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 I - CP_CPS EN

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

Document OID: 2.16.756.1.17.3.1.0

V3.52, 06.06.2025

Classification *	Not classified
Status **	Freigegeben
Project Name	Swiss Government Root CA I
Auftraggeber	PKI Director
Authors	Jürgen Weber, Daniel Stich, Cornelia Enke, Hans Kramer
Contributors	Cornelia Enke
Reviewers	PKI Management Board
Approved by	PKI Management Board
Distribution	Subscribers, Swiss Government PKI Employees, Auditors, Third Parties https://www.pki.admin.ch/cps/2_16_756_1_17_3_1_0.pdf
Doc_ID	0038-RV-CP-CPS Root_CA_I_(2.16_756_1_17_3_1_0).docx
Short Description	Certificate Policy and Certification Practice Statement of the Swiss Government Root CA I
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
2012/12/20	2.0	J. Weber	Approved
2013/03/06	2.1	J. Weber	Updates and precisions
2016/12/19	2.2	D. Stich	Formal adjustments, consolidation with other CP/CPS. Inclusion of Regulated Certificates, especially Electronic Seal (Behördenzertifikat)
2018/02/02	2.3	A. Clerc	Induction review findings
2018/02/22	2.4	D. Stich, R. Dietschi	Implementation of risk findings
2018/06/20	2.5	D. Stich	finalization prior to approval
2018/09/17	2.6	C. Enke	review prior to approval
2018/10/25	2.7	C. Enke	Adjustment Chapter 1.5.5 new sketch PKI participant documentation of decommissioning of the issuing CAs for Class A certificates
2019/05/15	2.8	D. Stich	Adding of Identification of “Ausweis F”
2019/08/16	2.9	C. Enke	Annual review Adding new CA Hierarchy for the issuance of qualified and regulated certificates Added E-Mail address for complaints
2020/03/30	2.91	C. Enke	Chapter 4.1.1 – adding administrative unit to apply for a subscriber certificate (during recruitment process)
2021/01/05	3.0	C. Enke	Annual Review Documentation Decommissioning of Qualified CA01 Update of several renewed ETSI standards Addition of CIS Corrected description of the PIN Reset User Explanation to expired certs on CRL Update on CRL and OCSP publication interval New issuing CAs • EnhancedCA03 • EnhancedCA04 • EnhancedCA05
2022/07/12	3.1	HW Kramer	Annual Review and fixed missing previous entries
2022/09/16	3.2	HW Kramer	Updated version dates in references and end-user certificate expiration and audit findings.
2022/12/06	3.3	HW Kramer	Streamlined with other CP/CPS
2023/01/13	3.4	HW Kramer	Finalisierte Version zur Freigabe.
2023/03/23	3.5	HW Kramer	New clause regarding subscribers. Reason code shall be suppressed in CRL. Fix typo.
2025/05/27	3.51	C. Enke	annual review • adopted definition for PKI Management Board • removed expired ICA Enhanced CA 1 • Third parties KeyRecovery documented
2025/06/06	3.52	B. Metaj	Formal and textual review for publication

Approval

Date	Version:	Signer 1	Signer 2
2025/06/06	V3.52		
	Roth Beat 0RQGGW 10.06.2025 Info: admin.ch/esignature | validator.ch		Zuercher Roger UXJMSB 10.06.2025 Info: admin.ch/esignature | validator.ch
		Product Manager ID & Trust Services Beat Roth	BO Identity and Access Management Services Roger Zürcher

References

Identifier	Title, Source
[1]	**Minutes of Swiss Government Root CA I root ceremony** Version: 1.0, Date: 15.02.2011 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]	**SR 172.010.59 Verordnung über Identitätsverwaltungs-Systeme und Verzeichnisdienste des Bundes** vom 19. Oktober 2016 (Stand am 1. Januar 2019) Source: https://www.admin.ch/opc/de/classified-compilation/20161261/index.html
[6]	**Ordinance on security checks for persons (VPSPV) of 08.11.2023** Source: AS 2023 736
[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: 01.11.2020, 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 (OV-EFD) of 17.02.2010** Version: 01.01.2022, 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

[1] The document referenced is not available in the public domain, but is ready to be consulted by auditing bodies onsite.

