Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Federal Department of Finance FDF

Federal Office of Information Technology, Systems and Telecommunication FOITT
Swiss Government PKI

NOT CLASSIFIED

Swiss Government PKI - Root CA IV - CP_CPS EN

Certificate Policy and Certification Practice Statement of the Swiss Government Root CA IV

Document OID : 2.16.756.1.17.3.5.0

V1.41, 03.09.2024

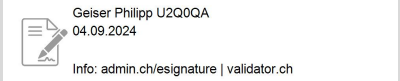
Classification *	Not classified
Status **	Released
Project Name	Swiss Government Root CA IV
Auftraggeber	PKI Director
Authors	Jürgen Weber, Daniel Stich, Cornelia Enke, Hans W. Kramer
Contributors	Cornelia Enke, Pascal Joye
Reviewers	PKI Management Board
Approved by	PKI Management Board
Distribution	Subscribers, Swiss Government PKI Employees, Auditors, Third Parties https://www.pki.admin.ch/cps/CPS_2_16_756_1_17_3_5_0.pdf
Doc_ID	0261-RV-CP-CPS Root_CA_IV_(2.16_756_1_17_3_5_0).docx
Short Description	Certificate Policy and Certification Practice Statement of the Swiss Government Root CA IV
Library	Certified PKI

* Nicht klassifiziert - Not classified, Intern - Internal, Vertraulich - Confidential
** In Arbeit - In Progress, In Prüfung - Being Reviewed , Freigegeben - Released, Abgeschlossen - Closed

Change History

Date	Version	Author	Description
2018/09/18	0.1	C.Enke, Jürgen Weber, Daniel Stich	Initial Version
2019/02/12	1.0	C.Enke	Finalization
2019/03/18	1.1	C.Enke	Introduction Regulated CA02
2019/05/10	1.1	C.Enke	Release of Version 1.1
2019/07/19	1.2	C.Enke	Introduction TW4S
2019/08/16	1.3	C.Enke	Adding E-Mail address for complaints
2021/01/05	1.31	C.Enke	Annual Review Update ETSI Standards Added Organization Authorization New Issuing CA Update CRL publication interval Adoption of new role model Implementation new design of Organization certificates for governmental institutions
2021/05/10	1.32	C.Enke	Added Policy OID for COVID-certificate Self issuing for staff members
2022/08/22	1.33	P. Joye	Added Policy OID : Regulated CA03 ZertES - qcp-l-hsm (HSM-1OU), OID 2.16.756.1.17.3.5.2.15
2022/09/14	1.34	HW Kramer	Annual Review
2022/09/22	1.35	P. Joye	Update Organization
2022/09/22	1.36	P. Joye	Update Organization
2022/11/23	1.37	HW Kramer	Prepare the finalization
2023/01/25	1.38	HW Kramer	Added comments from Stefanie Schäfer and fixes in table 1.
2023/01/25	1.39	HW Kramer	Final version
2023/03/23	1.40	HW Kramer	Surpress reason code in CRL.
2024/09/03	1.41	C.Enke	Clan up policy OIDs for issued certificates update reference table

Approval

Date	Version:	Signer 1	Signer 2
03.09.2024	1.41	 SG-PKI Trust Backend Product Owner Philipp Geiser	 SG-PKI Security Officer C.Enke

References

Identifier	Title, Source
[1]	**Minutes of Swiss Government Root CA IV root ceremony** Version: 1.0, Date: 02.12.2018 Source: Swiss Government PKI internal document[1]
[2]	**SR 943.03 Bundesgesetz über Zertifizierungsdienste im Bereich der elektronischen Signatur und anderer Anwendungen digitaler Zertifikate vom 18.03.2016 (Federal law on the certification services supporting electronic signatures and other applications of digital certificates ZertES)** Version: 1.1.2020, Status: in force since 01.01.2017 Source : http://www.admin.ch/ch/d/sr/c943_03.html
[3]	**SR 943.032 Verordnung über Zertifizierungsdienste im Bereich der elektronischen Signatur und anderer Anwendungen digitaler Zertifikate vom 23.11.2016 (Regulation on certification services supporting electronic signatures and other applications of digital certificates VZertES)** Version: 2.10.2020, Status: in force since 01.01.2017 Source: http://www.admin.ch/ch/d/sr/c943_032.html
[4]	**SR 943.032.1 Verordnung des BAKOM über Zertifizierungsdienste im Bereich der elektronischen Signatur und anderer Anwendungen digitaler Zertifikate vom 23.11.2016 (Ordinance of OFCOM for certification services supporting electronic signatures and other applications of digital certificates)** Version: 15.3.2022, Status: in force since 01.01.2017 Source: https://www.admin.ch/opc/de/classified-compilation/20162169/index.html
[5]	**Technical directive I006 'Structure of the Admin-Directory' by the Federal IT Steering Unit of 28.02.2007** Version: 2.02 , Status: in force since 05.11.2015 Source: https://www.bk.admin.ch/dam/bk/de/dokumente/dti/ikt-vorgaben/standards/i006/i006-admin-directory_v2-02_genehmigt_d.pdf.download.pdf/i006-admin-directory_v2-02_genehmigt_d.pdf
[6]	**Ordinance on Security Checks for Persons (OSCP) of 04.03.2011** Version: 01.01.2022, Status: in force since 01.01.2017 Source: https://www.admin.ch/opc/de/classified-compilation/20092321/index.html
[7]	**SR 170.32 Federal Act on the Responsibility of the Swiss Confederation, the Members of its Official Bodies and their Officers of 14.03.1958** Version: 1.11.2020, Status: in force since 01.01.1959 Source : https://www.admin.ch/opc/de/classified-compilation/19580024/index.html
[8]	**SR 172.010 Federal law on the Organization of Government and Administration (RVOG) of 21.03.1997** Version: 2.12.2019, Status: in force since 01.10.1997 Source : http://www.admin.ch/ch/d/sr/c172_010.html
[9]	**SR 172.215.1 Regulation on the Organization of the Federal Department of Finances (OVEFD) of 17.02.2010** Version: 01.1.2022, Status: in force since 01.03.2010 Source : http://www.admin.ch/ch/d/sr/c172_215_1.html
[10]	**SR 235.1 Federal Act on Data Protection (FADP) of 19.06.1992** Version: 01.03.2019, Status: in force since 01.07.1993 Source : https://www.admin.ch/opc/de/classified-compilation/19920153/index.html
[11]	**SR 235.11 Ordinance to the Federal Act on Data Protection of 14.06.1993** Version: 16.10.2012, Status: in force since 01.07.1993 Source : https://www.admin.ch/opc/de/classified-compilation/19930159/index.html

.

Identifier	Title, Source
[12]	**Frame contract between Subscriber and FOITT** (Swiss Government PKI as organizational unit of FOITT automatically honors such contracts) Version, Date : Frame contracts are individually entered between FOITT and customer Source: Swiss Government PKI internal document[1]
[13]	**Addendum to Frame contract between Subscriber and FOITT** Anhang zum Rahmenvertrag für Zertifikate der Swiss Government PKI Qualifizierte Zertifikate (Klasse A) (0084-RV-SGPKI-CLA-Anhang zum Rahmenvertrag.docx) Version: 1.1, Date: 30.06.2016 Source: Swiss Government PKI internal document[1]
[14]	**Swiss Government PKI security policy** (0027-RV-SG-PKI Betriebliche Sicherheitsprinzipien) Source: Swiss Government PKI internal document(filed with “BIT Kundenkontakte”)
[15]	**Swiss Government PKI access control directive** Source: Swiss Government PKI internal document[1]
[16]	**Swiss Government PKI manual on operation and organization** (Betriebshandbuch (BHB) / Organisationshandbuch (OHB) Certified PKI) Source: Swiss Government PKI internal document[1]
[17]	**Policy of Time Stamping Authority** Source: Swiss Government PKI internal document[1]
[18]	**Administration der SG-PKI LRA-Officer und RIO** (0100-RV-SGPKI-Administration der LRAOs und RIOs) Source: Swiss Government PKI internal document[1]
[19]	**Swiss Government PKI Registrierrichtlinien Klasse A - Qualifiziert** (0239-RV-Registrierrichtlinien Klasse A - Qualifiziert-d) Source: Swiss Government PKI internal document[1]
[20]	**Benutzervereinbarung und Nutzungsbedingungen Klasse A - qualifiziert** (0094-RV-Terms and Conditions Class A - qualified.docx) Source: Swiss Government PKI internal document[1]
[21]	**Guidelines zum Bezug von Zertifikaten der Klasse A - qualifiziert** (0096-RV-Guidelines Class A - qualified.docx) Source: Swiss Government PKI internal document[1]
[22]	**Swiss Government PKI Registrierrichtlinien Klasse A - geregelte Behördenzertifikate** (0228-RV-Registrierrichtlinien Klasse A – geregelte Behördenzertifikate) Source: Swiss Government PKI internal document[1]
[23]	**Benutzervereinbarung und Nutzungsbedingungen Klasse A - geregeltes Behördenzertifikat** (0263-RV-Terms and Conditions Class A - regulated authority certificate) Version 1.0 vom 03.04.2019 Source: Swiss Government PKI internal document[1]
[24]	**Guidelines zum Bezug von Zertifikaten der Klasse A - geregeltes Behördenzertifikat** (0264-RV-Guidelines Class A - regulated authority certificate) Source: Swiss Government PKI internal document[1]
[25]	**European REGULATION (EU) No 910/2014 on electronic identification and trust services on 23 July 2014** Source: https://ec.europa.eu/futurium/en/content/eidas-regulation-regulation-eu-ndeg9102014
[26]	**ETSI EN 319 401: General policy requirements for trust service providers (replaces TS 101 456 v1.4.3: Electronic Signatures and Infrastructures (ESI) – Certificate Policy and Certification Practices Framework)** Version: V3.1.1(2024-06)

Identifier	Title, Source
[27]	**ETSI EN 319 411-1: Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements** Version: V1.4.1 (2023-10)
[28]	**ETSI EN 319 411-2: Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates** Version: V2.5.1 (2023-10)
[29]	**ETSI EN 319 422: Electronic Signatures and Infrastructures (ESI);Time-stamping protocol and time-stamp token profiles** **(replaces TS 101 861 v1.3.1: Time Stamping Profile)** Version: V1.1.1, Status: published 2016-03
[30]	**ETSI EN 319 412-1: Electronic Signatures and Infrastructures (ESI);Certificate profiles; Part 1 Overview and common data structures** Version: V1.5.1, (2023-09)
[31]	**ETSI EN 319 412-2: Electronic Signatures and Infrastructures (ESI);Certificate profiles; Part 2: Certificate profile for certificates issued to natural persons** Version: V2.3.1, (2023-09)
[32]	**ETSI EN 319 412-3: Electronic Signatures and Infrastructures (ESI);Certificate profiles; Part 3: Certificate profile for certificates issued to legal persons** Version: V1.3.1, Status: (2023-09)
[33]	**ETSI EN 319 412-4: Electronic Signatures and Infrastructures (ESI);Certificate profiles; Part 4: Certificate profile for web site certificates** Version: V1.3.1, (2023-09)
[34]	**ETSI EN 319 412-5: Electronic Signatures and Infrastructures (ESI);Certificate profiles; Part 5: QCStatements** Version: V2.4.1, (2023-09)
[35]	**IETF RFC 3647: Internet X.509 Public Key Infrastructure – Certificate Policy and Certification Practices Framework** Version: 2003, Status: published November 2003
[36]	**IETF RFC 5280 (May 2008): Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile**
[37]	**Company Identification Number (CIN) - Unternehmens-Identifikationsnummer (UID)**
[38]	**Swiss Accreditation Service SAS**
[39]	**T.50 : International Reference Alphabet (IRA)**
[40]	**CEN EN-419 241-1** General Requirements
[41]	**CEN EN-419 241-2** Protection profile for QSCD for Server Signing
[42]	**CEN EN 419 221-5** Cryptographic Module
[43]	**Swiss Government CA Layout and Policies** 0040-RV-CA Layout and Policies
[44]	**Handlungsvollmacht zur Beantragung eines geregelten Behördenzertifikates der Klasse A**
[45]	**Technische und administrative Vorschriften über Zertifizierungsdienste im Bereich der elektronischen Signatur und anderer Anwendungen digitaler Zertifikate** Version 2:, 17. February 2022, Enforcement 15. March 2022
[46]	**CEN EN-419 211-2** Protection profiles for secure signature creation device - Part 2: Device with key generation

Table of Contents

List of Figures

List of Tables

1 Introduction

Swiss Government PKI (hereinafter referred to as "SG-PKI") operates a public key infrastructure on behalf of the Swiss government to enable secure electronic document exchange based on certificates for natural and legal persons. The service is primarily available for staff and bodies of the federal, cantonal and communal administrations of Switzerland, but is also extended to external natural or legal persons having a need for securing the document exchange with administrative bodies.

The Swiss Government PKI also issues certificates for themselves or their own purposes. The corresponding legal and / or certification requirements will be fulfilled.
The objectives, mandate and tasks of the SG PKI are based on Appendix 2 to the rules of procedure of the Federal Office of Information Technology, Systems and Telecommunication FOITT (legal basis in the FOITT (admin.ch)). The SG PKI itself is part of the Platform Services (PS) main division in the IAM Services business unit (BU IAM) of the FOITT.

1.1 Overview

1.1.1 SG-PKI

The SG-PKI operates different CA hierarchies for different purposes:

1. Swiss Government Root CA I hierarchy responsible for high assurance enhanced certificates, i.e. issuing enhanced certificates according to the Swiss federal administrations' terminology (see: www.pki.admin.ch). Enhanced certificates are issued on QSCD exclusively
2. Swiss Government Root CA II hierarchy issuing certificates at a lower security level for persons, organizations/organizational units
3. Swiss Government Root CA III hierarchy supporting "Lightweight Certificate Policy" certificates [27].
4. Swiss Government Root CA IV hierarchy responsible for high assurance regulated and qualified certificates, i.e. issuing regulated and qualified certificates according to the Swiss federal administrations' terminology (see: www.pki.admin.ch).
   Regulated and qualified certificates are issued on QSCD (Qualified Signature Creation Device) exclusively.
   CA specific compliance target: All issuing CA and TSA under the SwissGovernment Root CA IV are compliant to ZertES [2]

The current document describes the Swiss Government Root CA IV hierarchy, i.e. CAs supporting regulated and qualified certificates, including regulated authority certificates (geregelte Behördenzertifikate) for electronic seals.

The CAs of this hierarchy are:

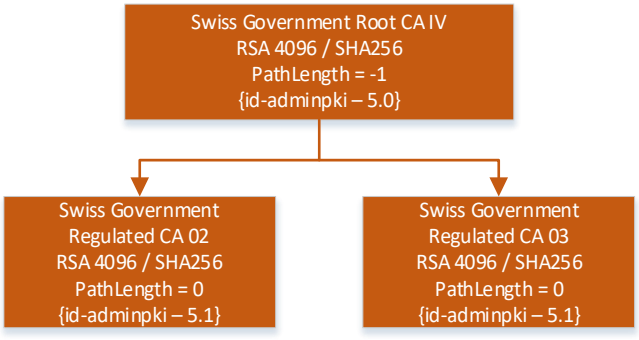


Figure 1 : CA hierarchy 'Swiss Government Root CA IV'

Swiss Government Root CA IV operating at first-root-level (hereinafter referred to as "Root CA") acts as the common trust reference for all CAs issuing regulated and qualified end-user certificates. It issues CA certificates to the CAs (hereinafter referred to as "Issuing CA") operating at second level exclusively, while these CAs in turn issue certificates to the end-user. The two-level CA-hierarchy enables SG-PKI to easily add additional Issuing CAs to an existing Root CA when needed and thus avoid the comparably large effort to establish new Root CAs among all relying parties (requires incorporation of Root CA certificate in all relevant browsers, installation by trusted personnel, etc.).

Now, as the above CAs all comply with the identical security requirements this particular document serves two purposes

- It details the policies governing and practices followed by the Root CA's issuance of CA certificates for the issuing CAs, i.e. it is certificate policy (CP) and certificate practices statement (CPS) for the Swiss Government Root CA IV.
- It also details the policies and practices of the issuing CAs, i.e. it serves as CP and CPS for the CAs issuing regulated and qualified certificates to natural and legal persons (Regulated Authority Certificates or 'Geregelte Behördenzertifikate für Amtssiegel'). Where applicable, the differences between the individual certificate types are set out in specific paragraphs or subchapters.

The document is structured according to RFC 3647 'Certificate Policy and Certification Practices Framework', chapter 6.

