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 Verifying CAs (Swiss CVCAs)

Author	Michael Zaugg, fedpol		
Publication date	**12.10.2023**		
Version	2.5		
Status	in process	under review	authorised for use
	☐	☐	☑

Roles

Reviewer	Markus Waldner, fedpol Andreas Häsler, SEM
Authorisation	Patrick Beer, Federal Office of Police, fedpol, National PKI Co-ordinator Roman Vanek, Federal Office of Police, fedpol Christian Rölli-Fässler, SEM

Authorisation

Place and date: Berne, 12.10.2023

Signed by:

Patrick Beer

Digital signature

Beer Patrick 4DK7EM
12.10.2023

Info: admin.ch/esignature | validator.ch

Roman Vanek

Digital signature

Vanek Roman NEPMQP

Digital unterschrieben von Vanek Roman NEPMQP
Datum: 2023.10.13 08:28:26 +02'00'

Version History			
Date	***Version***	***Author***	***Remarks***
19.08.2018	2.0	Arnaldo Cremisini, fedpol	First Release of Version 2
24.09.2018	2.1	Arnaldo Cremisini, fedpol	Revision based on reviewer's notes
19.07.2021	2.2	Nicolas Meuwly, Arnaldo Cremisini, fedpol	Revision Life-cycle and Reference to EU-CCP v2.4
16.08.2023	2.3	Nicolas Meuwly	Editorial revision
18.09.2023	2.4	Nicolas Meuwly	Revision based on reviewer's notes
29.09.2023	2.5	Michael Zaugg	Revision 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 the Swiss CVCAs and its Subscribers must adhere to when issuing and managing digitally signed objects.

Switzerland operates two separate Country Verifying Certification Authorities controlling the access rights to fingerprints stored in the Swiss documents supporting the EAC security feature.

This CP/CPS refers to the BSI TR-03139 Common Certificate Policy for the Extended Access Control Infrastructure for Passports and Travel Documents issued by the EU Member States, v2.4, 8 January 2021 [EUCCP].

1.2 Definitions and Acronyms

The keywords "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	The Certification Authority is an entity that issues digital certificates.
CP	The Certificate Policy is a document that aims to state the different actors of a public key infrastructure (PKI), their roles and duties.
CPS	The Certification Practice Statement is a Certificate Authority document describing their practice for issuing and managing public key certificates.
CVCA	Country Verifying Certification Authority as defined in [TR03110].
DV	Document Verifier: The Document Verifier is a sub-CA of the CVCA and controls the issuance of certificates as well as the access rights of the IS to the biometrics stored in the MRTDs.
EAC	Extended Access Control, security features protecting and restricting the access to biometrics stored in passports, Residence Permits etc.
eMRTD	Electronic Machine-Readable Travel Document (e.g., ePassport).
fedpol	Federal Office of Police of the Swiss Federal Department of Justice and Police.
FOITT	Federal Office of Information Technology, Systems and Telecommunication.

Acronym	Definition
IS	Inspection System: An Inspection System is both an organisation as well as an IT system responsible for the verification of documents.
National PKI Co-ordinator	The National PKI Co-ordinator is responsible for all issues related to the Swiss CVCA and coordinates the Swiss CVCA relations with foreign countries and international organisations.
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.
Swiss eDoc PKD	Swiss National Public-Key Directory. In the context of adopting biometric eMRTDs and Residence Permits, all required information will be stored in this system and be accessible to national participants only.
Swiss Government PKI	The Swiss organisation is responsible for operating the Swiss DV and IS under the supervision of the Swiss CVCA from fedpol.

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 Verifying Certification Authorities (Swiss CVCA).

