Visible Digital Seals.
CSN369791	Information technology – Country Verifying Certification Authority Key Management Protocol for SPOC, ČSN 36 9791.
EUCCP	COMMON CERTIFICATE POLICY FOR THE EXTENDED ACCESS CONTROL INFRASTRUCTURE FOR PASSPORTS AND TRAVEL DOCUMENTS ISSUED BY EU MEMBER STATES, BSI TR-03139, V 2.4, 8 January 2021.
SR1431	SR 143.1, Bundesgesetz vom 22. Juni 2001 über die Ausweise für Schweizer Staatsangehörige (Ausweisgesetz, AwG).
SR17032	SR 170.32, Bundesgesetz vom 14. März 1958 über die Verantwortlichkeit des Bundes sowie seiner Behördenmitglieder und Beamten (Verantwortlichkeitsgesetz, VG).
PSPV	Verordnung über die Personensicherheitsprüfungen, vom 4. März 2011, SR 120.4 (Stand am 1. Januar 2021).
RFC2119	Key words for use in RFCs to Indicate Requirement Levels.
RFC3647	Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework.
FIPS186-4	NIST, Digital Signature Standard (DSS), July 2013.
FIPS140-2	NIST, SECURITY REQUIREMENTS FOR CRYPTOGRAPHIC MODULES, May 25, 2001.
ISO15408	ISO/IEC 15408, Information technology – Security techniques – Evaluation criteria for IT security.
OPMAN	EPASS PKI Betriebshandbuch. (confidential)
OPMAN1	DVI ISMS PKI Prozesse eDokumente. (confidential)
OPMAN2	Swiss Government PKI's operating manual 'Periodic Monitoring or Functions and Activities'. (confidential)
OPMAN3	DVI ISMS Incident Management Process. (confidential)
OPMAN4	EDOC Handling PKI Credential. (confidential)
DECO	eDoc PKI HSM Decommissioning Requirements. (confidential)

Table 5: References