1.1.2 Certificates issued under this CP/CPS

The following certificates are issued:

Certificate Policy for Regulated CA02 (CP)	OID
Swiss Government Regulated CA 02	2.16.756.1.17.3.5.1.2
Swiss Government OCSP Responder	2.16.756.1.17.3.5.2.1
Class A - Geregeltes Behördenzertifikat on Smartcard (qcp-l-qscd)	2.16.756.1.17.3.5.2.2
Class A - Qualified Digital Signature on SmartCard (qcp-n-qscd)	2.16.756.1.17.3.5.2.3
Class A - Time Stamp Signer (qcp-l-hsm)	2.16.756.1.17.3.5.2.4
Class A - Geregeltes Behördenzertifikat for TW4S (qcp-l-hsm)	2.16.756.1.17.3.5.2.7
Class A - Qualified Signature for TW4S(qcp-n-hsm)	2.16.756.1.17.3.5.2.13
Class A - Qualified Signature COVID certificate (qcp-l-hsm)	2.16.756.1.17.3.5.2.14

Table 1: Certificate Types under Swiss Government RegularCA02 Document name and identification

Certificate Policy for Regulated CA03 (CP)	OID
Swiss Government Regulated CA 03	2.16.756.1.17.3.5.1.3
Class A - Time Stamp Signer (qcp-l-hsm)	2.16.756.1.17.3.5.2.10
Swiss Government Regulated CA 03 OCSP Responder	2.16.756.1.17.3.5.2.11
Class A - Geregeltes Behördenzertifikat for TW4S (qcp-l-hsm)	2.16.756.1.17.3.5.2.8
Class A - Qualified Signature for TW4S(qcp-n-hsm)	2.16.756.1.17.3.5.2.9
Class A - Geregeltes Behördenzertifikat on Smartcard (qcp-l-qscd)	2.16.756.1.17.3.5.2.15
Class A - Qualified Digital Signature on SmartCard (qcp-n-qscd)	2.16.756.1.17.3.5.2.16

Table 2: Certificate Types under Swiss Government RegularCA03 Document name and identification

This document is the Swiss Government Root CA IV Certificate Policy and Practice Statement. The object identifier (OID) exclusively used for this document is: OID **2.16.756.1.17.3.5.0**.

The OID is based on the Relative Distinguished Names (RDN) assigned by the Swiss Federal Office of Communications (OFCOM).

The elements are detailed in Table 3 and 3 below:

Position	OID Component	Meaning of OID Component
1	2	joint-iso-itu-t
2	16	Country
3	756	CH
4	1	organization[2]
5	17	Bundesamt für Informatik und Telekommunikation (BIT)
6	3	Swiss Government PKI
7	5	Swiss Government Root CA IV
8	0	CP/CPS

Table 3 : CP-OID of Swiss Government Root CA IV

1.2 PKI participants

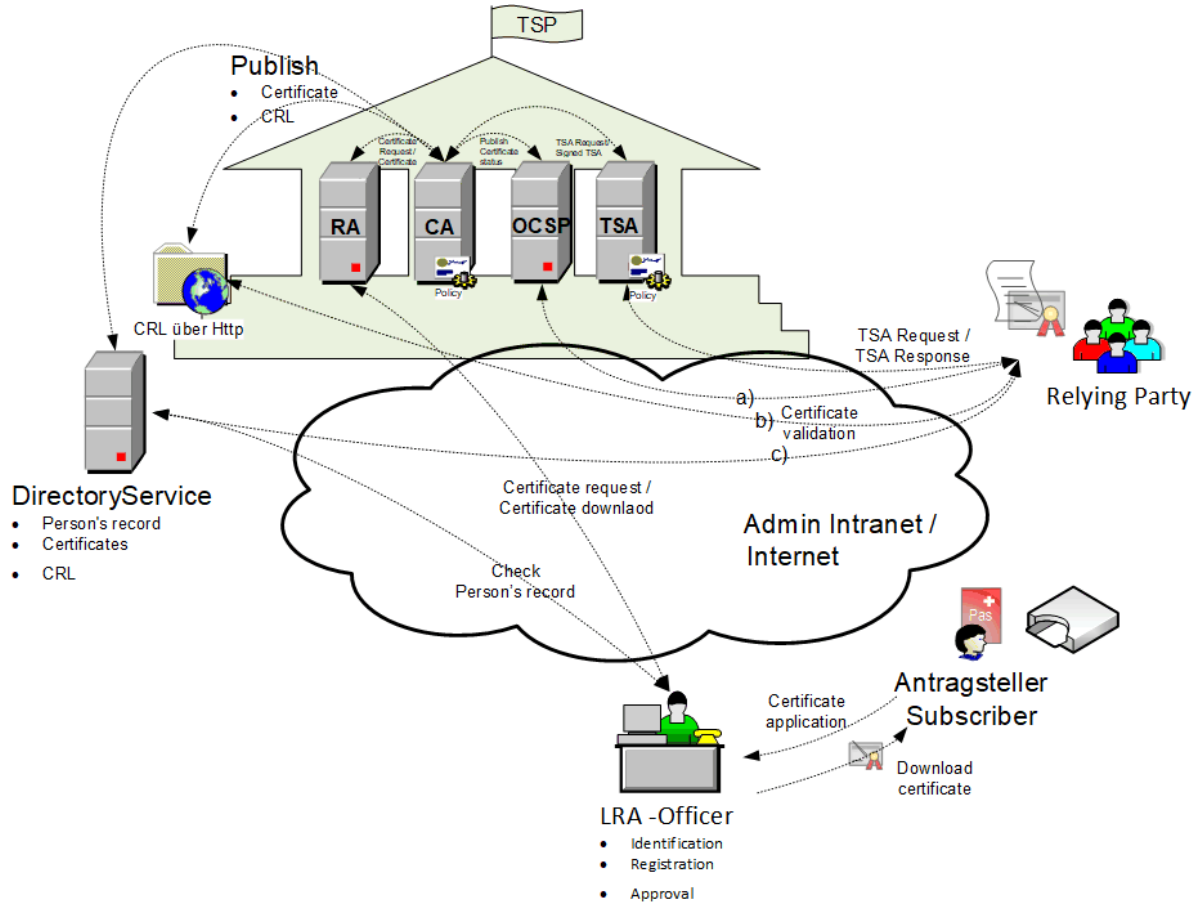


Figure 2 : Overview of PKI participants

[2] Allocated by the Swiss Federal Office of Communications (OFCOM)

1.2.1 Certification authorities

1.2.1.1 Swiss Government Root CA IV

1.2.1.1.1 Swiss Government Root CA IV

Serial Number	dfb34d9a6a2ccf875629e9adafd28c04
Subject DN	CN - Swiss Government Root CA IV OU - Swiss Government PKI O - Bundesamt für Informatik und Telekommunikation (BIT) C – CH
Validity Period	From Friday, November 29 2018 23:01:00 UTC To Sunday, November 29 2043 22:59:00 UTC
Public Key	30 82 02 0a 02 82 02 01 00 c7 69 ff 15 9e da f0 fe 0b a3 1c f4 12 90 d9 84 3d c5 6b cd 72 83 4b a0 a9 91 e3 8f 52 0d 23 84 ec 53 fd 67 01 f9 62 46 1f 57 e8 96 f8 fd 43 ab 13 fe 32 83 bf 49 47 69 3a e7 c5 21 9b 04 ac 4a 4b 1d 2c d9 de ca 79 1d 49 9e 5f 5c 66 d5 6f cd f2 32 77 ff 17 3d d4 93 74 aa 71 3b 7f 32 1a 5d 86 26 9a 04 bf e6 5b 70 ea 98 a3 21 80 79 ac 10 81 9a 82 18 94 6c 7b 6c 03 d4 0a 60 e1 1c 6a 7a 11 5f b7 d0 df ba f4 b6 83 1e e6 70 8e 06 be 74 cd c0 cc 92 5f b9 93 ca a8 9c 52 26 ca 8c 68 05 5f 18 b0 73 c4 50 57 78 a4 96 2c d5 ab 09 96 a3 09 b8 76 62 90 06 39 23 2f de d8 03 77 ef 20 90 e9 6b 31 c8 62 d7 2c f9 ce ae ec ed 0d fb 70 23 1e 5a f1 b0 08 19 bb ce a9 ea c5 e8 6f 07 62 a8 45 b6 e0 22 bb 6a a4 9f 6c 23 95 40 e5 71 5b 22 2a e3 f9 2a 17 76 23 72 22 38 91 08 e0 ad 75 35 f5 9e 42 04 0a df a2 96 91 81 30 6b 13 29 cc 86 fa 49 2f 97 95 6c 16 2c 5b 5e 95 e3 50 4b 4b c5 56 e0 7e 08 d8 27 a7 9c b5 cd de b7 42 11 13 81 c9 8e 49 d4 74 de c0 3a 7a a5 21 a9 ac bc fd 24 ab f0 44 a9 81 e1 e6 c4 38 ea f3 fe 8d f6 d3 91 e2 5c dc 27 b2 86 9f c5 cf 60 59 90 76 2d 11 f8 93 3c 06 90 a1 ca 18 62 67 29 a5 d1 f7 47 34 1c 28 67 05 d7 e9 f5 e7 4c 1c 75 39 2f 7d ec 8e 47 b5 aa ba dc bb 8f fa 63 ad 57 66 08 59 64 c5 bc 9f 1d db 79 26 8b 54 3a 9f 3c 31 64 83 6b fa 29 0e c5 31 59 4a 07 18 67 89 d0 14 c8 80 c4 8f c1 e6 d6 f6 c7 b6 53 a7 f3 b3 ae df 30 f5 bd d9 6c 6b 7e 2a ff 16 73 46 0f 8c ea 37 2a cc ef 6d 8c 01 0a 33 be a0 a5 35 5a 1b 31 37 36 9e 7c 58 fd cd 62 fc 1f e4 c2 88 a9 c8 83 46 8f 28 e4 86 7e 16 6d 80 9d 01 33 ea 3b 78 bc 6a b6 af c4 c1 51 02 03 01 00 01
Signature Algorithm	sha256RSA
Fingerprint(SHA1)	e46a4dd6de3e273015ceec246d534d1399983cfd

Table 4 : Certificate Swiss Government Root CA IV

Swiss Government Root CA IV is the top level CA constituting the basis of trust for all regulated and qualified certificates according to the ZertES [2]. Its Root CA key and certificate have been generated on 29th November 2018 and evidences have been taken [1]. The Root CA certificate is formally distributed as 'trust anchor' to all participants within the Swiss administration.

Swiss Government Root CA IV's tasks are:

- Ensure adherence to the processes defined for registration, certificate issuance, certificate revocation and distribution of status information by all parties concerned.
- Validate requests for the issuance and revocation of certificates issuing CA.
- Issue certificates for issuing CAs as requested.
- Revoke Issuing CA certificates where necessary.
- Generate and publish ARLs to support validation of Issuing CA certificates at all times.
- Publish/distribute the Root CA certificate fingerprint, thereby enabling relying parties to manually validate the Root CA certificate – Root CA certificates are self-signed and thus cannot be chained back to any other reference for electronic validation.

Swiss Government Root CA IV is operated by SG-PKI staff appointed to the task.

1.2.1.2 Subordinated Issuing Certification Authorities

There are two issuing CAs subordinated to Swiss Government Root CA IV. The tasks of these issuing CA are:

- Ensure adherence to the processes defined for registration, certificate issuance, certificate revocation and distribution of status information by all parties concerned.
- Validate requests for the issuance and revocation of end-user certificates.
- Issue end-user certificates as requested.

- Revoke end-user certificates on user-request or in case they are misused.
- Generate and publish CRLs to support validation of end-user certificates at all times.

The Swiss government issuing CAs are operated by SG-PKI staff appointed to the task.

1.2.1.2.1 Swiss Government Regulated CA 02

Throughout the rest of the document, statements pertaining to a certain class of certificates are marked by identifiers in square brackets. A list of these identifiers can be found in '1.5.3 - Certificate Policy Abbreviations'.

Serial Number	036a07988f3b5139def52be5a8ea755e
Subject DN	CN - Swiss Government Regulated CA 02 OU - Swiss Government PKI O - Bundesamt fuer Informatik und Telekommunikation (BIT) OI - VATCH-CHE-221.032.573 C – CH
Validity Period	From Monday, 11. März 2019 15:30:28 To Saturday, 11. März 2034 15:30:28
Public Key	30 82 02 0a 02 82 02 01 00 c0 c8 0a d0 88 b7 17 a1 a6 d9 b2 92 c6 d4 03 40 60 6a 65 c2 32 39 f2 11 b8 68 de ef 32 9b 22 b9 6b bf 68 ea fd 7f 4b f1 d8 08 98 ca 3a bd 7c ac 51 2f 51 af 7a ff ea 25 7a 85 17 32 92 02 d2 b3 c4 9b df 60 5b c7 8e d4 b9 74 e4 11 5f ba d3 a9 d3 04 0e 26 99 bb 93 3b e6 ff dc 95 d1 03 e9 da 13 da c4 90 8f ea 55 34 be e7 90 31 e0 9a 42 b1 02 4c 70 3a 2a fe 57 64 41 f0 a3 e9 8d 15 ef c4 f5 6a 85 23 9b 64 c3 92 a7 27 70 97 b5 e8 42 d3 52 18 79 92 10 ae c7 9a f4 d7 5c 18 b9 8f da 3c 0c df 1f 6d ab 48 99 40 ae e1 be d4 b0 00 c3 8f c6 c8 50 c2 07 65 50 d6 b2 11 c1 9d 73 1b cb f0 5b 21 84 e5 38 b3 d1 1a 9b c9 dd 62 d6 0f 46 f2 c6 52 1a d7 61 cf 41 9d e1 eb 5d 7a 98 3a a0 23 af 34 57 e9 3f 17 7c 65 93 5b 36 27 89 85 54 f8 f3 46 4f c6 4c 14 48 15 bb 77 3b 8d 99 62 b1 75 ce 6b dd be b2 bd 71 e2 24 dd 5f 32 c9 fb 7a 3a c7 49 03 95 af 37 b9 d8 0c 9b 89 0d b5 56 c9 c2 18 6b 61 db eb d8 8c 5f f8 39 c9 76 cc f3 19 09 1f 7e 33 4d 47 c8 c9 64 74 aa 87 eb ec 46 4c 66 ea e0 50 f5 dd 74 a4 8f dd 37 86 61 71 54 b7 46 8c e7 21 97 56 b9 04 14 f7 8a a9 5a a9 4f 66 0f b8 1b bc 4b 41 9f 15 8e 70 94 91 e6 20 4b 12 02 f5 be 9e 08 ad 33 8b 58 f6 cc a5 bb 48 75 9b 70 69 8b 91 a4 af 09 6a fa c6 0c 2d 42 35 2b 35 16 f4 1b 9a 23 93 3b 16 6e b3 04 2b 05 fe 11 4a 4f 19 34 d9 b1 32 0e a6 d2 9a 1e c2 8d 34 34 34 18 97 48 cd 36 38 70 2c 26 e0 fb 5b b9 fd b6 d6 fe ce d6 31 87 4a e5 61 40 6e 58 cd 29 14 94 d3 96 04 45 93 bc 96 7d f8 1f cf 42 19 f2 b8 1c c5 65 de 50 27 0a f9 e8 6f e9 ad 08 ad 91 67 5a cf 78 8d 0c 28 8a 4f c6 d4 73 a0 43 b8 64 55 ee 7f 93 02 03 01 00 01
Signature Algorithm	sha256RSA
Fingerprint (SHA1)	9c34ba000581e6df99f88bc79bb9b7eed6dbc6a3

Table 5 : Certificate Swiss Government Regulated CA 02

The Swiss Government Regulated CA 02 issues:

- [QCP-n] qualified signature certificates for natural persons
- [RCP-l] regulated certificates for legal persons (primarily for authorities of the Swiss public administration and time stamping service)

These certificates meet the requirements laid down in the Swiss federal law on certification services in the area of electronic signatures and other uses of digital certificates, ZertES [2].

1.2.1.2.2 Swiss Government Regulated CA 03

Throughout the rest of the document, statements pertaining to a certain class of certificates are marked by identifiers in square brackets. A list of these identifiers can be found in '1.5.3 - Certificate Policy Abbreviations'.