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

2.16.756.5.55.1.2

2 eCP/CPS Statement

2.1 Responsibilities

a) The Swiss Federal Office of Police, fedpol, is responsible for the Swiss CVCA controlling the access to the fingerprints stored in the Swiss eMRTDs.

b) The Swiss State Secretariat for Migration, SEM, is responsible for the Swiss CVCA controlling the access to the fingerprints stored in the Swiss Residence Permits.

c) The Swiss CVCAs SHALL have one and only one Document Verifier (DV) enabled to act as a Subscriber to the National and Foreign CVCAs.
The Swiss Federal Office of Police, fedpol, is responsible for the Swiss DV controlling the access to the fingerprints stored in the Swiss and foreign documents supporting the EAC security feature.
The Swiss National Document Verifier (DV) SHALL only relate to the Swiss CVCA placed under the responsibility of the Swiss Federal Office of Police, fedpol (Maintaining CVCA) and controlling the Swiss IS access to the biometrics stored in the Swiss and foreign documents supporting the EAC security feature.

2.2 Policy Administration

2.2.1 Organisation Administering the Document

Federal Department of Justice and Police

Federal Office of Police, fedpol

2.2.2 Contact Person

National PKI Co-ordinator

Federal Office of Police, fedpol

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

2.2.3 Person Determining CPS Suitability for the Policy

The National PKI Co-ordinator determines the CP/CPS suitability.

2.2.4 CPS approval procedures

The National PKI Co-ordinator 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 Co-ordinator together with the CVCA Owners.

3 PUBLICATION AND REPOSITORY RESPONSIBILITIES

3.1 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 CVCAs.

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

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

`https://www.bit.admin.ch/bit/de/home/themen/swiss-government-pki/certificate-service-provider-csp/rootzertifikate.html`

3.2 Publication of Certification Information

The Swiss CVCAs SHALL publish this CP/CPS and SHALL guarantee the Swiss CVCA compliance with this CP/CPS.

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

`https://www.pki.admin.ch/policy/CPS_2_16_756_5_55_1_2.pdf`

The ISO 27001 Certificate MAY be retrieved through the following link:

`https://www.pki.admin.ch/iso/certificate-iso-27001.pdf`

3.3 Time or Frequency of Publication

The Swiss CVCA 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.

3.4 Access Controls on Repositories

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

4 Identification and Authentication

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

4.1 Naming

The Swiss CVCAs and DV SHALL be identified as follows:

a) The Swiss CVCA placed under the responsibility of the Federal Office of Police, fedpol, SHALL be identified through the following Mnemonics [TR03110]

`CVCA1PP`

b) The Swiss CVCA placed under the responsibility of the State Secretariat for Migration, SEM SHALL be identified through the following Mnemonics [TR03110]

`CVCA1RP`

c) The only Swiss DV related to the Swiss CVCA and controlling the Swiss IS access to the biometrics stored in the Swiss and foreign MRTDs SHALL be defined by the following Mnemonics [TR03110]

`DV1GEN`

4.2 Implementation

The Swiss CVCAs SHALL implement the [EUCCP].

5 Certificate Life-Cycle Operational requirements

5.1 Certificate Application

5.1.1 Who can submit a Certificate Application

The “Owner” of each CVCA (as defined in Table 2) SHALL submit a request.

The Submission SHALL be carried out under the presence of the Swiss Federal Office of Police Personal authorised for that purpose and the National PKI Co-ordinator.

5.1.2 Enrolment Process and Responsibilities

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

The enrolment SHALL be carried out by the “Owner” of each organisation according to Table 2: Owners

.

Certificate	Definition	Owner / Organisation
CVCA1PP	The Swiss Country Verifying Certification Authority for eMRTD’s	fedpol
CVCA1RP	The Swiss Country Verifying Certification Authority for Residence permits	SEM
DV	Document Verifier Authority	fedpol
IS	Inspection System Authority	fedpol

Table 2: Owners

5.2 Certificate Application Processing

5.2.1 Performing Identification and Authentication Functions

The Swiss Federal Office of Police Security Officers SHALL verify the involved representatives' identity and confirm their role.

The verification SHALL be recorded in a protocol.

5.2.2 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 5.1.2 “Enrolment Process and Responsibilities”)
- The Possession of the Key Pair SHALL be proved (refer to 5.1.2 “Enrolment Process and Responsibilities”)

- The Mnemonics of the Certificate Application SHALL be defined according to 4.1 “Naming”.

