



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	Arnaldo Cremisini, fedpol		
Publication date	24.08.2021		
Version	2.2		
Status	in process	under review	authorised for use
	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>

Roles

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

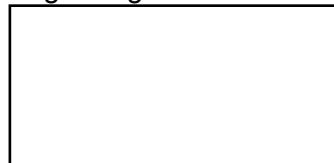
Authorisation

Place and date: Berne, 21.07.2021

Signed by:

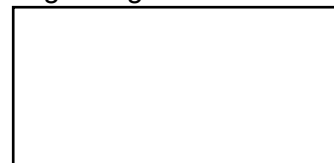
Patrick Beer

Digital signature



Roman Vanek

Digital signature



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

Table of Contents

<i>Certificate Policy (CP) and Certification Practice Statement (CPS) of the Swiss Country Verifying CAs (Swiss CVCAs)</i>	<i>1</i>
<i>1 Introduction</i>	<i>5</i>
<i>1.1 Overview</i>	<i>5</i>
<i>1.2 Definitions and Acronyms</i>	<i>5</i>
<i>1.3 Document Name and Identification</i>	<i>6</i>
<i>1.4 Policy Administration</i>	<i>6</i>
1.4.1 Organization Administering the Document	6
1.4.2 Contact Person	6
1.4.3 Person Determining CPS Suitability for the Policy	7
1.4.4 CPS approval procedures	7
<i>2 CP/CPS Statement</i>	<i>8</i>
<i>2.1 Responsibilities</i>	<i>8</i>
<i>2.2 Naming</i>	<i>8</i>
<i>2.3 Implementation</i>	<i>8</i>
<i>3 Compliance Audit and other Assessment</i>	<i>9</i>
<i>3.1 Compliance Audit</i>	<i>9</i>
<i>3.2 Frequency or Circumstances of Assessment</i>	<i>9</i>
<i>3.3 Identity/Qualifications of Assessor</i>	<i>9</i>
<i>3.4 Actions Taken as a Result of Deficiency</i>	<i>9</i>
<i>3.5 Communication of Results</i>	<i>9</i>
<i>4 PUBLICATION AND REPOSITORY RESPONSIBILITIES</i>	<i>10</i>
<i>4.1 Repositories</i>	<i>10</i>
<i>4.2 Publication of Certification Information</i>	<i>10</i>
<i>4.3 Time or Frequency of Publication</i>	<i>10</i>
<i>4.4 Access Controls on Repositories</i>	<i>10</i>
<i>5 Other Business and Legal Matters</i>	<i>11</i>
<i>5.1 Term and Termination</i>	<i>11</i>
5.1.1 Term	11
5.1.2 Termination	11
5.1.3 Effect of Termination and Survival	11
<i>5.2 Amendments</i>	<i>11</i>
5.2.1 Circumstances under which OID Must be Changed	11
<i>5.3 Governing Law</i>	<i>11</i>
<i>6 References</i>	<i>12</i>

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 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 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.
CVCA	Country Verifying Certification Authority as defined in [TR03110].
DV	Document Verifier: a 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 permit etc..
eMRTD	Electronic Machine Readable Travel Document (e.g. ePassport).
fedpol	Federal Office of Police of the Swiss Federal Department of Justice and Police.

Acronym	Definition
FOITT	Federal Office of Information Technology, Systems and Telecommunication.
IS	Inspection System: an Inspection System is both an organisation as well as an IT-system responsible for the verification of documents.
National PKI Coordinator	The National PKI Coordinator 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. Where, in the context of the adoption of biometric eMRTDs and Residence Permits, all required information will be accessible to national participants only. It is also responsible for the international distribution of the Swiss CVCA public objects.
Swiss Government PKI	Is the Swiss Organisation in charge of the Swiss PKI, moreover it is responsible for operating the Swiss CVCA and for the publication of the Swiss CVCA public entities such as certificates etc.

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:

2.16.756.1.17.3.72.1

1.4 Policy Administration

1.4.1 Organization Administering the Document

Federal Department of Justice and Police

Federal Office of Police, fedpol

1.4.2 Contact Person

National PKI Coordinator

Federal Office of Police, fedpol

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

1.4.3 Person Determining CPS Suitability for the Policy

The National PKI Coordinator determines the CP/CPS suitability.

1.4.4 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 CVCA Owners.

2 CP/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 MRTDs.
- 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 CVCA's SHALL have one and only one Document Verifier (DV) enabled to act as a Subscriber to the National and Foreign CVCA's.

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 and controlling the Swiss IS access to the biometrics stored in the Swiss and foreign documents supporting the EAC security feature.

2.2 Naming

The Swiss CVCA's 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

2.3 Implementation

The Swiss CVCA's SHALL implement the [EUCCP].

3 Compliance Audit and other Assessment

3.1 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.

3.2 Frequency or Circumstances of Assessment

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

The frequency and circumstances of the assessment of the Swiss Document Verifier (DV) SHALL also comply with the ISO/IEC 27001:2013 norm.

3.3 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 27001:2013 norm.

3.4 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.

3.5 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 Coordinator, the national and foreign registered CVCAs, the EU Commission and MAY be transmitted to further Relying Parties of the Swiss CVCAs.

4 PUBLICATION AND REPOSITORY RESPONSIBILITIES

4.1 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/en/home/subsites/allgemeines-zur-swiss-government-pki/rootzertifikate/swiss-country-verifying-certification-authority--cvca-/cvca-production.html>

4.2 Publication of Certification Information

The Swiss CVCAs SHALL publish this CP/CPS and SHALL guarantee the Swiss CVCA 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_72_1.pdf

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

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

4.3 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.

4.4 Access Controls on Repositories

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

5 Other Business and Legal Matters

5.1 Term and Termination

5.1.1 Term

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

5.1.2 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 last certificate issued by the Swiss CVCA is valid.

5.1.3 Effect of Termination and Survival

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

5.2 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.

5.2.1 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.

5.3 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].

6 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	Key words 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 2: References