Serial Number	2f65372a7df6d51383e6378cbd902049
Subject DN	CN - Swiss Government Regulated CA 03 OU - Swiss Government PKI O - Bundesamt fuer Informatik und Telekommunikation (BIT) OI - NTRCH-CHE-221.032.573 C – CH
Validity Period	From Tuesday, 01. December 2020 10:22:18 To Saturday, 01. December 2035 10:22:18
Public Key	30 82 02 0a 02 82 02 01 00 d0 99 c1 28 aa 27 f9 c4 f9 7c 85 76 a3 76 c4 34 db 80 18 87 a6 51 8d 4f a9 89 54 bb cb ab 2f 3c 40 2a c3 3e 9a 09 0f 63 5e 32 6b 4c 85 3c 58 2a 92 68 20 ed 89 16 09 3f 65 6d d1 f0 72 fc d6 f1 75 ab b7 a1 53 a9 f0 42 f7 79 d7 be 90 12 8b 98 72 7d 2d 4e fd 7f c0 4e 79 48 aa 0d 06 60 3a 73 02 55 29 5f fa 50 89 66 61 d8 4b 98 ce 49 cc 95 70 fa 5a 5e 2d 49 57 e2 a7 90 a1 65 b1 36 80 2a 2b 8e 18 73 0b 80 72 6a 5a 31 1e 76 ca 41 be a7 15 59 75 ca f2 73 d9 a8 63 9a 88 ca ef 22 01 92 d9 48 13 6f 68 b4 32 74 4f 06 89 52 de be 07 60 78 a8 08 5f 11 95 86 9e 77 05 58 b3 fd fb cf e6 48 55 2f ab cc 98 90 86 63 9e 14 02 70 69 a8 2a 5f f5 f8 54 be 45 35 ca 90 a0 60 0a d0 ac ab cf ce

	bd de 4c 3b 7f e0 eb b5 4b f9 5c a1 02 31 d7 ce 08 fb b2 2a 9b 93 a1 e3 16 21 b6 b1 4c f5 29 93 fc c1 fa db b8 1d 91 35 37 73 a0 5e 4b f8 6d e4 73 fe 23 85 7c 1a bf 9f fb e0 0f 4c b8 11 70 d2 06 82 11 05 2b 52 dc 6e c1 69 ea 0c d7 1b e9 50 ff 85 0a b8 f8 fa f5 c0 e5 14 ed 51 3a f3 66 e4 9d 43 cb 0a b8 1a ee e5 9e b9 88 8a e1 d4 dc b5 76 90 3e 6a 77 70 0a b6 3f 57 93 6f 64 57 f7 30 c8 91 6f 70 d2 d9 f5 d3 66 97 82 f7 71 f7 ca 16 f7 29 ff 17 de 09 34 3d ee 77 aa 4b 1a 2e 3f 57 eb 84 e8 a4 7e a2 dc e1 08 70 7f bc 61 2b ba 09 34 23 f7 d2 93 f2 dd 68 10 14 d5 90 1f 54 80 1c 30 2b 34 c7 cc 59 64 43 2b 27 4c d9 45 69 69 cc 82 f8 35 da 2e f7 81 ba bc 08 fe ca 39 b2 39 d0 de 1e 87 51 c4 0f c9 00 c4 87 eb 05 6f 55 2d a9 e0 55 a1 bf 60 5f 5e 05 74 d7 72 bf 1b 95 2a 3f 29 77 de f7 b3 04 32 d3 33 d0 df c0 14 50 aa 9f f4 3d 7c eb cc 90 71 87 cf 93 a3 2c 43 4d 47 02 03 01 00 01
Signature Algorithm	sha256RSA
Fingerprint (SHA1)	4648179576d10ea00e268e2f758cc4ae34062e17

Table 6 : Certificate Swiss Government Regulated CA 03

The Swiss Government Regulated CA 03 issues:

- [QCP-n] qualified signature certificates for natural persons
- [RCP-l] regulated certificates for legal persons (primarily for authorities of the Swiss public administration and time stamping service)

These certificates meet the requirements laid down in the Swiss federal law on certification services in the area of electronic signatures and other uses of digital certificates, ZertES [2].

1.2.2 Registration authorities

Registration of certificate applicants is done by local registration authorities (LRAs). These are units of the federal, cantonal or communal administration. They operate on the basis of a frame contract [12] and a service level agreement (SLA) stipulated with SG-PKI.

1.2.2.1 Local Registration Authority Officer (LRAO)

The Local Registration authorities assign individual agents (LRA Officer) to the tasks of the LRA. The tasks of the LRA Officers are:

- Identify the applicant for a personal certificate according to the rules set up in the document ‘Swiss Government PKI Registrierrichtlinien Klasse A - Qualifiziert’ [19].
- ‘Register’ applicants once these have submitted formal requests, i.e. link their identities with the public keys to be certified.
- Initiate or verify and approve revocation requests.
- Take part in the regular audits to validate compliance with Swiss Government Root CA IV CP/CPS
- Inform certificate applicants of their rights and duties as detailed in the ‘Guidelines’ [21] [24] ‘Terms and Conditions’ [20] [23] for the relevant certificate type.
- Approve and carry out unblocking of QSCD (by resetting PINs). Tokens with qualified certificates MUST be unblocked jointly with the respective holder.

1.2.2.2 LRAO contractual requirement

SG-PKI requires LRAOs by contract to:

- Fully comply with this Swiss Government Root CA IV CP/CPS, especially
    - Meet the qualification requirements of Section 5.3.1, when applicable to the delegated function
    - Retain documentation in accordance with Section 5.5.2
    - Abide by the other provisions of these requirements that are applicable to the delegated function

The requirements listed above are part of the respective application forms as specified in [17][18] 'Administration der SG-PKI LRA-Officer ' and have to be signed by the future LRA Officers. SG-PKI is keeping record of all signed applications and annually verifies the Registration Agents audit and domain authorization status.

1.2.2.3 LRAO Authentication

For the above tasks the LRA Officers have to apply for and be granted the appropriate rights by the PKI security officer according to the processes described in [18] 'Administration der SG-PKI LRA-Officer '.

1.2.3 Subscribers

Subscribers are natural persons holding qualified certificates for natural persons or regulated certificates for legal persons issued by the Swiss Government Regulated CA02 or Swiss Government Regulated CA03 subordinate to Swiss Government Root CA IV. These subscribers are

- members of units within the federal or cantonal or communal administrations,

or

- Representatives of companies having a need for exchanging electronically signed documents in the context of their collaboration with one/several of the administration's units[3].

All subscribers are REQUIRED to use their keys/certificates in conformance with the law on the organization of government and administration [8] as well as the regulation on organization of the Federal Department of Finances FDF [9] and always within the framework of the respective applications (see section 1.3 Certificate Usage).

When requesting certificates subscribers are 'applicants'. In the context of X.509 certificates they are 'subjects' and, once they've received the issued certificates, they are 'holders' of certificates.

To avoid any conflicts of interests, the subscriber and TSP organization entity shall be separate entities with the exception of employees of the FOITT Swiss Federal Office of Information Technology, Systems and Telecommunication.

1.2.4 Relying parties

Relying Parties are individuals or organizations that use certificates of this CA to validate the electronic signatures of documents exchanged with these Subscribers.

Relying Parties are allowed to use such digital certificates only in accordance with the terms and conditions set forth in this CP/CPS. It is in their sole responsibility to verify legal validity, digital signatures,

[3] The administrative unit concerned is required to confirm these subscribers' eligibility for getting issued Swiss Government PKI certificates.

authenticate remote users, transaction limits and applicable policies.

The applications used for verifying signatures/validating certificate chains MUST adhere to the procedures as defined RFC 5258.

1.2.5 Other participants

The Federal Office of Communications OFCOM http://www.bakom.admin.ch/ specifies the technical and administrative requirements for certification services supporting electronic signatures and other applications of digital certificates [4].

The Swiss Accreditation Service SAS http://www.seco.admin.ch/sas/ identifies organizations responsible for verifying and attesting PKI provider's compliance with the electronic signature laws. It is the accreditation authority, chooses the auditors for the certification of CSPs in Switzerland.

1.3 Certificate Usage

1.3.1 Appropriate certificate uses

The usage of keys certified by Swiss Government Root CA IV or one of its issuing CAs is restricted to the actions detailed in the following table:

Entity	Private key usage	Certificate usage
Swiss Government Root CA IV	Sign certificates for subordinated certification authorities (Issuing CAs) Sign ARLs (Authority Revocation List)	Validate end-user certificates chaining back to Swiss Government Root CA IV Validate the integrity of ARL and OCSP responses
Swiss Government Regulated CA 02	[QCP-n] Sign qualified certificates for end-users [RCP-l] Sign regulated certificates for legal persons Sign CRLs (certificate Revocation List)	Validate end-user certificates or authority certificates issued by the CA Validate the integrity of CRL and OCSP responses
Subscriber	[QCP-n] Qualified certificates according ZertES [2]: sign documents requiring formal signatures (content commitment)	Verify certificate holder's qualified electronic signature and authenticity
	[RCP-l] Create electronic seal: sign documents (digital signature)	Verify electronic seal and certificate holder's authenticity
Relying Party	not applicable	Verify electronic signatures and electronic seals Verify authenticity of certificate holder Verify role of certificate holder

Table 7 : Authorized usage of private keys and certificates

Subscriber certificates issued by SG-PKI as well as the corresponding keys MAY be used exclusively in conjunction with applications appropriate for the purpose.

1.3.2 Prohibited certificate uses

Any use other than that defined in chapter 1.4.1 is prohibited.

1.4 Policy administration

1.4.1 Organization administering the document

The SG-PKI Trust Backend Team is responsible for administering and publishing the current CP/CPS (see also section 9.12 Amendments).

1.4.2 Contact person

1.4.2.1 SG-PKI Security & Compliance

Contact person for all security and compliance inquiries is Michael von Niederhäusern

Swiss Government
Federal Office of Information Technology, Systems and Telecommunication FOITT
PS-IAM-TRC
Campus Meielen
3003 Bern
Switzerland

1.4.3 Person determining CPS suitability for the policy

The SG-PKI Management Board determines the document's suitability for the purposes of the accepted policies.

Changes or updates to relevant documents will be made in accordance with the stipulations of Swiss Digital Signature Law and if necessary, approved by the organization appointed by Swiss Accreditation Service (SAS) [36].

Currently, the conformity assessment body (CAB) is held by:

KPMG AG
Badenerstrasse 172
8026 Zürich
Switzerland

1.4.4 CPS approval procedures

SG-PKI Management Boardannually reviews this CP/CPS and its related documentation so that it adheres to applicable law,

See also section '9.12 - Amendments'.

1.5 Definitions and acronyms

1.5.1 Definitions

Term	Definition	Source
Affiliate	A corporation, partnership, joint venture or other entity controlling, controlled by, or under common control with another entity, or an agency, department, political subdivision, or any entity operating under the direct control of a Government Entity	BR[4]
Amtssiegel	Electronic document signature based on the use of a 'regulated authority certificate' (geregeltes Behördenzertifikat).	ZertES

[4] Baseline Requirements (BR) for the Issuance and Management of Publicly-Trusted Certificates

Term	Definition	Source
Applicant	The natural person or Legal Entity that applies for (or seeks renewal of) a Certificate. Once the Certificate is issued, the Applicant is referred to as the Subscriber. For Certificates issued to devices, the Applicant is the entity that controls or operates the device named in the Certificate, even if the device is sending the actual certificate request.	BR
Application Software Supplier	A supplier of Internet browser software or other relying-party application software that displays or uses Certificates and incorporates Root Certificates	BR
Audit Report	A report from a Qualified Auditor stating the Qualified Auditor's opinion on whether an entity's processes and controls comply with the mandatory provisions of these Requirements.	BR
Authority Certificate	Behördenzertifikat	
Behördenzertifikat geregelt	Regulated certificate compliant with the Swiss law on digital signatures (ZertES) for legal persons of the Swiss public administration for the creation of electronic seals (Amtssiegel)	ZertES
Certificate	An electronic document that uses a digital signature to bind a public key and an identity	BR
Certificate Management Process	Processes, practices, and procedures associated with the use of keys, software, and hardware, by which the CA verifies Certificate Data, issues Certificates, maintains a Repository, and revokes Certificates.	BR
Certificate Policy	A set of rules that indicates the applicability of a named Certificate to a particular community and/or PKI implementation with common security requirements	BR
Certificate Problem Report	Complaint of suspected Key Compromise, Certificate misuse, or other types of fraud, compromise, misuse, or inappropriate conduct related to Certificates	BR
Certificate Renewal	Certificate renewal is a process in which a new certificate is issued to a Subscriber. The certificate contains new validity information, but retains subject and key information (previously used key)	BR
Certificate Revocation List	A regularly updated time-stamped list of revoked Certificates that is created and digitally signed by the CA that issued the Certificates	BR
Certification Authority	An organization that is responsible for the creation, issuance, revocation, and management of Certificates. The term applies equally to both Roots CAs and Subordinate CAs	BR
Certification Practice Statement	One of several documents forming the governance framework in which Certificates are created, issued, managed, and used	BR
CIS	The "Central Identity Store (CIS)" automatically supplies all office automation platforms daily with data for the daily updated maintenance of user accounts.	SG-PKI
Control	"Control" (and its correlative meanings, "controlled by" and "under common control with") means possession, directly or indirectly, of the power to: (1) direct the management, personnel, finances, or plans of such entity; (2) control the election of a majority of the directors; or (3) vote that portion of voting shares required for "control" under the law of the entity's Jurisdiction of Incorporation or Registration but in no case less than 10%.	BR
Country	Either a member of the United Nations OR a geographic region recognized as a sovereign nation by at least two UN member nations	BR
Digitally Signed Document	In the context of this CP/CPS, a Digitally Signed Document refers to a PDF/A document with a valid signature executed with a "Klasse A" certificate issued under the Swiss Government Root CA IV	SG-PKI
Directory Service	CIS or AdminDir: A meta directory service, used by the Swiss Government.	SG-PKI
Domain Name	The label assigned to a node in the Domain Name System	BR
Domain Name Registrant	Sometimes referred to as the "owner" of a Domain Name, but more properly the person(s) or entity(ies) registered with a Domain Name Registrar as having the right to control how a Domain Name is used, such as the natural person or Legal Entity that is listed as the "Registrant" by WHOIS or the Domain Name Registrar.	BR

Term	Definition	Source
Domain Name Registrar	A person or entity that registers Domain Names under the auspices of or by agreement with: (i) the Internet Corporation for Assigned Names and Numbers (ICANN), (ii) a national Domain Name authority/registry, or (iii) a Network Information Center (including their affiliates, contractors, delegates, successors, or assigns).	BR
Electronic Seal	Digital signature created on the basis of a Regulated Certificate for legal persons	ZertES
Expiry Date	The “Not After” date in a Certificate that defines the end of a Certificate’s validity period.	BR
FIPS 140-2	Federal Information Processing Standard Publication 140-2	Internet
FreeDN	For certificates of “Klasse A” there is a special option called "FreeDN". This option provides the possibility to include in the certificate additional information according to the subscriber’s preference. Examples of such information are: Academic title, association with a particular office of the Swiss Government, a hierarchical position like Vice President etc.	SG-PKI
Government Entity	A government-operated legal entity, agency, department, ministry, branch, or similar element of the government of a country, or political subdivision within such country (such as a state, province, city, county, etc.).	BR
QSCD	Also hardware token, a user controlled, physical device (e.g. smart card) used to store cryptographic information and possibly also perform cryptographic functions (s.a. Qualified Signature Creation Device = qscd)	SG-PKI
Internal Name	A string of characters (not an IP address) in a Common Name or Subject Alternative Name field of a Certificate that cannot be verified as globally unique within the public DNS at the time of certificate issuance because it does not end with a Top Level Domain registered in IANA’s Root Zone Database	BR
Issuing CA	In relation to a particular Certificate, the CA that issued the Certificate. In the context of this document, it is a CA that issues leaf certificates and is subordinate to the Swiss Government Root CA IV.	BR
Key Compromise	A Private Key is said to be compromised if its value has been disclosed to an unauthorized person, an unauthorized person has had access to it, or there exists a practical technique by which an unauthorized person may discover its value. A Private Key is also considered compromised if methods have been developed that can easily calculate it based on the Public or if there is clear evidence that the specific method used to generate the Private Key was flawed.	BR
Key Generation Script	A documented plan of procedures for the generation of a CA Key Pair	BR
Key Pair	The Private Key and its associated Public Key	BR
Klasse A	Certificates of type “Klasse A” issued by SG-PKI are certificates as defined by the Swiss law on digital signatures ZertES [2]. Specifically qualified signature certificates and regulated authority certificates (Behördenzertifikate)	SG-PKI
Legal Entity	An association, corporation, partnership, proprietorship, trust, government entity or other entity with legal standing in a country’s legal system.	BR
Object Identifier	A unique alphanumeric or numeric identifier registered under the International Organization for Standardization’s applicable standard for a specific object or object class.	BR
OCSP Responder	An online server operated under the authority of the CA and connected to its Repository for processing Certificate status requests. See also, Online Certificate Status Protocol	BR
Online Certificate Status Protocol	An online Certificate-checking protocol that enables relying-party	BR
Organization	An Organization is a legal entity represented by natural persons	SG-PKI
PKCS#10	Syntax for certification requests. https://tools.ietf.org/html/rfc2986	RSA
PKCS#12	Binary Format for storing a certificate chain and private key in single encrypted file	RSA