5.2.3 Time to Process Certificate Applications

A Certificate application SHALL be processed within seven days once the Certificate Request has been initiated.

5.3 Certificate Issuance

5.3.1 Swiss CVCA Actions during Certificate Issuance

The Swiss National PKI Co-ordinator SHALL confirm the issuance of any new Swiss CVCA and Subscriber Certificates.

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

5.3.2 Notification to Subscriber and Relying Parties by the Swiss CVCA of Issuance of Certificate

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

The Swiss CVCA Certificate Issuance SHALL be notified to the EU Commission.

The Swiss CVCA Certificate Issuance MAY be notified to non-national Relying Parties according to a non-exhaustive list maintained by the Swiss Federal Office of Police.

The Swiss CVCA Subscriber’s Certificate Issuance MAY be notified to Relying Parties according to a non-exhaustive list maintained by the Swiss Federal Office of Police.

5.4 Certificate Acceptance

5.4.1 Conduct Constituting Certificate Acceptance

5.4.1.1 Swiss CVCA Self-signed and Link Certificates

The National PKI Co-ordinator SHALL verify the Swiss CVCA Self-signed and Link Certificates after their issuance according to the certificate profile specified in the certificate parameters.

The National PKI Co-ordinator SHALL accept the Swiss CVCA Self-signed and Link Certificates after the successful verification.

5.4.1.2 Swiss DV Certificates

The National PKI Co-ordinator SHALL verify the DV Certificates after issuance according to the certificate profile specified in the certificate parameters.

The National PKI Co-ordinator SHALL accept the DV Certificates after the successful verification.

5.4.1.3 Swiss IS Certificates

The National PKI Co-ordinator SHALL verify the IS Certificates after their issuance according to the certificate profile specified in the certificate parameters.

The National PKI Co-ordinator SHALL accept the IS Certificates after the successful verification.

5.4.1.4 SPOC TLS Server and Client Certificates

The National PKI Co-ordinator SHALL verify the SPOC TLS Server and Client Certificates after 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.

5.4.2 Publication of the Certificate by the Swiss CVCA

The Swiss CVCA SHALL publish the Swiss CVCA Self-signed and Link Certificates as specified in [CSN369791].

5.4.3 Notification of Certificate Issuance by the Swiss CVCA to Other Entities

The National PKI Co-ordinator SHALL notify the International Entities (i.e., EU Commission, EU SPOC Members) of the Issuance of a new Swiss CVCA Self-signed and Link Certificates.

The National PKI Co-ordinator MAY notify other Entities of the Issuance of a Swiss CVCA Self-signed and Link Certificates.

If the Notification of Certificate Issuance is required, it MAY be carried out through diplomatic channels.

5.5 Key Pair and Certificate Usage

5.5.1 Subscriber Private Key and Certificate Usage

The Subscriber to the Swiss CVCA SHALL use the private keys and certificates as specified in [EUCCP].

5.5.2 Relying Party Public Key and Certificate Usage

Relying parties SHALL use public keys and certificates to access and read the fingerprints stored in the Swiss eMRTDs as specified in [EUCCP].

5.6 Certificate Renewal

5.6.1 Circumstance for Certificate Renewal

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

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

5.6.2 Who May Request Renewal

The Renewal of the Swiss CVCA Certificate SHALL be requested, in extreme conditions, by the CVCA owners as defined in Table 2: Owners

.

Only the Owner of a Swiss CVCA Subscriber Certificate (according to Table 2: Owners

) SHALL be authorised to request a renewal of its certificate.

5.6.3 Processing Certificate Renewal Requests

Each Renewal Request SHALL be verified and confirmed by the National PKI Co-ordinator.

The processing of a Swiss CVCA Renewal SHALL be carried out according to 5.3 “Certificate Issuance”.

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

5.6.4 Notification of New Certificate Issuance to Subscriber

Refer to 5.3.2 “Notification to Subscriber and Relying Parties by the Swiss CVCA of Issuance of Certificate”.

5.6.5 Conduct constituting acceptance of a renewal certificate

Refer to 5.2.2 “Approval or Rejection of Certificate Applications”.