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]
[14]	**Swiss Government PKI security policy** (0027-RV-SG-PKI Betriebliche Sicherheitsprinzipien) Source: Swiss Government PKI internal document[1]
[15]	**Swiss Government PKI manual on operation and organization Chapter 3.2** (Betriebshandbuch (BHB) / Organisationshandbuch (OHB) Certified PKI) Source: Swiss Government PKI internal document[1]
[16]	**Administration der SG-PKI LRA-Officer und RIO** (0100-RV-SGPKI-Administration der LRAOs und RIOs) Source: Swiss Government PKI internal document[1]
[17]	**Swiss Government PKI Registrierrichtlinien Klasse B** (0002-RV-Swiss Government PKI Registrierrichtlinien Klasse B LRA-d) Source: Swiss Government PKI internal document[1]
[18]	**Benutzervereinbarung und Nutzungsbedingungen Klasse B** (0092-RV-Terms and Conditions Class B.docx) Source: Swiss Government PKI internal document[1]
[20]	**Verification of the applicant's identity class B (Überprüfung Identität Antragsteller Klasse B)** (0003-RV-Überprüfung Identität Antragsteller Klasse B) Source: Swiss Government PKI internal document[1]
[21]	**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
[22]	**ETSI EN 319 401: General policy requirements for trust service providers (Electronic Signatures and Infrastructures (ESI) – Certificate Policy and Certification Practices Framework)**
[23]	**ETSI EN 319 4011-1: Electronic Signatures and Trust Infrastructures (ESI);** **Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements**
[24]	**ETSI EN 319 422: Electronic Signatures and Infrastructures (ESI);Time-stamping protocol and time-stamp token profiles**
[25]	**ETSI EN 319 412-1: Electronic Signatures and Infrastructures (ESI);Certificate profiles;** **Part 1 Overview and common data structures**
[26]	**ETSI EN 319 412-2: Electronic Signatures and Infrastructures (ESI);Certificate profiles;** **Part 2: Certificate profile for certificates issued to natural persons**
[27]	**ETSI EN 319 412-3: Electronic Signatures and Infrastructures (ESI);Certificate profiles;** **Part 3: Certificate profile for certificates issued to legal persons**
[28]	**ETSI EN 319 412-4: Electronic Signatures and Infrastructures (ESI);Certificate profiles;** **Part 4: Certificate profile for web site certificates**
[29]	**IETF RFC 3647: Internet X.509 Public Key Infrastructure – Certificate Policy and Certification Practices Framework**
[30]	**IETF RFC 5280 (May 2008): Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile**

Identifier	Title, Source
[31]	**Company Identification Number (CIN) - Unternehmens-Identifikationsnummer (UID)** Source: https://www.uid.admin.ch/Search.aspx
[32]	**Swiss Accreditation Service SAS** Source: https://www.sas.admin.ch/sas/en/home.html
[33]	**ITU-T recommendation T.50** Source: http://www.itu.int/ITU-T/recommendations/rec.aspx?id=2570
[34]	**Swiss Government CA Layout and Policies** Source: CA Layout/Policies und Object Identifier (OID)

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 certificate-based authentication, data integrity and confidentiality protection in the administration's IT networks as well as its electronic document exchange. 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 or to have authorized access to applications of the 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 exclusively on hard-tokens.
2. Swiss Government Root CA II hierarchy issuing internal SSL certificates.
3. Swiss Government Root CA III hierarchy supporting "Lightweight Certificate Policy" certificates and issuing certificates at a lower security level for persons, organizations/organizational units, Shared Mailbox and Systems.
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 QSCDs (Qualified Signature Creation Device) exclusively. CA specific compliance target: All issuing CA under the SwissGovernment Root CA IV are compliant to ZertES [2] The time stamp service offered by the SG-PKI is operated under this CPS and complies with the requirements of ETSI EN 319 421 and ETSI EN 319 422.
5. Swiss Government Root CA VI hierarchy supporting "Lightweight Certificate Policy" certificates supporting automated enrollment and distribution.

The current document describes the Swiss Government Root CA I hierarchy, i.e. CAs enhanced certificates. The CAs of this hierarchy are:

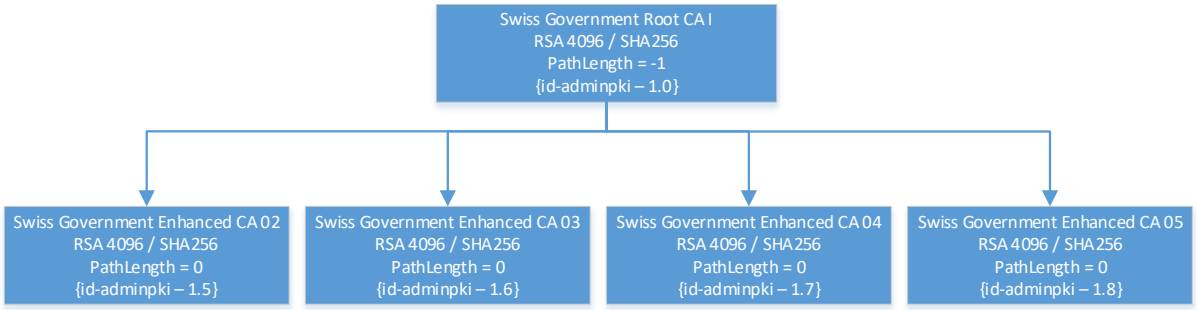

Figure 1 : CA hierarchy ‘Swiss Government Root CA I’

Swiss Government Root CA I (hereinafter referred to as "Root CA") has 4 subordinates CAs (hereinafter referred to as "Issuing CA") that issue enhanced end-user certificates. 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.).