Term	Definition	Source
Private Key	The key of a Key Pair that is kept secret by the holder of the Key Pair, and that is used to create Digital Signatures and/or to decrypt electronic records or files that were encrypted with the corresponding Public Key.	BR
Public Key	The key of a Key Pair that may be publicly disclosed by the holder of the corresponding Private Key and that is used by a Relying Party to verify Digital Signatures created with the holder's corresponding Private Key and/or to encrypt messages so that they can be decrypted only with the holder's corresponding Private Key.	BR
Public Key Infrastructure	A set of hardware, software, people, procedures, rules, policies, and obligations used to facilitate the trustworthy creation, issuance, management, and use of Certificates and keys based on Public Key Cryptography.	BR
Publicly-Trusted Certificate	A Certificate that is trusted by virtue of the fact that its corresponding Root Certificate is distributed as a trust anchor in widely-available application software	BR
Qualified Auditor	A natural person or Legal Entity that meets the requirements of Section 8.3 (Auditor Qualifications)	BR
Qualified Signature Creation Device	A qualified signature creation device (QSCD) is a specific hardware device that ensures that the signatory only has control of their private key. The device must meet the rigorous requirements laid out under Annex II of Regulation (EU) No 910/2014 (eIDAS).	EU No910/ 2014
Registered Domain Name	A Domain Name that has been registered with a Domain Name Registrar	BR
Registration Authority (RA)	Any Legal Entity that is responsible for identification and authentication of subjects of Certificates, but is not a CA, and hence does not sign or issue Certificates. An RA MAY assist in the certificate application process or revocation process or both. When “RA” is used as an adjective to describe a role or function, it does not necessarily imply a separate body, but can be part of the CA.	BR
Relying Party	Any natural person or Legal Entity that relies on a Valid Certificate. An Application Software Supplier is not considered a Relying Party when software distributed by such Supplier merely displays information relating to a Certificate	BR
Repository	An online database containing publicly-disclosed PKI governance documents (such as Certificate Policies and Certification Practice Statements) and Certificate status information, either in the form of a CRL or an OCSP response	BR
Role certificate	Authentication certificate proving certificate holder has been assigned the role identified by the certificate (on top of proving his identity).	SG-PKI
Root CA	The top level Certification Authority whose Root Certificate is distributed by Application Software Suppliers and that issues Subordinate CA Certificates	BR
Root Certificate	The self-signed Certificate issued by the Root CA to identify itself and to facilitate verification of Certificates issued to its Subordinate CAs	BR
Subject	The natural person, device, system, unit, or Legal Entity identified in a Certificate as the Subject. The Subject is either the Subscriber or a device under the control and operation of the Subscriber	BR
Subject Identity Information	Information that identifies the Certificate Subject. Subject Identity Information does not include a domain name listed in the subjectAltName extension or the Subject CommonName field.	BR
Subordinate CA	A Certification Authority whose Certificate is signed by the Root CA, or another Subordinate CA.	BR
Subscriber	A natural person or Legal Entity to whom a Certificate is issued and who is legally bound by a Subscriber or Terms of Use Agreement	BR
Subscriber Agreement	An agreement between the CA and the Applicant/Subscriber that specifies the rights and responsibilities of the parties	BR
Subsidiary Company	A company that is controlled by a Parent Company	BR

Term	Definition	Source
Swiss authorities	Entity of federal, cantonal and communal administrations of Switzerland.	SG-PKI
System	A System is a logical entity controlled by a Person or Organization	SG-PKI
Terms of Use	Provisions regarding the safekeeping and acceptable uses of a Certificate issued in accordance with these Requirements when the Applicant/Subscriber is an Affiliate of the CA	BR
Trustworthy System	Computer hardware, software, and procedures that are: reasonably secure from intrusion and misuse; provide a reasonable level of availability, reliability, and correct operation; are reasonably suited to performing their intended functions; and enforce the applicable security policy.	BR
Unregistered Domain Name	A Domain Name that is not a Registered Domain Name	BR
Valid Certificate	A Certificate that passes the validation procedure specified in RFC 5280	BR
Validation Specialists	Someone who performs the information verification duties specified by these Requirements.	BR
Validity Period	The period of time measured from the date when the Certificate is issued until the Expiry Date.	BR

1.5.2 Acronyms

Term / Acronym	Full text	Explanation
AIS	Auftragsinformationssystem	AIS is a directory service controlled by the Federal Department of Defense, Civil Protection and Sport.
ARL	Authority Revocation List	A list of revoked Certification Authority certificates.
BR	Baseline Requirements	Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates Baseline Requirements Documents - CAB Forum
CA	Certification Authority	An entity that issues certificates.
CIS	Central Identity Store	CIS automatically supplies all office automation platforms daily with data for the daily updated maintenance of user accounts.
CP	Certificate Policy	A named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements.
CPS	Certificate Practice Statement	A statement of the practices that a CA employs in issuing, managing, revoking and renewing or re-keying certificates.
CRL	Certificate Revocation List	A list of revoked certificates.
DN	Distinguished Name	Distinguished Names are used to uniquely identify objects in a directory.
EKU	Extended Key Usage	Certificate Extension as specified in RFC 5280: This extension indicates one or more purposes for which the certified public key MAY be used, in addition to or in place of the basic purposes indicated in the key usage extension. In general, this extension will appear only in end entity certificates.
FCA	Federal Customs Administration	The Swiss Federal Customs Administration
FDF	Federal Department of Finance	The Swiss Federal Department of Finance
FIPS	Federal Information Processing Standards	FIPS are issued by NIST, the U.S. National Institute of Standards and Technology http://www.itl.nist.gov/fipspubs/ .

Term / Acronym	Full text	Explanation
FOITT	Swiss Federal Office of Information Technology, Systems and Telecommunication	Bundesamt für Informatik und Telekommunikation (BIT) www.bit.admin.ch
ITU-T	International Telecommunication Union, Telecommunication Standardization Sector	The ITU-T X-series recommendations cover data networks, open system communications and security. www.itu.int/ITU-T
IDN	Internationalized Domain Name	An internationalized domain name (IDN) is an Internet domain name that contains at least one label that is displayed in software applications, in whole or in part, in a language-specific script or alphabet, such as Arabic, Chinese, Cyrillic, Tamil, Hebrew or the Latin alphabet-based characters with diacritics or ligatures, such as French. These writing systems are encoded by computers in multi-byte Unicode. Internationalized domain names are stored in the Domain Name System as ASCII strings using Punycode transcription.
LDAP	Lightweight Directory Access Protocol	An open, vendor-neutral, industry standard application protocol for accessing and maintaining distributed directory information services over an Internet Protocol (IP) network.
LRA	Local Registration Authority	
LRAO	Local Registration Authority Officer	
MITM	Man In The Middle (Attack)	The man-in-the middle attack intercepts a communication between two systems.
OCSP	Online Certificate Status Protocol	Online trusted source of certificate status information. The OCSP protocol specifies the syntax for communication between the OSCP server (which contains the certificate status) and the client application (which is informed of that status).
OFCOM	Federal Office of Communications	The Federal Office of Communication (OFCOM) handles questions related to telecommunications and broadcasting (radio and television) www.bakom.admin.ch .
OID	Object Identifier	A unique numerical sequence allowing the identification of any “thing”, in particular also documents.
OV	Organization Validation	Organization validation provides assurance that the subscriber is entitled to use the domain name(s) listed in the certificate application, that the subscriber organization does in fact exist, that the organization has authorized the certificate application, and that the person submitting the certificate application (Registration Agent) on behalf of the Subscriber was authorized to do so. OV certificates MAY contain one or more domain names. Those MUST be validated to the same or greater degree as DV certificates.
PIN	Personal Identification Number	A personal identification number is a numeric or alphanumeric code that can be used to authenticate the user to the system.
PKCS	Public-key Cryptography Standards	PKCS are specifications produced by RSA Laboratories in cooperation with secure systems developers worldwide http://www.rsa.com/rsalabs/node.asp?id=2124 .
PKI	Public Key Infrastructure	A set of hardware, software, people, procedures, rules, policies, and obligations used to facilitate the trustworthy creation, issuance, management, and use of Certificates and keys based on Public Key Cryptography.

Term / Acronym	Full text	Explanation
PUK	PIN Unlock Key	Key used to unlock a blocked QSCD.
RA	Registration Authority	An entity that establishes enrolment procedures for certificate applicants, performs the identification and authentication of certificate applicants, initiates or passes along revocation requests for certificates, and approves applications for renewing or re-keying certificates on behalf of a CA.
RFC	Request For Comments	Standards issued by the Internet Engineering Task Force (IETF) http://www.ietf.org/ .
RIO	Registration Identification Officer	The RIO acts on behalf of a Local Registration Authority Officer (LRAO). He formally identifies certificate applicants/subscribers and confirms their authenticity with his signature. He informs subscribers on their rights and duties, has them sign the required registration documents and forwards all data and documents to the responsible LRAO. The LRAO at the LRA-workstation approves the requests processed through RIO.
RSA	Rivest-Shamir-Adleman	The most widely used algorithm today supporting public key cryptography.
SG-PKI	Swiss Government PKI	The PKI of the OFITT responsible for and operating PKI services provided by the Swiss federal administration.
SHA2	Secure Hash Algorithm	The algorithm used most widely today for hashing data to be digitally signed.
SLA	Service Level Agreement	Service contract where the PKI services are formally defined.
TW4S	Trustworthy Systems Supporting Server Signing	Trustworthy Systems Supporting Server Signing as defined in CEN 419 241-1/2
UID	Enterprise Identification Number	Each enterprise active in Switzerland receives a unique enterprise identification number (UID). To ensure that numbers are correctly allocated and managed, the UID register is run by the Federal Statistical Office. The UID register can be accessed via the following address: www.uid.admin.ch
QSCD	Qualified Signature Creation Device	A qualified signature creation device (QSCD) is a specific hardware device or QSCD that ensures that the signatory only has control of their private key. The device must meet the rigorous requirements laid out under Annex II of Regulation (EU) No 910/2014 (eIDAS).

1.5.3 Certificate Policy Abbreviations

For the purposes of the present document, the following certificate policy abbreviations apply:

Certificate Policy Abbreviation	Meaning
RCP	Policy for regulated certificate as specified in **ZertES** [2] (including [RCP-l] and [RCP-n]) (Klasse A) RCP is explicitly introduced here, as ZertES establishes the concept of regulated certificates for legal entities. Regulated certificates [RCP] comply with the standard for qualified certificates QCP-l-qscd as defined in ETSI EN 319 411-2 [28].
RCP-l	Policy for regulated certificate issued to a legal person as specified in **ZertES** [2] (Klasse A - Behördenzertifikat)
RCP-n	Policy for regulated certificate issued to a natural person as specified in **ZertES** [2] (Klasse A)

Certificate Policy Abbreviation	Meaning
QCP-n	Policy for qualified signature certificate issued for a natural person as specified in **ZertES** [2] (Klasse A - qualifiziert) Qualified certificates QCP-n comply with the standard for qualified certificates QCP-n-qscd as defined in ETSI EN 319 411-2 [28].

Table 8 : Certificate Policy Abbreviations

1.5.4 Notation

The requirements identified in the present document include:

a) Requirements applicable to any certificate policy. Such requirements are indicated by clauses without any additional marking;

b) Requirements applicable to the services offered under the applicable certificate policy. Such requirements are indicated by clauses marked by the applicable certificate policy indicator: "[RCP]", "[RCP-l]", "[RCP-n]" and/or "[QCP-n]".

c) Requirements applicable for Trustworthy Systems Supporting Server Signing as defined in CEN 419 241-1/2 are indicated by clauses marked by using [TW4S]

1.5.5 Conventions

The key words “MUST”, “MUST NOT”, “REQUIRED”, “SHALL”, “SHALL NOT”, “SHOULD”, “SHOULD NOT”, “RECOMMENDED”, “MAY”, and “OPTIONAL” in this CP/CPS SHALL be interpreted in accordance with RFC 2119

2 Publication and Repository Responsibilities

2.1 Repositories

SG-PKI makes information related to Swiss Government Root CA IV and its Issuing CAs publicly available through SG-PKI's web site (www.pki.admin.ch).

2.2 Publication of certification information

SG-PKI publishes information related to certificates issued by Swiss Government Root CA IV and its issuing certification authorities with the following methods:

- Publication on the SG-PKI homepage (7 x 24 h availability):
    - The current version of the CP/CPS for the Swiss Government Root CA IV and its issuing certification authorities.
    - A schematic overview of the actual CA structure
    - Certificate(s) of the Swiss Government Root CA IV
    - Fingerprint of the certificate of the Swiss Government Root CA IV
    - Certificate(s) of each Issuing CA
    - Fingerprint of the certificate(s) of each Issuing CA
    - Terms and conditions "Klasse A" for natural persons [20]
    - Terms and conditions "Behördenzertifikate" [23]
    - Guidelines "Klasse A - qualifiziert" [21]
    - Guidelines "Klasse A – geregeltes Behördenzertifikat" [24]
    - Certificate of the TSA

2.3 Time or frequency of publication

SG-PKI will publish the current version of the following publications on its web site:

- Swiss Government PKI - Root CA IV – CP/CPS: This document. If updates are required, the new version of this document will publish as soon as they have been approved.

SG-PKI will publish the following information on a regular schedule:

- **Swiss Government Root CA IV** updates its **ARL** at least **once a year** and immediately after revoking a Issuing CA's certificate.
- **Swiss Government Regulated CA 02** updates its **CRL at least every hour**
- **Swiss Government Regulated CA 03** updates its **CRL at least every hour**
-

2.4 Access controls on repositories

The CRL and OCSP information are clearly managed. All access to the data is managed through SG-PKI and requires sufficient authorization. The type of authorization required depends on how the process is executed. Manager/Administrator access always requires multi factor authentication.

This CP/CPS is provided as public information on the SG-PKI web site. Public documents are only valid if they are published as a PDF with the digital signatures of the SG-PKI Management Board. Write access to the document repository is controlled through multi factor authentication.

Repositories CRL distribution points and OCSP Server are freely accessible on a best effort i.e. 24/7 basis to all users having access to the respective network.

3 Identification and Authentication

Unless it is explicitly stated, this section concentrates on the identification and authentication of subscribers, i.e. applicants for and holders of end-user certificates. Obviously, requests for the issuance and revocation of CA and Root CA certificates have to be authenticated, too. However, as the respective processes are all initiated by SG-PKI personnel specifically appointed to the tasks, the identities and roles have already been well established and the authentication can be based on existing certificates.

3.1 Naming

3.1.1 Types of names

All subscribers require a distinguished name that is in compliance with the X.500 standard for Distinguished Names and with RFC 5280. Certificates issued by this CA (SG-PKI) comply with these standards and Certification Authority approves the naming conventions.

The distinguished name (DN) is a non-empty sequence of printable characters recommended by the X.501 (ITU-T), which includes all or a subset of the following fields:

- Common Name (CN)
- Given Name (GN)
- Surname (SN)
- Organizational Unit (OU)
- Organization (O)
- Organization Identifier (OI)
- Locality (L)
- State or Province (S)
- Country (C)
- Email Address (E)

3.1.1.1 Natural Persons

For natural persons, the DN MUST MUST comply with the details set out in the current version of the **Federal law on the certification services supporting electronic signatures ZertES** [2] and the **Regulation on certification services supporting electronic signatures VZertES** [3].

‘Standard’ subscribers are employees of the federal, a cantonal or a communal administration. They are identified by their name, first name and a unique alphanumerical code generated by Directory Service (for details see section 3.1.5). For these ‘standard’ subscribers there is normally no other identifying data provided in the certificates such as function, title, organizational unit etc

Persons from outside the administrations are not eligible as subscribers as a standard. However, administrative bodies collaborating closely with external partners MAY authorize exceptions and have SG-PKI certificates issued to representatives of these companies. The respective subscribers are identified in the same way as standard subscribers.

Given name and surname must correspond exactly to the details in the identification document used and archived for identification purposes.

For the CommonName the information provided by the Directory Service is used.