5.6.6 Publication of the renewal certificate by the Swiss CVCA

Refer to 5.4.2 “Publication of the Certificate by the Swiss CVCA”.

5.6.7 Notification of certificate issuance by the Swiss CVCA to Other Entities

Refer to 5.4.3 “Notification of Certificate Issuance by the Swiss CVCA to Other Entities”.

5.7 Certificate Re-Key

5.7.1 Circumstance for Certificate Re-Key

The expiration date of the validity of the Swiss CVCA Private Key SHALL trigger the CVCA Re-Key.

The Swiss CVCA Re-Key MAY take place in case the specifications require modifications to the Swiss CVCA’s certificates.

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

5.7.2 Who May Request Certification of a New Public Key

The National PKI Co-ordinator MAY request the certification of a New Swiss CVCA public key.

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

5.7.3 Processing Certificate Re-Keying Requests

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

5.7.4 Notification of New Certificate Issuance to Relying Parties

The New Certificate Issuance SHALL be notified to the EU Commission [EUCCP].

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

5.7.5 Conduct Constituting Acceptance of a Re-Keyed Certificate

Refer to 5.4.1 “Conduct Constituting Certificate Acceptance”.

5.7.6 Publication of the Re-Keyed Certificate by the Swiss CVCA

The Swiss CVCA SHALL publish the Re-keyed Certificate in the repositories defined 3.1 “Repositories”.

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

5.8 Certificate Modification

5.8.1 Circumstance for Certificate Modification

A Certificate Modification MAY occur in case of

- a change in the international rules [EUCCP] or [TR03110] or in case of
- an operational requirement by the Swiss CVCA and its Subscribers.

5.8.2 Who May Request Certificate Modification

Refer to 5.7.2 “Who May Request Certification of a New Public Key”.

5.8.3 Processing Certificate Modification Requests

Refer to 5.7.3 “Processing Certificate Re-Keying Requests”.

5.8.4 Notification of New Certificate Issuance to Relying-Parties

Refer to 5.7.4 “Notification of New Certificate Issuance to Relying Parties”.

5.8.5 Conduct Constituting Acceptance of Modified Certificate

Refer to 5.4.1 “Conduct Constituting Certificate Acceptance”.

5.8.6 Publication of the Modified Certificate by the Swiss CVCA

Refer to 5.7.6 “Publication of the Re-Keyed Certificate by the Swiss CVCA“.

5.9 Certificate Revocation and Suspension

The Revocation of certificates is not possible within the EAC-PKI due to technical reasons.

There are two registration status of a CVCA, DV or IS. Their default registration status is not suspended;

The status of their registration is set to “suspended” by their own registration authority (for CVCA) or domestic / foreign parental registration authority (for DV and IS).

Certificates issued or certificate requests sent by a suspended CVCA, DV or IS SHALL NOT be trusted, proceed or forwarded.

5.9.1 Circumstances for a Suspension

A CVCA, DV or IS SHALL be suspended in case of:

- any incidents as key compromise or other security vulnerabilities
- being no longer conformant to the [EUCCP].

A DV or IS SHALL be also suspended if it is no longer allowed to apply for certificates of foreign Member States.

The Suspension MUST be processed by the SPOC, CVCAs and DV having registered the suspenden CVCA, DV or IS.

5.10 Key Escrow and Recovery

5.10.1 Key Escrow and Recovery Policy and Practices

Key Escrow for the Swiss CVCA and any Swiss CVCA Subscriber SHALL be forbidden by this CP/CPS.

If applicable, a recovery SHALL be performed by restoring a standard backup as defined in 7.2.4 “Private Key Backup”.

5.10.2 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].

6 Facility, Management and Operational Controls

6.1 Physical Controls

6.1.1 Site Location and Construction

The Swiss CVCA is operated in the Swiss Federal Department of Justice and Police (FDJP) and 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 CVCA main central components SHALL be solely run in the Swiss Federal Department of Justice and Police (FDJP) area.