3.1.1.2 Legal Persons

[RCP-l] The subscriber DN in authority certificates for electronic seals MUST comply with the details set out in the current version of the **Federal law on the certification services supporting electronic signatures ZertES** [2] and the **Regulation on certification services supporting electronic signatures VZertES** [3]. The detailed content of the DN is specified in ‘7.1.4 Name forms’.

3.1.2 Need for names to be meaningful

The subject and issuer name contained in a certificate MUST be meaningful in that they either identify an employee of an administrative unit, a natural person as representative of a company or an organization.

3.1.3 Anonymity or pseudonymity of subscribers

[QCP]: Given SG-PKI's explicit consent, subscribers using FreeDN MAY give a pseudonym as identifier. In that case the subscriber DN MUST include the term 'PSEUDO' in the distinguished name.

For all other certificates pseudonyms are not supported.

3.1.4 Rules for interpreting various name forms

According to the ITU-T recommendation T.50 International Reference Alphabet (IRA, Information technology - 7-bit coded character set for information interchange) special characters will be converted as follows:

- In general, national characters are represented by their ASCII equivalent, e.g. é, è, à, ç are represented by e, e, a, c.
- The German characters ("Umlaute") MAY receive special treatment: ä, ö, ü are represented by either ae, oe, ue or a, o, u.

At the explicit request of the subscriber, special characters can be used. This may, however, adversely affect the compatibility with applications using such certificates.

3.1.5 Uniqueness of names

Names in SG-PKI qualified and enhanced certificates MUST be unique. SG-PKI enforces this through the following procedure:

- Subscribers with a record in the Swiss Government Directory Service (see 3.2.3 - Authentication of individual identity) have already a common name that has been added a unique suffix by the Directory Service application. It is derived by hashing the subscriber's name, first name and employee number. With employees of cantonal or communal administrations a number identifying the canton or the community, together with the personnel number, is used as the basis for calculating the hash value. For subscribers external to the administration the unique alphanumerical value is computed by Directory Service from the date/time they are registered in the administrative database.
- In case an applicant's distinguished name should nonetheless duplicate the DN of an existing subscriber, the responsible registration authority MUST contact SG-PKI to resolve the conflict.
- For regulated authority certificates, the subject MUST contain the UID of the subscriber's organization in the attribute organizationIdentifier. This ensures the uniqueness of the subscriber's distinguished name.

3.1.6 Recognition, authentication, and role of trademarks

Not relevant. SG-PKI qualified, regulated and enhanced certificates don't convey any data related to trademarks.

3.2 Initial identity validation

3.2.1 Method to prove possession of private key

3.2.1.1 Key Generation as part of the issuing process

The signature keys are generated inside the qualified signature creation device (QSCD) at a local registration office in the presence of the applicant.

The QSCD ensures that the private key can never be exported.

Within the use of the remote signing service (TW4S) the private key is generated on a dedicated HSM.

3.2.2 Authentication of organization identity

3.2.2.1 Qualified certificates [QCP-n]

Qualified certificates are exclusively issued for natural persons. This DN and the applicant's entitlement to use the DN is verified by a LRA officer (LRAO) according to the applicant's input and on the basis of the documents submitted.

3.2.2.2 Regulated certificates for organizations (authority certificates) [RCP-l]

Applicants for authority certificates MUST prove their identity by personally presenting to the local registration agency a valid travel document, i.e. a passport or an identity card, qualified for entering Switzerland. In addition, they MUST prove that they are duly authorized to represent the organization for which the certificates are applied for (**VZertES** [3], Art. 6, para. 1). To apply for a Regulated Authority Certificate, the form "Power of Attorney to Apply for the Regulated Authority Certificate" must be completed in detail and attached to the certificate application together with all the necessary evidence.

The core data of the organization MUST be verified against its entry in the Swiss national UID-register [35] in accordance with **VZertES** [3] Art. 6, para. 2.

3.2.3 Authentication of individual identity

Applicants for certificates MUST prove their identity by personally presenting either a valid passport, Swiss identity card or an identity card qualified for entering Switzerland. The LRA MUST carry out the following checks:

- verify the validity of the presented identification document
- verify the contents of the applicant certificate request form,
- verify the applicant is registered in a directory under the control of the authorities of the Swiss Government (e.g. Directory Service or AIS),
- verify the applicant CN in the directory,
- verify the applicant Given Name and Surname is identical to the one in the identity document presented.
- [TW4S] Certificates dedicated for the use within the remote signature service, the applicant has to be identified in person (see VZertES [3], Art. 4) by an LRA-Officer especially trained and qualified for issuing these certificates.

3.2.3.1 Qualified certificates [QCP-n]

For qualified certificates, the applicant has to be identified in person (see VZertES [3], Art. 4) by an LRA-Officer especially trained and qualified for issuing these certificates.

3.2.3.2 Regulated certificates [RCP]

For regulated certificates, the applicant has to be identified in person by an LRA-Officer trained and qualified as for qualified certificates.

3.2.4 Non-verified subscriber information

The LRA verifies all data necessary for identifying an applicant as specified in ‘3.2.2 - Authentication of organization identity’ and ’3.2.3 - Authentication of individual identity’. It doesn’t do any further verification of requests for certificates.

3.2.5 Validation of authority

With certificate requests from subscribers external to the administration, the LRA validates the authority of the representative as described in "Power of Attorney to Apply for the Regulated Authority Certificate" by consulting the administrative unit having authorized the external partner originally.

3.2.6 Criteria for interoperation

Not applicable.

3.3 Identification and authentication for re-key requests

Re-key is not supported.

3.4 Identification and authentication for revocation request

The detailed process for revoking certificates is documented in section ‘4.9.3 Procedure for revocation request’.

Any authorized requestor MAY authenticate a revocation request by:

- Personal appearance and presentation of a valid travel document (ID card, a passport or an identity document recognized for entry into Switzerland) at a LRA
- Sending the revocation request by registered mail to the local LRA.
- Electronically signing the revocation request with his signing key, provided the revocation is not done because of a suspected or actual key compromise or of the loss/theft of the qualified signature creation device.
- Contacting FOITT’s ServiceDesk which will forward the request to an LRA for approval.
- [QCP-n] Using the application SG-PKI offers for the purpose.

The LRA verifies the requestor’s identity and authorization on the basis of the documents he presents and the data provided in conjunction with the original certificate request.

4 Certificate Life-Cycle Operational Requirements

This paragraph details all requirements for end-user certificates. For Root CA and Issuing CA key pairs and certificates there exist identical or more stringent requirements. However, as the respective processes are strictly handled by SG-PKI personnel in a secure environment they are not explicitly mentioned here, except where the results have an impact on the other participants.

4.1 Certificate application

4.1.1 Who can submit a certificate application

As a standard, every employee of the federal administration as defined in the law on the Organization of Government and Administration (see [8]) as well as the regulation on organization of the FDF (see [9]), and all employees of cantonal and communal authorities MAY submit requests for SG-PKI qualified or enhanced certificates, provided his/her organization has signed the frame contract [12] and the service level agreement with FOITT.

[QCP-n] For Klasse A certificates, also the Addendum to the frame contract with FOITT [13] has to be signed by the organization.

[RCP-l] As a general rule, authority certificates for electronic seals are only issued to organizations of the federal administration as defined above. Authority certificates for cantonal or communal organizations can be issued when there is due reason to facilitate document and data exchange with the federal authorities.

In each individual application for a certain certificate type the following signed documents have to be included:

Type	Documents
RCP-l	Terms and conditions for Electronic Seals Swiss Government PKI (Benutzervereinbarung und Nutzungsbedingungen Klasse A - geregeltes Behördenzertifikat [22]) Guidelines for Electronic Seals of Swiss Government PKI (Guidelines zum Bezug von Zertifikaten der Klasse A - geregeltes Behördenzertifikat [24])
RCP-n	At this time no RCP-n certificates are issued under this CP/CPS.
QCP-n	Terms and conditions for Klasse A certificates Swiss Government PKI (Benutzervereinbarung und Nutzungsbedingungen Klasse A - qualifiziert [20]) Guidelines for Klasse A certificates of Swiss Government PKI (Guidelines zum Bezug von Zertifikaten der Klasse A - qualifiziert [21])
TW4S	The **T**rust**W**orthy **S**ystem **S**upporting **S**ecure **S**ignatures is using QCP-n and RCP-l certficates.

Table 9 : Required Documents for Application

Representatives of companies working closely with one of the administrative units MAY request SG-PKI qualified, regulated or enhanced certificates as well, provided the administrative units concerned formally confirm to SG-PKI the certificates are necessary for securing documents or data exchange with the applicants for certificates. Companies outside the federal, cantonal or communal authorities cannot apply for regulated certificates for legal persons with SG-PKI.

4.1.2 Enrollment process and responsibilities

The enrollment processes supported and the responsible parties are:

Process	Description	Responsible
[QCP-n] Decentralized Key Generation	1. Applicant initiates request. 2. Applicant is identified through a valid identification document (passport or identity card) 3. The presence and validity of all documents as required in paragraph 9 of ZertES [2] is checked. 4. Applicant signs required documents specified in 'Table 9 : Required Documents for Application' 5. QSCD is fully personalized at LRA in presence of the applicant. In detail: After the generation of the private and public keys and the CSR the CRS will be uploaded to the CA. The certificate will be issued by the CA and will finally written to applicant's token.	Applicant LRAO LRAO LRAO LRAO/CA
[RCP-I] Decentralized Key Generation	1. Applicant initiates request. 2. Applicant is identified through a valid identification document (passport or identity card) 3. The granted power of attorney for the organization will be verified using the form and the ID copy of the person granting the power of attorney for the organization. 4. The presence and validity of all documents as required in paragraph 9 of ZertES [2] is checked. 5. Applicant signs required documents specified in 'Table 9 : Required Documents for Application' 6. QSCD is fully personalized at LRA in presence of the applicant. In detail: After the generation of the private and public keys and the CSR the CRS will be uploaded to the CA. The certificate will be issued by the CA and will finally written to applicant's token.	Applicant LRAO at SGPPKI LRAO at SGPKI LRAO at SGPKI LRAO at SGPKI LRAO/CA at SGPKI

Table 10 : Registration application processing

4.2 Certificate application processing

4.2.1 Performing identification and authentication functions

All identification and authentication functions are done by LRAOs. Independent of the enrollment process (see 0

Enrollment process and responsibilities) the LRAO identifies the applicants as follows: Applicants present themselves in person to the LRAO.

- Applicants' identities are verified on the basis of a valid travel document (valid Swiss passport or identity card or foreign travel document recognized for entry into Switzerland).
- LRAO scans the identity documents presented to be stored as evidence by the CAs concerned.
- [RCP-l] The identity of a person applying for a certificate for a legal person is verified on the basis of a valid travel document (ID card or a passport) that entitles the bearer to enter Switzerland. The applicant has to prove that he/she is entitled to represent the legal person, either by presenting a duly signed mandate or an extract of the companies' register record.
- [RCP-l] The legal person is identified with an UID (Enterprise Identification Number)). Proof for the UID has to be presented in accordance with clause 6 of the VZertES [3].

4.2.2 Approval or rejection of certificate applications

LRAOs accept certificate applications provided the following requirements are met:

- [QCP-n] The applicant is registered in a directory under the control of the authorities of the Swiss Government (e.g. Directory Service or AIS) matching the data in the application.
- The authenticated applicant's name matches the one in the application.
- Where applicable: The administrative unit responsible for a 'non-administrative' applicant confirms applicant's entitlement for requesting SG-PKI certificates.
- The DN given in the request doesn't duplicate any of the DNs in existing SG-PKI certificates (except the ones of the actual applicant).
- [RCP-l] The UID of the legal person specified in the application matches the UID of the legal person in the UID-register [35].
- [RCP-l] The organization name attribute of the DN of the application matches exactly the name as specified in the UID-register [35].

Applications that don't meet all of the requirements are either held pending to enable amendments or are rejected by the LRAs in case an application is clearly invalid. If they are in doubt, LRAs consult with SG-PKI.

4.2.3 Time to process certificate applications

Certificate applications are processed instantaneously once the requests have been formally approved. Consequently, certificates are issued within minutes after registration by an LRAO.

4.3 Certificate issuance

4.3.1 CA actions during certificate issuance

The CAs subordinated to Swiss Government Root CA IV issue certificates on-line, i.e. once a valid request has been approved by an LRAO the responsible CA automatically issues the certificate asked for. Depending on the enrollment process used (see 0

Enrollment process and responsibilities), the CA either downloads the certificate directly to the LRA having approved the request (to be transferred to the QSCD) or holds it pending for download until the subscriber actively retrieves it from his/her own workstation.

4.3.2 Notification to subscriber by the CA of issuance of certificate

After a certificate is issued, the CAs subordinated to Swiss Government Root CA IV send an e-mail notification the subscriber of the certificate using the e-mail address indicated in the certificate.

4.4 Certificate acceptance

4.4.1 Conduct constituting certificate acceptance

SG-PKI doesn't require a formal acceptance of the certificates it issues. Certificates are deemed to be accepted with the handover of the fully personalized QSCD or with the successful download of certificates by the applicants.

4.4.2 Publication of the certificate by the CA

Certificates issued by CAs under this CP/CPS may be published in Directory Service, accessible to employees of the federal administration. Certificates issued to 'non-administrative' users may be published in the public part of Admin-Directory, i.e. they are accessible to all Internet users as well (by means of LDAP).

4.4.3 Notification of certificate issuance by the CA to other entities

Other entities are not actively notified of certificate issuance by the CAs subordinated to Swiss Government Root CA IV. However, the LRAOs can retrieve data on certificates they have issued at their convenience.

4.5 Key pair and certificate security rules

4.5.1 Subscriber private key and certificate usage

Subscribers MUST use their private keys and certificates strictly as stipulated in section 1.3 Certificate Usage.

[QCP-n] In particular, signature keys and the corresponding qualified certificates MUST be used exclusively for electronically signing documents and for verifying signatures.

In addition to the adherence to the key usages specified, subscribers are bound to the following rules when using their keys and certificates:

- Ensure they alone have access to their private keys and the QSCD, i.e. keep PIN and PUK strictly confidential.
- When suspecting or knowing that one or several of their private keys has been compromised, subscribers MUST stop using the key(s) and report the incident to an LRA or FOITT's Service Desk.
- In case data included in certificates is no longer valid, subscribers MUST have the certificates concerned revoked (see 4.9) and MUST stop using these keys.

4.5.2 Relying party public key and certificate usage

Relying parties MAY only use public keys and certificates

- if certificates are valid and active (i.e. neither suspended nor revoked);
- for the purpose(s) indicated in the certificates.

Furthermore Relying Parties SHALL:

- be held responsible for understanding the proper use of public key cryptography and certificates and its related risks;
- agree to all terms and conditions of this CP/CPS;
- verify certificates issued by this CAs, including use of revocation information, in accordance with the certification path validation procedure, taking into account any critical certificate extensions (ITU-T recommendation X.509);

4.6 Certificate renewal

Certificate renewal is not supported by any of the Issuing CAs subordinated to Swiss Government Root CA IV.

4.7 Certificate re-key

Certificate re-keying is not supported by any of the Issuing CAs subordinated to Swiss Government Root CA IV.

4.8 Certificate modification

CAs under this CP/CPS do not support certificate modification.

4.9 Certificate revocation and suspension

4.9.1 Circumstances for revocation

4.9.1.1 Reasons for revoking a subscriber certificate

Certificates issued by CAs subordinated to Swiss Government Root CA IV MUST be revoked under the following circumstances:

- The subscriber (certificate holder) requests in writing that SG-PKI revoke the certificate.
- The subscriber notifies SG-PKI that the original certificate request was not authorized and does not retroactively grant authorization.
- A certificate has been acquired illegitimately.
- SG-PKI is made aware that the Certificate was not issued in accordance with these requirements or the CA’s certificate policy or certification practice statement
- SG-PKI obtains evidence that the subscriber’s private key corresponding to the public key in the certificate suffered a key compromise.
- SG-PKI obtains evidence that the certificate was misused.
- SG-PKI is made aware that a subscriber has violated one or more of its material obligations under the subscriber terms and conditions agreement.
- A subscriber or LRA personnel have violated the rules set out in this CP/CPS.
- A QSCD has been lost or stolen.
- A QSCD is defective.

- SG-PKI is made aware of a material change in the information contained in the certificate (e.g. e-mail address and additional data within the option ‘FreeDN’).
- SG-PKI determines that any of the information appearing in the Certificate is inaccurate or misleading;
- A subscriber has been dismissed or suspended by his employer.
- The frame contract with a subscriber’s organization has expired.
- A CA subordinated to Swiss Government Root CA IV or SG-PKI as a whole ceases operation and has not made arrangements for another CA to provide revocation support for the certificate.
- The CA’s right to issue certificates under these requirements expires or is revoked or terminated, unless SG-PKI has made arrangements to continue maintaining the CRL/OCSP repository
- SG-PKI is made aware of a possible compromise of the private key of the subordinate CA used for issuing the certificate

4.9.1.2 Reasons for revoking a subordinate CA certificate

SG-PKI revokes an Issuing CA certificate if one or more of the following occurs:

- SG-PKI obtains evidence that the Subordinate CA’s Private Key corresponding to the Public Key in the Certificate suffered a Key Compromise or no longer complies with the requirements of Sections 6.1.5 Key sizes and 6.1.6 Public key parameters generation and quality checking,
- SG-PKI obtains evidence that the Certificate was misused;
- SG-PKI is made aware that the Certificate was not issued in accordance with or that Subordinate CA has not complied with this CP or the applicable Certificate Policy or Certification Practice Statement;
- SG-PKI determines that any of the information appearing in the Certificate is inaccurate or misleading;
- SG-PKI or Subordinate CA ceases operations for any reason and has not made arrangements for another CA to provide revocation support for the certificate;
- The Issuing CA’s right to issue Certificates under this CP/CPS expires or is revoked or terminated, unless SG-PKI has made arrangements to continue maintaining the CRL/OCSP Repository;
- Revocation is required by the Issuing CA’s Certificate Policy and/or Certification Practice Statement.

4.9.2 Who can request revocation

Requests for revoking certificates can be placed by:

- The subscriber.
- LRA personnel having done the registration for the certificate in question.
- The administrative unit employing the subscriber.
- The administrative unit having vouched for ‘external’ subscribers.
- The SG-PKI Security Officer.
- The SG-PKI Management Board.

The Security Officer of the subscriber’s Department (ISBD) or Office (ISBO).

Certificates MAY also be revoked on the basis of a judicial decision. The ensuing request in writing including the basis of the decision MUST be addressed to the SG-PKI Management Board as per 5.2.1 - Trusted roles.

4.9.3 Procedure for revocation request

The procedure for revoking certificates issued by CAs subordinated to Swiss Government Root CA IV is as follows:

- The actual requestor (see 4.9.2 - Who can request revocation) initiates the process and is authenticated by an LRAO, (as detailed in 3.4 Identification and authentication for revocation request) during office hours or by FOITT's Service Desk (to forward the request to an LRA) at all other times.
- The LRAO verifies requestor's entitlement for launching the request. Provided the result is positive the LRAO approves the request and forwards it to the responsible CA.
- The CA processes the revocation request automatically and instantaneously. It then informs the LRA and certificate holder on the completed revocation.
- Finally, the LRAO investigates the reasons leading to the need for revocation, e.g. why a key has been compromised, what rules the certificate holder has violated and why, etc. The LRAO records its findings in a database run by SG-PKI for the purpose.
- Serial numbers of revoked certificates may not be reused.

4.9.4 Revocation request grace period

All parties concerned MUST request revocation without delay once they know there is a valid reason (see 4.9.1 - Circumstances for revocation).

4.9.5 Time within which CA must process the revocation request

CAs subordinate to Swiss Government Root CA IV revoke certificates without delay as soon as they receive approved requests from a LRA. With every revocation the responsible CA updates its CRL and publishes this under the provided CDP.

4.9.6 Revocation checking requirement for relying parties

All relying parties SHALL ensure they are in possession of a valid certificate status, provided by the OCSP service, or an actual CRL at the moment they verify a signature on the basis of a SG-PKI certificate.

4.9.7 CRL issuance frequency

4.9.7.1 CRL issuance frequency for the Status of Subscriber Certificates

The Swiss Government Regulated CA02/CA03 automatically generates a new CRL every hour. The value of the nextUpdate field is never more than ten days beyond the value of the thisUpdate field.

4.9.7.2 CRL issuance frequency for the Status of Subordinate CA Certificates

Swiss Government Root CA IV issues and publishes updated ARLs every year as a standard. Additionally, if one of its Issuing CA is revoked the Swiss Government Root CA IV updates its ARL and publishes it immediately. The value of the nextUpdate field is never more than one year beyond the value of the thisUpdate field

4.9.8 Maximum latency for CRLs

CRLs updated by the issuing CAs are published on the web site (see 2.1 - Repositories) with a maximum latency of 24 hours.

4.9.9 On-line revocation/status checking availability

The SG-PKI provides OCSP services as follows:

- [QCP-n], [RCP] OCSP compliant with RFC 6960

The certificate status databases, used by the OCSP services, are updated every hour during office hours.

OCSP responses are signed by an OCSP Responder whose Certificate is signed by the CA that issued the Certificate whose revocation status is being checked.

Within the OCSP response, the fields “This Update” and “Next Update” reflect the validity period of the returned OCSP status.

4.9.10 On-line revocation checking requirements

Relying parties SHOULD do on-line revocation checking when validating SG-PKI qualified, regulated or enhanced certificates.

4.9.11 Other forms of revocation advertisements available

No stipulation

4.9.12 Special requirements re-key compromise

There are no special requirements re-key compromise in addition to the ones specified in 4.7 - Certificate re-key and 4.9.3 - Procedure for revocation request.

4.9.13 Circumstances for suspension

SG-PKI does not support suspension of certificates issued under this CP/CPS.

4.9.14 Who can request suspension

Not applicable. (see section 4.9.13 - Circumstances for suspension).

4.9.15 Procedure for suspension request

Not applicable (see section 4.9.13 - Circumstances for suspension).

4.9.16 Limits on suspension period

Not applicable (see section Circumstances for suspension4.9.13 - Circumstances for suspension).

4.10 Certificate status services

4.10.1 Operational characteristics

Certificate status information is available via the CRLs of the CAs subordinated to Swiss Government Root CA IV or by requesting certificate status information from the OCSP responder.

The CRL of a given CA contains the serial numbers of revoked Certificates. Expired certificates will be listed in the CRL. The CRLs are published on the web site (see 2.1 Repositories). The integrity and authenticity of the status information is protected by a digital signature of the respective CA.

4.10.2 Service availability

The service (CRLs and OCSP responder) is available for at least 99% of the time during office hours. At all other times the availability of the service is not guaranteed. However, outages are shorter than 24h in 80% of all cases.

High-Priority Certificate Problem Reports can be reported to the Servicedesk FOITT on 7x24 hours by phone: Service Desk BIT: 058 **46 588 88**.

4.10.3 Operational features

There are no operational features offered for the status service.

4.11 End of subscription

End of subscription occurs after:

- successful revocation of the last certificate of a subscriber,
- Expiration of the certificate of a subscriber.

For reasons of legal compliance, the SG-PKI MUST keep all subscriber data and documentation for a minimum period of 11 years after termination of a subscription.

4.12 Key escrow and recovery

Since the Swiss federal law on electronic signatures ZertES [2] explicitly prohibits escrow of signature keys of qualified or regulated certificates, no escrow of these keys is done under this CP/CPS.

4.12.1 Key escrow and recovery policy and practices

Not applicable

4.12.2 Session key encapsulation and recovery policy and practices

Not applicable

5 Facility, Management, and Operational Controls

5.1 Physical Controls

5.1.1 Site location and construction

SG-PKI operates its PKI systems in an appropriately secured location of the FOITT.

5.1.2 Physical access

Physical access to the PKI systems is regulated in SG-PKI's access control directive [15].

Only persons possessing a badge with the specific permissions issued by FOITT security administration can enter the secured location containing SG-PKI's IT hardware. Access to the location is prohibited for all other persons unless accompanied by an authorized SG-PKI employee.

The secured location is protected by different security mechanisms which are regularly checked and audited.

5.1.3 Power and air conditioning

The PKI systems is powered through a no-break power supply which acts as power conditioner as well.

An air condition specifically run for the secured location ensures constant temperature and humidity 7x24h.

5.1.4 Water exposures

The secured location is equipped with water detectors connected to the building's surveillance center.

5.1.5 Fire prevention and protection

The secured location is equipped with smoke and heat detectors connected to the building's surveillance center.

5.1.6 Media storage

Not applicable. Data related to the PKI systems is backed up in specific servers exclusively (see 5.1.8).

5.1.7 Waste disposal

SG-PKI personnel use the appropriate mechanisms depending on the classification of the data held by media for removal, e.g. magnetic and mechanical shredders.

5.1.8 Off-site backup

SG-PKI maintains a backup-site from where certification can be upheld in case of an emergency.

SG-PKI uses an off-site, protected location for storing back-up data.

5.2 Procedural Controls

5.2.1 Trusted roles

To enable the necessary segregation of critical duties within its certification activities, SG-PKI distinguishes different trusted roles. Some of these MAY be attributed to the same persons, provided this

doesn't violate the 'four eyes' rule with security critical processes (see 5.2.2 - Number of persons required per task).

The trusted roles are:

- **PKI Director**
  The PKI Director represents SG-PKI in the FOITT directorate and is the primary responsible for SG-PKI. He takes the overall responsibility for keeping the TSP compliant.
- **PKI Security Officers**
  PKI Security Officers are responsible for enforcing compliance with all legal requirements, for the adherence to physical and functional security policies by SG-PKI and its environment. They manage the physical access control to the certification platform. PKI Security Officers report to the PKI Service & Design Manager.
- **System Administrators**

  The System Administrator / System Engineer are authorized to install, configure and maintain TWSs for service management. The System Administrator / System Engineer installs and configures all service software, including TSP key management. The System Administrator / System Engineer is responsible of the CA system and the HSM Backup. Administrators do not issue Certificates to Subscribers.

  The System Administrator / System Engineer installs and configures system hard- und software, including servers, routers, firewalls, and network configurations. The System Administrator / System Engineer also keeps critical systems updated with software patches and other maintenance needed for system stability and recoverability.
- **System Operators**

  System Operators are responsible for operating TWSs on a day-to-day basis. They are authorized to perform system backup and recovery.
- **System Auditors**

  The auditor role is responsible for:

  - Reviewing, maintaining, and archiving audit logs; and
  - Performing or overseeing internal compliance audits to ensure that the CA is operating in accordance with its CPS and this CP.
- **Registration Officer**

  PKI Registration Authority is responsible for the validation of certification requests on behalf of the Issuing CA.
- **Revocation Officer**

  Representative for revocation: Responsible for implementing changes to the certificate status.
- **PKI Management Board**
  The PKI Management Board consists of the PKI Operations Manager and the PKI Service & Design Manager. Its function is to combine the Strategic, Security and Operational view on the SG-PKI. Its main tasks are reviewing and approving security- and certification policies.
- The PKI Management Board reports to the PKI Director

5.2.2 Number of persons required per task

With the exception of the standard tasks performed by PKI Operators, security critical actions REQUIRE at least two individuals having different roles (see 5.2.1 Trusted roles) to jointly execute the steps. These actions include generating, activating, deactivating, backing up and recovering as well as

destroying CA keys in hardware security modules HSM, issuing, re-keying and revoking CA certificates.

5.2.3 Identification and authentication for each role

SG-PKI runs a tight access rights management and control for identifying and authenticating its personnel handling the certification processes. The access control uses security mechanisms capable of separating the different trusted roles detailed in 5.2.1 - Trusted roles and 5.2.2 - Number of persons required per task and identifying the specific functions within a role each of the role owners actually fulfills at any time, according to the security goals specified in section 6.5 - Computer security controls.

5.2.4 Roles requiring separation of duties

The PKI Director assigns roles to the different SG-PKI employees, ensuring that no conflicts regarding the separation of duties arise, e.g. members of PKI Operation MAY NEVER be PKI Security Officers and vice versa.

5.3 Personnel Controls

5.3.1 Qualifications, experience and clearance requirements

Swiss Government Root CA IV and its Issuing CAs are operated by qualified and experienced employees of the Swiss federal administration. They are appointed for an indefinite period of time, and normally they are assigned on a full-time basis to tasks associated with their responsibilities within the framework of the certification platform.

Each employee is personally informed by the PKI Security Officers of the extent and limits of his area of responsibility.

Each employee’s employment contract contains a special confidentiality clause.

Any person engaged in the process of Certificate Management, whether as an employee, agent or an independent contractor MUST be authenticated using a smart card based on a Certificate of type “Klasse B” issued under the Swiss Government Root CA I as specified in 1.5.1 - Definitions and Background Checks as specified in 5.3.2 - Background check procedures MUST be performed.

5.3.2 Background check procedures

To get assigned a SG-PKI role, SG-PKI staff are subjected to a security review as per the ordinance on security checks for persons [6].

5.3.3 Training requirements

SG-PKI staff MUST be familiar with the software, hardware and internal operational workflows of the certificate infrastructure components they work with. They MUST understand the processes they are involved in and understand the effects of all actions they take.

5.3.4 Retraining frequency and requirements

Each employee assigned a SG-PKI task receives an initial training covering the PKI system operated, its organization, security policy, emergency plans, software used and the activities he’ll be tasked with.

Each SG-PKI employee SHALL complete the necessary training after each major enhancement of system, organization, tools and/or methods.

5.3.5 Job rotation frequency and sequence

There is no job rotation established.

5.3.6 Sanctions for unauthorized actions

Unauthorized actions by SG-PKI staff are sanctioned as regulated by the federal act on the responsibility of the Swiss confederation, the members of its official bodies and their officers [11].

5.3.7 Independent contractor requirements

The security requirements for temporary employees or contractor's employees are identical to the ones for SG-PKI employees (see 5.3.1 - Qualifications, experience and clearance requirements, 5.3.2 - Background check procedures, 5.3.3 - Training requirements and 5.3.4 - Retraining frequency and requirements).

5.3.8 Documentation supplied to personnel

SG-PKI staff has access to the entire documentation of Swiss Governments' PKI and, in particular, to the following documents:

- Certificate Policy and Certification Practice Statement of the Swiss Government Root CA IV (this document).
- SG-PKI security policy [14].
- SG-PKI manual on operation and organization [16].
- Manuals on the hard- and software being used by the PKI system and applications.

5.4 Audit Logging Procedures

5.4.1 Types of events recorded

All relevant events related to the issuance and maintenance of SG-PKI certificates are logged 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 requestor, 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 SG-PKI's operating manual 'periodic monitoring or functions and activities' [16] Retention period for audit log

All log files are retained for at least eleven years following the end of the lifecycle of the Swiss Government Root CA IV.

5.4.3 Protection of audit log

PKI log data is signed by the certification application and stored encrypted on a dedicated server located off-site. Only PKI Security Officers and PKI Operations Backend are authorized to access server and log files.

5.4.4 Audit log backup procedures

The log files are backed up daily as part of SG-PKI's routine backup of its host system.

5.4.5 Audit collection system

A dedicated server within SG-PKI's infrastructure collects all log files maintained.

5.4.6 Notification to event-causing subject

PKI Operations Backend analyzes the log files daily and notifies PKI Security officers and the members of PKI Operation Backend staff of critical incidents. The event-causing subject is not informed.

5.4.7 Vulnerability assessments

SG-PKIs security program includes an annual Risk Assessment that:

- Identifies foreseeable internal and external threats that could result in unauthorized access, disclosure, misuse, alteration, or destruction of any Certificate Data or Certificate Management Process
- Assesses the likelihood and potential damage of these threats, taking into consideration the sensitivity of the Certificate Data and Certificate Management Process
- Assesses the sufficiency of the policies, procedures, information systems, technology, and other arrangements that SG-PKI has in place to counter such threats

A dedicated application analyzes SG-PKI's PKI systems at least once a week, identifying vulnerabilities and potential attempts at breaching the security of the system.

5.5 Records Archival

5.5.1 Types of records archived

SG-PKI archives all relevant data and log files relating to the issuance and maintenance of certificates. In particular, these are:

- Contractual agreements with clients.
- All certificates issued for Root CA, Issuing CAs and subscribers.
- All CRLs issued.
- Requests for revocation where electronically available.
- Subscribers' identification data together with all information supporting the registration and copies of the documents presented.
- Log files.
- Audit reports.

5.5.2 Retention period for archive

SG-PKI retains archived data for at least eleven years following the end of the lifecycle of the Swiss Government Root CA IV.

5.5.3 Protection of archive

Archived data is stored encrypted on two servers in two different, secured locations off-site.

All access to archives has to be formally authorized by the PKI Auditor.

Only PKI security officers are authorized to access the archived data in the presence of a second SG-PKI staff member (four eyes principle).

5.5.4 Archive backup procedures

All data to be archived is copied simultaneously to the off-site back-up servers.

5.5.5 Requirements for time-stamping of records

Each event registered, and, subsequently archived, gets time-stamped on the basis of the central date/time reference provided by FOITT.