The Swiss CVCA distributed components such as DV and IS MAY be operated in the premises or data centres of the Swiss Government Federal Office of Information Technology, Systems, and Telecommunication (FOITT).

The Swiss CVCA main central HSMs MAY be removed from the Swiss Federal Department of Justice and Police 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 CVCA 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].

6.1.2 Physical Access

Only persons belonging to the Swiss Federal Office of Police and identifiable by name and bearing special badges MAY have access to the area housing the Swiss CVCA 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 DV and IS components. An additional key SHALL be kept in a safe to which a limited 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 DV or IS components SHALL be under video surveillance.

6.1.3 Power and Air Conditioning

The areas (housing the Swiss CVCA, the DV, and IS components) SHALL be equipped with an air conditioning system to regulate temperature and humidity.

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

6.1.4 Water Exposures

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

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

6.1.5 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 CVCA, the DV, and IS components) shall be equipped with smoke sensors; the latter SHALL be directly linked to the building's security control centre.

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

6.1.6 Media Storage

Data media containing information relating to the Swiss CVCA, including safety copies, SHALL be kept at least in the Swiss Federal Office of Police area in a fireproof safe.

6.1.7 Waste Disposal

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

6.1.8 Off-Site Backup

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

6.2 Procedural Controls

6.2.1 Trusted Roles

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

- National PKI Co-ordinator
  The National PKI Co-ordinator is responsible for all issues related to the Swiss CVCA and SHALL verify and coordinate all activities of the Swiss CVCA and its Subscribers. The National PKI Co-ordinator is also responsible for the Swiss CVCA notifications and SHALL further keep and manage the international relations with foreign CVCA and their Co-ordinators, as well as international organisations (i.e., EU-Commission, etc.).
- Owner
  The Owner is responsible for generating, using and withdrawing the objects issued by the Swiss CVCA under its control and for which he is responsible.

- Swiss Federal Office of Police Personnel
  Inside the Swiss Federal Department of Justice and Police, 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 the Swiss Federal Office of Police 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 CVCA to this CP/CPS as well as to the Swiss Government Federal Department of Justice and Police detailed manuals and security policies.
  - Operating Team
    The Operating Team is responsible for running all services delivered by the Swiss Federal Department of Justice and Police PKI. In particular, its tasks are maintaining support contracts with suppliers, ensuring the availability of the certification infrastructure and coordinating Swiss Federal Office of Police 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 the Swiss Federal Office of Police PKI.

6.2.2 Number of Persons Required per Task

Except for the standard operating tasks performed by the Operating Team, all Tasks MUST be approved by three different persons who are employed in at least two different federal offices and who take on different roles (usually owner, security officer and operator).

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

6.2.3 Identification and Authentication for Each Role

The Swiss CVCA and Swiss Federal Office of Police PKI Personnel SHALL be identified by their own national identity documents, and their role SHALL be registered in [OPMAN4].

6.2.4 Roles Requiring Separation of Duties

The Swiss CVCA 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 CVCA.

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

6.3 Personnel Controls

6.3.1 Qualifications, Experience, and Clearance Requirements

The staff operating the Swiss CVCA SHALL be member either of the Swiss Federal Office of Police, the State Secretariat for Migration or of the FOITT. It SHALL possess the necessary qualifications and experience to provide PKI services. Members of FOITT SHALL be employed full-time by the Swiss Federal Government.

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

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

The Swiss Federal Office of Police PKI and Swiss CVCA Personnel SHALL understand the involved processes and MUST understand the effects and implications of all actions taken.

6.3.2 Background Check Procedures

Swiss Federal Department of Justice and Police PKI and the Swiss CVCA Personnel SHALL be subject to a security review according to [PSPV] permitting the role assignment inside the Swiss CVCA.

6.3.3 Training Requirements

The Swiss Federal Office of Police PKI and Swiss CVCA Personnel SHALL be trained to fulfil the requirements of section 6.3.1, “Qualifications, Experience, and Clearance Requirements” of this CP/CPS.

6.3.4 Retraining Frequency and Requirements

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

6.3.5 Job Rotation Frequency and Sequence

No Job Rotation SHALL be established.

6.3.6 Sanctions for Unauthorized Actions

Unauthorised actions by Swiss Federal Department of Justice and Police 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].

6.3.7 Independent Contractor Requirements

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

6.3.8 Documentation Supplied to Personnel

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

The Documents listed in section 11, “References”, MAY be supplied to the Personnel involved with the Swiss CVCA.

6.4 Audit Logging Procedures

6.4.1 Types of Events Recorded

All relevant events related to the issuance and maintenance of Swiss CVCA 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 the action, name of requester, name(s) of the person(s) approving (where applicable).

6.4.2 Frequency of Processing Log

Log files are checked as part of a daily verification as specified in the Swiss Federal Office of Police PKI’s operating manual ‘periodic monitoring of functions and activities’.

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

6.4.3 Retention Period for Audit Log

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

6.4.4 Protection of Audit Log

Audit Logs SHALL be secured on dedicated systems and, if required, MAY be signed by the Swiss Federal Office of Police PKI Personnel to guarantee their integrity.

6.4.5 Audit Log Backup Procedures

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

6.4.6 Audit Collection System (Internal vs. External)

No stipulation.

6.4.7 Notification to Event-Causing Subject

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

6.4.8 Vulnerability Assessments

The Swiss Federal Department of Justice and Police PKI SHALL at least guarantee to undertake, by appropriate means, a daily automatic security check of ALL components involved in the Swiss CVCA.

The results of the Vulnerability Assessment SHALL be documented.

6.5 Records Archival

6.5.1 Types of Records Archived

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

- the contractual agreements with providers,
- Swiss CVCA Self-signed and Link Certificates issued by the Swiss CVCA,
- ALL Logs,
- ALL incident reports and
- ALL vulnerability analysis reports.

6.5.2 Retention Period for Archive

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

6.5.3 Protection of Archive

ALL Archives SHALL be encrypted.

6.5.4 Archive Backup Procedures

ALL Information to be backed up SHALL be copied to all backup system instances (refer to 6.5.6 as well).

6.5.5 Requirements for Time-Stamping of Records

ALL archived Records SHALL be provided with a Time Stamp. The Time Stamp SHALL be generated according to 7.8 “Time-Stamping”.

6.5.6 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.

6.5.7 Procedures to Obtain and Verify Archive Information

The Swiss CVCA archived Information MAY be only retrieved by the Swiss Federal Office of Police PKI Personnel and under the supervision of Swiss Federal Personnel authorised by the National PKI Co-ordinator.

6.6 Key Changeover

No stipulation.

6.7 Compromise and Disaster Recovery

6.7.1 Incident and Compromise Handling Procedures

The Swiss Federal Department of Justice and Police PKI SHALL notify all incidents to the National PKI Co-ordinator and MAY notify all or some incidents to some Swiss CVCA Subscribers and Relying Parties.

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

6.7.2 Computing Resources, Software, and/or Data are Corrupted

In case of a major or critical incident or disaster related to Data Corruption, the Swiss Federal Office of Police 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 Federal Department of Justice and Police PKI SHALL recover the problem within 72 hours.

6.7.3 Entity Private Key Compromise Procedures

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

- Inform ALL Swiss CVCA Subscribers,
- Notify the Compromise according to 5.3.2 “Notification to Subscriber and Relying Parties by the Swiss CVCA of Issuance of Certificate”,
- Generate and certify a new key pair for the Swiss CVCA,
- Issue new Swiss CVCA certificates to ALL Swiss CVCA Subscribers,

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

- Revoke the concerned Swiss CVCA Subscriber’s Certificate and immediately issue a new Swiss CVCA Subscriber DV Certificate,
- Notify ALL Swiss CVCA Subscribers and National Relying Parties of the Compromise and Issuance of the new certificate.

6.7.4 Business Continuity Capabilities after a Disaster

The Swiss Federal Office of Police SHALL guarantee the disaster recovery of the Swiss CVCA within 30 days at most.

6.8 Swiss CVCA Termination

No stipulation.