5.5.6 Archive collection system

All data to be archived is integrity protected by hash-values and collected in a specific database running on a server within FOITT's central IT infrastructure. The DB's contents are then archived in a storage area network

5.5.7 Procedures to obtain and verify archive information

Archived information can only be retrieved by PKI Security Officers from the backup servers. There aren't any procedures in place for verifying archive information.

5.6 Key Changeover

None of the subordinate CA's support key changeover. Instead, the CA re-keys and uses the new CA key for signing subscriber certificates early enough for all subscriber certificates signed by the original CA key to expire within the validity period of the issuing CA's original certificate.

5.7 Compromise and Disaster Recovery

5.7.1 Incident and compromise handling procedures

SG-PKI plans procedures for incident and compromise handling and a Business Continuity Plan is established. The documents are not publicly disclosed.

The planned procedures are regularly tested and updated as needed.

All Backup / Recovery Systems are tested at least once a year.

5.7.2 Recovery procedures if Computer resources, software and/or data are corrupted

All active keys and certificates used by Swiss Government Root CA IV and its Issuing CAs are backed up off-site in at least two security modules at all times. All data related to the issuance and maintenance of end-user certificates is backed up daily as well.

Data on the registration and certification processes are backed up incrementally by the CAs' databases.

TSA Keys are not backed up. In case of loss they will be newly generated.

5.7.3 Entity private key compromise procedures

In case any of the CA or TSA keys should have been compromised or is suspected to be compromised, the SG-PKI Director activates the predefined action plan. In particular, this comprises the following steps:

- Inform supervisory authorities.
- Inform all subscribers concerned.

- Revoke all subscribers' certificate signed by the compromised key,
- Revoke the CA's certificate (by Swiss Government Root CA IV) and publish an updated ARL.
- Generate and certify a new key pair for the CA.
- Issue new certificates for the subscribers concerned.
- Inform software vendors supporting SG-PKI CA certificates as trust anchors and provide them with the necessary updates.

If the key of Swiss Government Root CA IV should have been compromised the above measures are carried out for all Issuing CAs and their subscribers as well as for the Root CA itself.

5.7.4 Business continuity capabilities after a disaster

There is an emergency facility available, capable of running SG-PKI's Swiss Government Root CA IV and its Issuing CAs and TSA with all necessary processes within seven days after a disaster.

5.8 CA or RA termination

5.8.1 Termination of SG-PKI

In case SG-PKI decides to terminate CA operation[5], it will inform the supervisory authorities and all subscribers at least 30 days in advance before it stops the certification activities in conjunction with Swiss Government Root CA IV.

All valid certificates, including Swiss Government Root CA IV and Issuing CA certificates and TSA, will be revoked and a final CRL and ARL published on FOITTs website for a minimum of eleven years. The Swiss Government Root CA IV key and the ones of the Issuing CAs inclusive of all backup copies will be destroyed.

The responsibility for all certification data archived (see section 5.5) will be handed over to a custodian to be named by FOITT's management and will be retained for at least eleven years.

5.8.2 Termination of a LRA

In case the activities of a LRA are to be terminated SG-PKI updates its lists of operational LRAs accordingly and, where necessary, amends its SLA with the administrative unit responsible for the LRA. The respective registration data is archived (by the standard archival process, see 5.5) and will be retained.

[5] The federal authorities don't plan to hand over their certification services to any other provider in such a situation.

6 Technical Security Controls

6.1 Key pair generation and installation

6.1.1 Key pair generation

- Root CA Key pair generation

  Root CA Key pairs are generated by following a Key Generation Script and have a PKI Security Officer, a PKI Operator, a Qualified Auditor and a Notary to witness the Root CA Key Pair Generation Ceremony. The Swiss Government Root CA IV Key Pair Generation Ceremony is documented and logged.

  Root CA Key pairs are generated in HSMs conformant to FIPS 140-2 Level 3 or [42] within the secured facilities of SG-PKI (5.1.1 - Site location and construction).

- Subordinate CA key pair generation

  Subordinate CA Key pairs are generated by following a Key Generation Script and have a PKI Security Officer, a PKI Operation Backend Staff member and an independent Witness to witness the Subordinate CA Key Pair Generation Ceremony. The Subordinate CA Key Pair Generation Ceremony is documented and logged.

  Subordinate CA Key pairs are generated in HSMs conformant to FIPS 140-2 Level 3or [42] within the secured facilities of SG-PKI (5.1.1 - Site location and construction).

- TSA key pair generation

  TSA CA Key pairs are generated by following a Key Generation Script and have a PKI Security Officer, a PKI Operation Backend Staff member and an independent Witness to witness the TSA Key Pair Generation Ceremony. The TSA Key Pair Generation is documented and logged.

  TSA Key pairs are generated in HSMs conformant to FIPS 140-2 Level 3 or [42] within the secured facilities of SG-PKI (5.1.1 - Site location and construction).

- Subscriber key pair generation

  [QCP-n] The key pairs are generated in presence of the applicant in a QSCD conformant to [45] / [46].

  [RCP-l] The key pairs are generated in presence of the applicant in a QSCD conformant to [45] / [46] centrally within the secured facilities of SG-PKI. The token is handed over to the applicant only after the respective certificates have been issued and stored on the token as well.

  [TW4S] For TW4S use, private keys to be certified are generated directly in a HSM, located together with the corresponding SAM, in a tamper-resistant environment in the facilities of SG-PKI. A signing key must only be associated with one signer and with one public key certificatePrivate key delivery to subscriber.

  [QCP-n] Private keys to be certified are generated in a QSCD conformant to [45] / [46] at LRAs in the presence of the respective subscribers. The QSCD with keys and certificates are handed to the subscribers by LRA officers once registration and certification have been accomplished.

  [RCP-l] Private keys to be certified are generated in a QSCD conformant to [45] / [46] centrally within the secured facilities of SG-PKI. The QSCD with keys and certificates are then handed to the subscribers by the LRA officer once registration and certification have been accomplished.

  [TW4S] For TW4S use, private keys remain on the HSM where they were generated.

6.1.2 Public key delivery to certificate issuer

Applicant's public key is delivered to the CA within the certificate signing request.

6.1.3 CA public key delivery to relying parties

Relying Parties can get the Swiss Government Root CA IV and Issuing CA certificate from the Directory Service or the SG-PKI website.

SG-PKI publishes the certificates of Swiss Government Root CA IV and its Issuing CAs

- in Admin-Directory,
- on its Website http://www.pki.admin.ch .

On request FOITT's Service Desk provides a copy of the Swiss Government Root CA IV certificate's fingerprint for verification.

6.1.4 Key sizes

Swiss Government Root CA IV and its Issuing CAs all use keys of 4096 bits in size.

Subscribers to the subordinate CAs use keys of 2048 bits in size.

6.1.5 Public key parameters generation and quality checking

- All CA keys are generated by HSMs conformant to FIPS 140-2 level 3.
- [QCP-n] Subscriber's qualified keys are generated by QSCD conformant to [45] / [46] or, with central key generation, by HSMs conformant to FIPS 140-2 level 3 or [42].
- [RCP] Keys that are used for regulated certificates issued to a legal person are generated by QSCD conformant to [45] / [46] or, with central key generation, by HSMs conformant to FIPS 140-2 level 3 or [42]
- [TW4S] All keys used for TW4S signing are generated by HSMs conformant to FIPS 140-2 level 3 or [42].

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

The key usage flags are populated automatically in all Swiss Government Root CA IV, CA and end-user certificates issued.

SG-PKI ensures Root CA and CA private keys are strictly used as indicated by the flags.

Swiss Government Root CA IV keys are not used to sign certificates except in the following states:

- Self-signed certificates to represent the Swiss Government Root CA IV itself
- Certificates for Infrastructure purposes

Subscribers are bound by the frame contract with SG-PKI to use their private keys only for the purposes indicated in the respective certificates as well.

6.2 Private Key protection and cryptographic module engineering controls

6.2.1 Cryptographic module standards and controls

SG-PKI CAs use modules (HSMs and QSCD) conformant to FIPS 140-2 Level 3 or [42] (see also 6.1 Key pair generation) or [42].

[QCP-n], [RCP] All subscribers for qualified or regulated certificates use modules (HSMs and QSCD)

conformant to FIPS 140-2 Level 3 or [45] / [46] (see also 6.1 Key pair generation).

QSCD certifications are monitored and appropriate adjustments are made if certification is lost.

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

All activities involving Root CA or CA keys except signing certificates and CRLs require the presence of at least two authorized SG-PKI staff members. In particular these are the generation, backup and recovery, activation and deactivation of the keys and the exchange of HSMs.

6.2.3 Private Key escrow

Since the Swiss federal law on electronic signatures ZertES [2] explicitly prohibits escrow of signature keys of qualified or regulated certificates, no escrow of these keys is done under this CP/CPS. This includes TSA private keys.

6.2.4 Private Key backup

Root CA and CA private keys are backed up in at least two HSMs stored in separate, secure locations off-site. For activating backup HSMs at least two appropriately authorized SG-PKI staff are required.

TSA private keys are not backed up.

Subscribers' keys will not be backed up in any way.

6.2.5 Private Key archival

There are no private keys archived.

6.2.6 Private Key transfer into or from a cryptographic module

Root CA and subordinate CA private keys are transferred between HSMs for backup purposes. The transfers require two SG-PKI staff authorized for the task, the keys to be transferred are encrypted.

[QCP-n], [RCP] Subscribers' keys are never transferred.

6.2.7 Private Key storage on cryptographic module

Root CA and Issuing CA's private keys are stored within the HSMs and marked 'not exportable'.

[QCP-n], [RCP] Subscribers' keys are stored un-encrypted in a secure container in the QSCD.

[TW4S] Subscriber keys are stored within a dedicated HSMs and marked 'not exportable'.

6.2.8 Method of activating private key

Root CA and Issuing CA's private keys are activated with the launching of the certification application by the security officer. The activation process requires the presence of at least one SG-PKI staff authorized for the task beside the PKI Security Officer.

[QCP-n], [RCP] Subscribers activate their QSCD and private keys by entering the token PINs.

[TW4S-QCP-n] Subscribers activate their private key token using a smartcard based 2factor authentication.

[TW4S-RCP] Subscribers activate the private key token using the authentication implemented a by the corresponding specialist application.

6.2.9 Method of deactivating private key

The deactivation process requires two SG-PKI staff members authorized for the task beside the PKI Security Officer.

[QCP-n], [RCP] Subscribers' private keys are deactivated when the QSCD are powered off, i.e. either with the removal of the tokens or the closing down of the subscribers' workstation.

[TW4S] Subscribers' private keys are deactivated by closing the signature application.

6.2.10 Method of destroying private key

Root CA and Issuing CA's private keys are destroyed by the HSMs in that the respective locations in HSMs memory are actively overwritten. The process requires at least two SG-PKI staff members authorized for the task.

[QCP-n], [RCP] Subscribers' private keys are destroyed by destroying the respective QSCD.

[TW4S] Subscribers' private keys are deleted in a dedicated process by the LRAO.

6.2.11 Cryptographic module rating

The Swiss Government PKI monitors continuously the certification status of the HSM. Should the suitability of an HSM expire in the foreseeable future, a project will be initiated to replace the used HSMs with newer ones that fulfill the compliance regulations.

6.3 Other aspects of key pair management

6.3.1 Public key archival

All public keys – Root CA's, Issuing CAs' and subscribers' – to be used for verification purposes are archived as integral parts of the certificates issued for at least eleven years (for details on archival see 5.5).

6.3.2 Certificate operational periods and key pair usage period

SG-PKI certificate validity periods are:

- 25 years for Swiss Government Root CA IV.
- 15 years for the Issuing CAs.
- a maximum of 3 years for end-user certificates.

The usage periods for the private signature keys are:

- a maximum of 3 years for end-user certificates. End-user certificates expire within the validity period of the issuing CA's original certificate.

The usage periods for private authentication keys and for public encryption keys are not explicitly limited, these expire together with the respective certificates. The public signature verification keys and the private decryption keys don't expire as they might be needed for verifying signatures or decrypting documents/data long after the respective certificates have expired.

6.4 Activation data

6.4.1 Activation data generation and installation

Root CA, Issuing CA:

- The activation data of the Root CA keys and the Issuing CA keys are generated during the Root or Issuing Key Ceremony supervised by PKI Security Officers.
- Activation data for the HSMs storing Root CA and Issuing CA keys is generated individually by the different authorized SG-PKI staff members. The passphrases and parameters are then entered as advised by the HSM's provider.

QSCD:

Activation data for the QSCD – PINs and PUKs – is generated and entered in either of the following ways:

[QCP-n-qscd, QCP-l-qscd] Smartcard as QSCD: PIN and PUK are entered by the subscriber at the time of registration.

[TW4S] HSM as remote QSCD for (TW4S)' according to ETSI EN-419241-1 and -2: Activation data is generated and controlled by the SAM of the relevant TW4S-Software.

6.4.2 Activation data protection

Root CA and Issuing CA keys:

SG-PKI staff members possessing parts of one or more HSMs' activation data MUST keep this data locked at all times unless there is a HSM to be activated or deactivated.

Subscribers Keys:

Subscribers are obliged to keep the activation data (PIN, PUK or passphrase) secret at all times.

6.4.3 Other aspects of activation data

Activation data for HSMs MUST comply with the rules laid down in SG-PKI's Security Policy (see [14]).

In the course of registration, the LRA officers instruct subscribers on how to adequately protect access to their QSCD and private keys and the possible consequences of neglect in that respect.

6.5 Computer security controls

6.5.1 Specific computer security technical requirements

SG-PKI uses mandatory access control with all applications used to operate its PKI services. With critical processes, segregation of duties is enforced.

6.5.2 Computer security rating

No stipulation.

6.6 Life cycle technical controls

6.6.1 System development control

Applications are developed and implemented by SG-PKI in accordance with SG-PKI and FOITT systems development and change management standards. SG-PKI operates a configuration management tool ensuring only approved and tested hard- and software is deployed. Changes are simulated on an acceptance environment before going into production.

6.6.2 Security management controls

PKI Security Officers regularly verify the integrity of the certification service's components. Appropriate malware countermeasures are established and monitored.

The verification and monitoring results are documented and retained.

6.6.3 Life cycle security controls

System Administrators and PKI Security Officers SHALL monitor development, operation, and maintenance of the SG-PKI system and regularly evaluate the effectiveness through audit.

6.7 Network security controls

SG-PKI's PKI systems is operated in a specific network-segment separated from the federal administration's intranet by a gateway acting as a firewall. This blocks all protocols which are not absolutely necessary for SG-PKI's operations. All private network communications are protected through integrity checks and encryption mechanisms.

The Swiss Government Root CA IV is operated in an offline state and only activated to generate new CRL's for the issuing CAs.

6.8 Time-stamping

SG-PKI provides a qualified time-stamping service supporting electronic signing under the Swiss Government Root CA IV conformant to [27]. SG-PKI operational rules apply likewise for the time-stamping service, for details see the time stamping authority's policy [17].

All SG-PKI Systems are time synchronized by using NTP, referring the time source provided by FOITT at least once a day.

7 Certificate, CRL and OCSP Profiles

All Swiss Government Digital Certificates conform to Digital Certificate and Certificate Revocation List profiles as described in RFC 5280 [36] and utilize the ITU-T X.509 version 3 Digital Certificate standard.

[QCP-n] [RCP] Certificates and CRLs issued by Swiss Government Root CA IV and the Issuing CAs conform to the technical and operational requirements specified by ZertES (see [2], article 3.4).

7.1 Certificate profile

Unless it is explicitly indicated, certificates issued for Swiss Government Root CA IV, its subordinate CAs and end-users adhere to the identical profile.

7.1.1 Version number(s)

SG-PKI qualified and enhanced certificates are of version 3, issued in accordance with recommendation X.509 v3.