7 Technical Security Controls

7.1 Key Pair Generation and Installation

7.1.1 Key Pair Generation

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

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

7.1.2 Private Key Delivery to Subscriber

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

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

7.1.3 Public Key Delivery to Certificate Issuer

The Public Key to be certified by the Swiss CVCA SHALL be submitted to the Swiss CVCA by the Subscriber through a specified Certificate Signing Request; the Request SHALL be generated at the Subscriber's premises according to this CP/CPS.

The Swiss SPOC distribute the Swiss CVCA certificates to National and International Instances according to its own rules.

7.1.4 Key Sizes

- CVCA:
  The CVCA key SHALL be based on the elliptic brainpoolp256r1 and comply with [FIPS186-4].
  The EC parameters SHALL be given explicitly in the CA certificate, including the cofactor, as specified in [TR03110].
- DV:
  The DV keys SHALL be based on the elliptic curve brainpoolp256r1 and comply with [FIPS186-4].

7.1.5 Public Key Parameters Generation and Quality Checking

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

7.2 Private Key Protection and Cryptographic Module Engineering Controls

7.2.1 Cryptographic Module Standards and Controls

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

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

The Swiss CVCA SHALL enforce a “n out of m” credentials requirement to generate the Swiss CVCA Private Key and sign the Swiss CVCA Subscribers’ Certificates.

The Swiss CVCA SHALL enforce a “2 out of 3” credentials requirement to carry out a Swiss CVCA Backup.

7.2.3 Private Key Escrow

The Swiss CVCA MUST NOT escrow any Private Keys.

The Swiss CVCA’s Subscribers MUST NOT escrow their respective Private Keys.

7.2.4 Private Key Backup

The Swiss CVCA 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.

7.2.5 Private Key Archival

The Swiss CVCA SHALL NOT archive its Private Keys.

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

7.2.6 Private Key Transfer into or from a Cryptographic Module

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

The conditions set in the sections 7.2.2 “Private Key (n out of m) Multi-Person Control” and 7.2.4 “Private Key Backup” MUST be applied.

7.2.7 Private Key Storage on Cryptographic Module

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

7.2.8 Method of Activating Private Key

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

Swiss CVCA Subscribers SHALL protect their Private Keys only.

7.2.9 Method of Deactivating Private Key

The Swiss CVCA Private Keys SHALL NOT be deactivated.

7.2.10 Method of Destroying Private Key

The Swiss CVCA 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.

7.2.11 Cryptographic Module Rating

Refer to 7.2.1 “Cryptographic Module Standards and Controls”.

7.3 Other Aspects of Key Pair Management

7.3.1 Public Key Archival

The Swiss CVCA and Swiss CVCA Subscribers’ Public Keys SHALL NOT be archived.

Only the Swiss CVCA and Swiss CVCA Subscribers’ Certificates MAY be archived.

7.3.2 Certificate Operational Periods and Key Pair Usage Periods

In the context of CVCA, the Certificate Operational Periods defines also the Key Pair Usage Periods.

7.3.2.1 Definitions

- Validity Period (Tval):
  For the Swiss CVCA and the Swiss CVCA Subscribers, the validity period of the public and private keys SHALL be expressed in days and MUST be positive.
- Lead-in Time:
  The Lead-in is the time between the end of the Validity Period of a precedent Public Key or Certificate and the beginning of the Validity Period of the new Public Key or Certificate and SHALL be expressed in days.
- Swiss CVCA Subscribers Lead-in time: (Tsbl)
  The Lead-in Time of the Swiss CVCA Subscribers MAY differ from zero days (if it differs from zero, it SHALL be positive).

7.3.2.2 Certificate Operational Periods

- The Certificate Operational Period of the Swiss CVCA Self-signed is set to: 1’095 days
- The Certificate Operational Period of the Swiss CVCA Link is set to: 1’095 days
- The Certificate Operational Period of the DV is set according to [EUCCP]

7.4 Activation Data

7.4.1 Activation Data Generation and Installation

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

7.4.2 Activation Data Protection

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

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

7.4.3 Other Aspects of Activation Data

No stipulation.

7.5 Computer Security Controls

7.5.1 Specific Computer Security Technical Requirements

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

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

7.5.2 Computer Security Rating

No stipulation.

7.6 Life Cycle Technical Controls

7.6.1 System Development Controls

The Swiss Federal Department of Justice and Police 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 CVCA.

The Swiss Federal Department of Justice and Police PKI SHALL operate a configuration management, which MUST ensure that ONLY approved hardware and software MAY be deployed.

7.6.2 Security Management Controls

The Swiss Federal Department of Justice and Police PKI Personnel SHALL regularly verify the integrity of ALL the Swiss CVCA components.

7.6.3 Life Cycle Security Controls

No stipulation.

7.7 Network Security Controls

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

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

7.8 Time-Stamping

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

8 Certificate Specifications

8.1 Certificate Specifications

The Swiss CVCA Self-signed and Link Certificates SHALL be generated according to the specifications specified in [EUCCP] and [TR03110].

The DV Certificates SHALL be generated according to the specifications specified in [EUCCP] and [TR03110].

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].

8.1.1 Version Number(s)

The Version Number of TLS -Client and -Server Certificates SHALL be set according to [Doc9303] or [CSN369791] according to 8.1.

8.1.2 Certificate Extensions

The Certificate Extensions of TLS -Client and -Server Certificates SHALL comply with [Doc9303] or [CSN369791] according to 8.1.

8.1.3 Algorithm Object Identifiers

The Algorithm Object Identifiers for the CVCA Self-signed and Link Certificate, DV certificate SHALL comply with [EUCCP] and [TR03110].

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

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

- CVCA ecdsa-with-SHA256
- DV ecdsa-with-SHA256

9 Compliance Audit and Other Assessments

9.1 Compliance Audit

The compliance of the Swiss CVCAs to this CP/CPS SHALL be guaranteed through regular assessments. The assessments SHALL comply with [EUCCP].

The Swiss Document Verifier (DV) identified by the Mnemonics `DV1GEN` SHALL be further submitted to an ISO 27001 certification.

9.2 Frequency or Circumstances of Assessment

The frequency and circumstances of the assessment SHALL comply with [EUCCP].

The frequency and circumstances of the Swiss Document Verifier (DV) assessment SHALL also comply with the ISO/IEC 27001 standard.

9.3 Identity/Qualifications of Assessor

The qualifications of the assessor SHALL comply with [EUCCP].

The qualifications of the assessor of the Swiss Document Verifier (DV) SHALL also comply with ISO/IEC 27001 standard.

9.4 Actions Taken as a Result of Deficiency

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

9.5 Communication of Results

The communication of results SHALL comply with [EUCCP].

The ISO 27001 certification of the Swiss Document Verifier (DV) identified by the Mnemonics `DV1GEN` SHALL be transmitted to the National PKI Co-ordinator, the national and foreign registered CVCAs, and the EU Commission and MAY be transmitted to further Relying Parties of the Swiss CVCAs.

10 Other Business and Legal Matters

10.1 Term and Termination

10.1.1 Term

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

10.1.2 Termination

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

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

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

10.1.3 Effect of Termination and Survival

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

10.2 Amendments

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

10.2.1 Circumstances under which OID Must be Changed

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

10.3 Governing Law

This CP/CPS is subject to the applicable Swiss Federal laws, in particular Article 6b(f) of [SR1431] and implementation regulations, as well as Article 41(6) of [SR14220].

11 References

References	
Identifier	***Title***
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.
RFC2119	Keywords for use in RFCs to Indicate Requirement Levels.
SR14220	SR 142.20, Bundesgesetz über die Ausländerinnen und Ausländer (Ausländergesetz, AuG).
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).
TR03110	TR-03110-1 Advanced Security Mechanisms for Machine Readable Travel Documents – Part 1, Version 2.10, BSI. TR-03110-3 Advanced Security Mechanisms for Machine Readable Travel Documents – Part 3, Version 2.10, BSI.

Table 3: References