7.1.2 Certificate extensions

Certificate extensions used with Swiss Government Root CA IV's and subordinate issuing CA's certificates:

Extension	Objective	Criticality
Authority Key Identifier	Identifies key used by issuer of certificate.	not critical
Subject Key Identifier	Identifies key used by subject of certificate.	not critical
Key Usage	Lists intended usages of private key.	critical
Certificate Policies	Identifies policy governing the operation of the Root CA (the current CP/CPS).	not critical
Basic Constraints	1. Indicates type of certificate subject: CA or end-user (here: CA). • Indicates how many CA levels MAY be subordinated to CA: For the Swiss Government Root CA IV the pathLenConstraint field is not present according to [BR] clause 7.1.2.1 (no limit given). For the Issuing Cas the pathLenConstraint field is present according to [BR] clause 7.1.2.2 (limit is 0).	critical
CRL Distribution Points	Lists address(es) where status information on certificate may be found. *Not included in the Root CA certificate*	not critical
AIA	Authority Information Access list address(es) to download the Authority certificate and the access point for OCSP requests. *Not included in Root CA certificate*	not critical

Table 11 : Swiss Government Root CA IV and CA certificate extensions

Certificate extensions used with end-user certificates:

Extension	Objective	Criticality
Authority Key Identifier	Identifies key used by issuer of certificate.	not critical
Subject Key Identifier	Identifies key used by subject of certificate (the end-user).	not critical
Key Usage	Lists intended usages of private key.	critical
Certificate Policies	Identifies policy governing the operation of the Root CA (the current CP/CPS).	not critical
CRL Distribution Points	Lists address(es) where status information on certificate may be found.	not critical
Authority Information Access	list address(es) to down-load the Authority certificate and the access point for OCSP requests	Not critical

Table 12 : End-user certificate extensions

7.1.3 Algorithm object identifiers

There are two algorithms used in conjunction with SG-PKI qualified and enhanced certificates identified by an OID:

- OID 1.2.840.113549.1.1.11 identifies algorithm ‘sha256WithRSAEncryption’, the algorithm SG-PKI uses for signing certificates throughout.
- OID 1.2.840.113549.1.1.1 identifies algorithm ‘rsaEncryption’, the algorithm to be used for verifying electronic signatures generated by SG-PKI’s subscribers.

7.1.4 Name forms

Swiss Government Root CA IV and the Issuing CAs are identified in the certificates (as issuer and/or subject) as follows (see also 3.1.1 - Types of names):

Extension	Objective
Common Name (cn)	Swiss Government <Name of individual CA>
Organization (o)	Bundesamt fuer Informatik und Telekommunikation (BIT)
Organizational Unit (ou)	Swiss Government PKI
Organization Identifier	NTRCH-CHE-221.032.573
Country (c)	CH

Table 13 : CA name forms

[QCP-n] Subscribers are identified as certificate subjects in the following way:

DN Field	Value
Common Name (cn)	<Lastname> <Firstname> <Suffix>
GivenName	<First Name of Subscriber identical to the presented ID Document>
Surname	<Last Name of Subscriber identical to the presented ID Document >
SubjektAltName	eMail Address
Country (c)	CH

Table 14 : Subscriber name forms

[RCP-l] Subscribers are identified as certificate subjects in the following way:

DN Field	Value
Common Name (cn)	<Name commonly used for the organization>
Organizational Unit (ou)	<More detailed designation of the organizational unit (department, division, etc.) that is assigned to the certificate. Multiple OU fields can be specified.> This field is optional.>
Organizational Unit (ou)	<More detailed designation of the organizational unit (department, division, etc.) that is assigned to the certificate. Multiple OU fields can be specified.> This field is optional.
Organizational Unit (ou)	<Authority identification: GE - 0220 - Office abbreviation or designation federal authority (federal office). GE - 0221 - Cantonal abbreviation - Official abbreviation or designation cantonal authority GE - 0222 - Cantonal abbreviation - Hist. BFSNR - Official abbreviation or designation Authority of a district GE - 0223 - Hist. BFSNR - official abbreviation or designation municipal authority> This field is mandatory.
Organization (o)	<Organization name. MUST be an exact copy of the name as defined in the Swiss UID-register [35]>
Organization Identifier (oi)	<according to clause 5.1.4 of 'ETSI EN 319 412-1' [28]. The syntax is: NTRCH-CHE-999.999.999, where CHE-999.999.999 represents the enterprise identification number (UID) [35]>
Bussines Category	<"governmental Institution" This field is optional.>
Locality (l)	<Locality where the organization is located>
State or Province (st)	<State or Province where the organization is located>

DN Field	Value
SubjektAltName	<Mail address that may be listed in a verification report during an automated verification of an electronically sealed document to indicate the information point for the signed document type.> This field is optional.
Country (c)	CH

7.1.5 Name constraints

Name constraints are not used by SG-PKI with the issuance of regulated and qualified certificates.

7.1.6 Certificate policy object identifier

The OIDs of the policies used by the different issuing CAs und the Swiss Government Root CA IV are listed in ‘1.1.2 - Certificates issued under this CP/CPS’. Usage of policy constraints extension

Policy constraints are not used by SG-PKI with the issuance of qualified and regulated certificates.

7.1.7 Policy qualifiers syntax and semantics

The policy including policy qualifiers and semantics of the subscriber certificates follow the requirements as defined in clause 2.3.2 of ‘Ordinance of OFCOM for certification services supporting electronic signatures and other applications of digital certificates’ [4].

7.1.8 Processing semantics for the critical certificate policies extension

With the issuance of qualified and enhanced certificates the certificate policies extension is set to ‘not critical’, SG-PKI doesn’t expect relying parties to process policy information electronically.

[RCP] The syntax of the attribute organizationIdentifier follows the specifications set up in clause 5.1.4 of ‘ETSI EN 319 412-1: Electronic Signatures and Infrastructures (ESI);Certificate profiles; Part 1 Overview and common data structures’ [28].

7.2 CRL profile

7.2.1 Version number(s)

CRLs generated by SG-PKI qualified and enhanced CAs are of version 2,

7.2.2 CRL and CRL entry extensions

CRL and CRL entry extensions used with Swiss Government Root CA IV's and subordinate CAs' certificates are:

CRL Extension	Objective	Criticality
CRL number	Number of CRL (CRLs are sequentially numbered).	not critical
CRL Entry Extension		
Certificate Serial Number	Serial Number of the revoked certificate	not critical
Reason Code	Identifies actual reason for revoking certificate. The reason code shall be surpressed.	not critical
Invalidity Date	Indicates known or suspected date a key was compromised.	not critical
expiredCertsOnCRL	Indicates that expired certs will not be removed from CRL	not critical

Table 15 : CRL and CRL entry extensions

7.3 OCSP profile

The SG-PKI OCSP responders implement either the RFC 6960 profile [QCP-n] or the RFC 2560 profile [RCP].

7.3.1 Version number(s)

The SG-PKI OCSP responders operate in Version 1.

7.3.2 OCSP extensions

OCSP Signer Extension	Objective	Criticality
Key Usage	digitalSignature	Critical
Extended Key Usage	OCSP Signing (OID: 1.3.6.1.5.5.7.3.9)	not critical
Subject Alternative Name	DNS-Name=<DNS-Name of OCSP-Responder>	not critical
1.3.6.1.5.5.7.48.1.5	No check	not critical
OCSP Response Extension		
Version	1	Critical
Extended Key Usage	OCSP Signing (OID: 1.3.6.1.5.5.7.3.9)	not critical
Status	good, revoked (RFC 2560) or good, revoked, unknown (RFC 6960)	
This update	Time OCSP response starts to be valid	
Next update	Time OCSP response ends to be valid	

Table 16 : OCSP Signer and OCSP Response extensions

8 Compliance Audit and other Assessments

8.1 Frequency or circumstances of compliance audit and other assessments

Compliance Audit:

[QCP-n], [RCP] Swiss Government Root CA IV together with the Issuing CAs issuing qualified and regulated certificates are subject to the provisions of the Swiss Digital Signature Law (ZertES [2]). Accordingly, a recertification of Swiss Government Root CA IV and the Regulated CA 02 is conducted yearly by the Certification Body (see 1.2.5. - Other participants).Compliance with this CP/CPS:

Swiss Government Root CA IV and its Issuing CAs are subject to a verification of their compliance with the requirements of this CP/CPS at least yearly. These audits are done by the Auditor (see 5.2.1 - Trusted roles).

Self-Audits:

SG-PKI performs regular internal self-audits. All PKI participants MAY be subject to this internal audit. This requirement is part of the Subscriber Agreement and Terms & Conditions of SG-PKI.

SG-PKI system configurations are compliance checked at least bi-annually.

8.2 Identity/qualifications of assessor

- The Certification Body MUST be accredited by the Swiss Accreditation Service to perform the specific audits.
- The Auditor assigned by FOITT is an independent company carrying out audits in accordance with the statutory and regulatory provisions.

8.3 Assessor’s relationship to assessed entity

The audits are conducted by organizations mandated by FOITT, completely independent of the federal administration.

In addition to the foregoing prohibition on conflicts of interest, the assessor SHALL have a contractual relationship with SG-PKI or FOITT for the performance of the audit, but otherwise, SHALL be independent. The assessor SHALL maintain a high standard of ethics designed to ensure impartiality and the exercise of independent professional judgment, subject to disciplinary action by its licensing body.

8.4 Topics covered by assessment

Audits on the services issuing qualified certificates verify that all respective requirements emanating from the federal laws on electronic signatures are met by SG-PKI.

The audits ordered by FOITT cover SG-PKI’s adherence to this CP/CPS in terms of its organization, operation, personnel training and management.

8.5 Actions taken as a result of deficiency

The PKI Auditor agrees with the assessor on the necessary actions and time schedules to correct/eliminate the deficiencies identified. They’ll jointly see to the initiation and successful completion of the resulting tasks.

PKI Security Officers are responsible to track the necessary actions and report to the PKI Management Board the actual status of completion.

8.6 Communication of results

Audit results are just communicated to PKI Director, PKI Auditor and PKI Security Officers as a standard and, where advisable, to other employees/units of the federal administration on a ‘need to know’ basis.

9 Other Business and Legal Matters

9.1 Fees

SG-PKI's costs for running the certification services basing on Swiss Government Root CA IV and all subordinate CAs are covered by the administrative units at federal, cantonal or communal level employing the certificate subscribers, as agreed in the respective SLA.

The costs for providing registration services (registering and supporting applicants, etc.) are covered by the administrative units running the LRA.

Costs arising on subscriber's side are covered by the responsible administrative unit or company/organization.

Due to the fact that there aren't any further fees according to the sub chapters from RFC 3647 (see 9.1 ff) these chapters (9.1.1 - 9.1.5) are not listed below.

9.2 Financial responsibility

9.2.1 Insurance coverage

By its declaration of 1 June 2006, the FDF has confirmed it is liable for SG-PKI's certification services, thereby eliminating the need for insurance (as per paragraph 2 of the article).

Registration Agents MUST ensure they are adequately insured against damages caused by their registration activities.

9.2.2 Other assets

The cantonal and communal administrations' liability is regulated in an appendix to their respective SLA.

9.2.3 Insurance or warranty coverage for end-entities

Subscribers MUST ensure they are adequately insured against damages caused by their using SG-PKI certificates (e.g. signing documents).

9.3 Confidentiality of business information

9.3.1 Scope of confidential information

The following data is regarded as internal and treated according to the Federal Act on Data Protection (FADP) [10]:

1. All subscriber related data which are not shown in certificates or CRLs.
2. Audit logs generated with SG-PKI's operation of the certification services and all data archived.
3. Audit reports and any other assessment results.

9.3.2 Information not within the scope of confidential information

Explicitly not within the scope of internal information are:

- All data on subscribers shown in certificates and CRLs are not confidential; these are usually published formally (see section 2).
- SG- PKI documents intended for subscribers, relying parties and third parties, e.g. this CP/CPS.

9.3.3 Responsibility to protect confidential information

All SG-PKI staff and Registration Agents are responsible for protecting confidential information. PKI Security Officers specify the respective requirements and measures and enforces these in the daily operation.

9.4 Privacy of personal information

All SG-PKI staff and Agents MUST observe the requirements stipulated in the Swiss laws on data protection [10] and on electronic signatures [2], where applicable.

All SG-PKI staff and Agents SHALL collect only subscriber data necessary for registration and certification and use it for these purposes exclusively. In particular, they MUST NOT use subscriber data for any commercial purposes.

9.5 Intellectual property rights

SG-PKI is owner of the intellectual property rights of the following documents:

- Certificate Policy and Certification Practice Statement of Swiss Government Root CA IV (this document).
- Directives for Registration for certificates.
- Contracts and other agreements concluded between SG-PKI and its clients (federal, cantonal and communal administrative units).
- Certificates issued by Swiss Government Root CA IV
- certificates issued by subordinate CAs Swiss Government Regulated CA 02

The reproduction, presentation (including publication and distribution) as a whole or in part, by any means, without SG-PKI's explicit authorization in writing obtained in advance, is strictly forbidden.

Administrative units employing subscribers or subscribers themselves do not acquire ownership of the certificates issued by SG-PKI, they just obtain the right to use these.

9.6 Representations and warranties

9.6.1 CA representations and warranties

SG-PKI is committed to provide its services for issuing qualified and enhanced certificates in compliance the current CP/CPS.

9.6.2 RA representations and warranties

The Registration Agents are committed by contract to do registration in compliance with the current CP/CPS.

9.6.3 Subscriber representations and warranties

Subscribers commit to acquire, use and maintain their private keys, certificates and QSCD in compliance the current CP/CPS and have to accept the SG-PKI Subscriber Agreement.

9.6.4 Relying party representations and warranties

Relying parties SHALL use certificates issued by SG-PKI in accordance with the current CP/CPS.

9.6.5 Representations and warranties of other participants

No stipulation.

9.7 Disclaimers of warranties

All other warranties by any of the parties identified are excluded.

9.8 Limitations of liability

9.8.1 SG-PKI limitation of liability

The liability of the SG-PKI is limited to the extent permitted by applicable law.

SG-PKI is liable in accordance with ZertES, article 17 (see [2]). As far as possible the liability of the SG-PKI is limited to the extent permitted by applicable law. In particular the SG-PKI is not liable for:

- all damages resulting from the usage of certificates or key pairs in any other way than defined in this document, in the SG-PKI instructions or stipulated in the certificate itself,
- all damages caused by force majeure,
- all damages caused by malware (such as virus attacks, Trojans) on the clients infrastructure

9.8.2 Registration Agent's limitation of liability

The cap on Registration Agent's liability is specified in the contract between Registration Agent and SG-PKI. In particular, the Registration Agent is liable for the registration of subscribers and for revoking certificates in case of a misuse.

9.8.3 Subscriber limitation of liability

Limitations of liability of subscribers (employees of federal, cantonal or communal administrations, or of private companies) are as specified in the Federal law on electronic signatures [2]. In particular, the Subscriber is liable for damages caused by a breach of his due diligences (such as handling over token and PIN to somebody else or not revoking his compromised certificate).

9.9 Indemnities

SG-PKI cannot give explicit information on indemnities in addition to the statements in sections 9.6 - Representations and warranties through 9.8. - Limitations of liability

9.10 Term and termination

9.10.1 Term

This CP/CPS becomes valid the day it is published on SG-PKI's website (see section 2.2 - Publication of certification information).

9.10.2 Termination

This CP/CPS is valid until

- it is replaced by a newer version, or
- SG-PKI ceases its activities as issuer of certificates.

9.10.3 Effect of termination and survival

Even once CP/CPS may no longer be valid, the regulations pertaining to the laws on data protection and on archival of information are still observed.

9.11 Individual notices and communications with participants

By default, SG-PKI communicates by e-mail with all participants.

Agreements and contracts are to be exchanged in writing to become effective. Alternatively, the documents MAY be signed electronically and exchanged by email where applicable.

9.12 Amendments

Subscribers will be notified where necessary.

9.12.1 Procedure for Amendment

The PKI Security Officers MAY apply minor changes to this CP/CPS (typographic corrections, revise parts of the document, etc.) autonomously and publish it without notification to the other participants.

9.12.2 Notification Mechanism and Period

Material changes to the CP/CPS MUST be advertised 30 days in advance and be made in agreement with the Certification Body's security officer (see 1.2.5 - Other participants).

9.12.3 Circumstances under which OID SHALL be changed

No stipulation.

9.13 Dispute resolution provisions

The dispute resolution provisions form part of the frame contract concluded between SG-PKI and the subscribers.

Complaints regarding the content or format of a certificate must be submitted in writing or via E-Mail using servicedesk@bit.admin.ch. According to the requirements to the relevant ETSI Standards, SGPKI will react to a notification of a failure or miss issuance of a certificate within 24 hours.

9.14 Governing law

This CP/CPS is subject to the applicable Swiss federal laws, particularly the laws on electronic signatures ZertES (see [2]) and on data protection FADP ([10]). The only place of jurisdiction is Berne.

9.15 Compliance with applicable law

This CP/CPS and rights or obligations related hereto are in accordance with Swiss Law.

9.16 Miscellaneous provisions

No stipulation.

9.17 Other provisions

9.17.1 Legally binding version of CP/CPS

This English version of the CP/CPS is legally binding. Versions of this CP/CPS in other languages serve informational purposes only.