As the above CAs all comply with the identical security requirements, this 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. its certificate policy (CP) and certificate practices statement (CPS) for the Swiss Government Root CA I.
- It also details the policies and practices of the issuing CAs, i.e. it serves as CP and CPS for the CAs, issuing enhanced certificates to end-users and to organizations. 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 Subscriber Certificates issued under this CP/CPS

A detailed description of all certificates issued under this policy is described in the document CA Layout and Policies [34], chapter 2.5.6 for Enhanced CA02, chapter 2.5.7 for Enhanced CA03, chapter 2.5.8 for Enhanced CA04 and chapter 2.5.9 for Enhanced CA05.

The following major subscriber certificates are issued under this CP/CPS.

Certificate Policy (CP)	OID
SG Enhanced CA 02	2.16.756.1.17.3.1.5
SG Enhanced CA 03	2.16.756.1.17.3.1.6
SG Enhanced CA 04	2.16.756.1.17.3.1.7
SG Enhanced CA 05	2.16.756.1.17.3.1.8
Class B Standard (or Prestaged) Encryption	2.16.756.1.17.3.2.10
Class B Standard (or Prestaged) Digital Signature	2.16.756.1.17.3.2.11
Class B Standard (or Prestaged) Authentication	2.16.756.1.17.3.2.15
Class B Prestaged FUB Authentication Swiss Government Enhanced CA02	2.16.756.1.17.3.2.30
Class B Prestaged FUB Signature Swiss Government Enhanced CA02	2.16.756.1.17.3.2.31
Class B Prestaged FUB Encryption Swiss Government Enhanced CA02	2.16.756.1.17.3.2.32
Class B Prestaged BV Authentication Swiss Government Enhanced CA02	2.16.756.1.17.3.2.33
Class B Prestaged BV Signature Swiss Government Enhanced CA02	2.16.756.1.17.3.2.34
Class B Prestaged BV Encryption Swiss Government Enhanced CA02	2.16.756.1.17.3.2.35
Class B Prestaged Authentication Only (for A-Accounts or 2nd Token) Swiss Government Enhanced CA02	2.16.756.1.17.3.2.36
OCSP Responder Swiss Government Enhanced CA 02	2.16.756.1.17.3.2.39
Class B Standard Authentication Only (for A-Accounts or 2nd Token)	2.16.756.1.17.3.2.40
Class B pre-staged (BV): Authentication Only	2.16.756.1.17.3.2.50
Class B SCMS Bund pre-staged Authentication	2.16.756.1.17.3.2.51
Class B SCMS Bund pre-staged Digital Signature	2.16.756.1.17.3.2.53
Class B SCMS Bund pre-staged Encryption	2.16.756.1.17.3.2.52
Class B SCMS Bund pre-staged Authentication Only	2.16.756.1.17.3.2.54
Class B SCMS Bund pre-staged Authentication Only (90-Days)	2.16.756.1.17.3.2.55
Class B FUB Zusatzkarten Auth only	2.16.756.1.17.3.2.67
OCSP Responder Swiss Government Enhanced CA 03	2.16.756.1.17.3.2.68
OCSP Responder Swiss Government Enhanced CA 04	2.16.756.1.17.3.2.69
OCSP Responder Swiss Government Enhanced CA 05	2.16.756.1.17.3.2.70

Table 1: Certificate Types under Swiss Government Root CA I

1.2 Document name and identification

This document is the Swiss Government Root CA I Certificate Policy and Practice Statement. The object identifier (OID) exclusively used for this document is: OID **2.16.756.1.17.3.1.0**.

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 2 below:

Position	OID Component	Meaning of OID Component
1	2	joint-iso-itu-t
2	16	Country

Position	OID Component	Meaning of OID Component
3	756	CH
4	1	organization[2]
5	17	Bundesamt für Informatik und Telekommunikation
6	3	Swiss Government PKI
7	1	Swiss Government Root CA I
8	0	CP/CPS

Table 2 : CP-OID of Swiss Government Root CA I

1.3 PKI participants

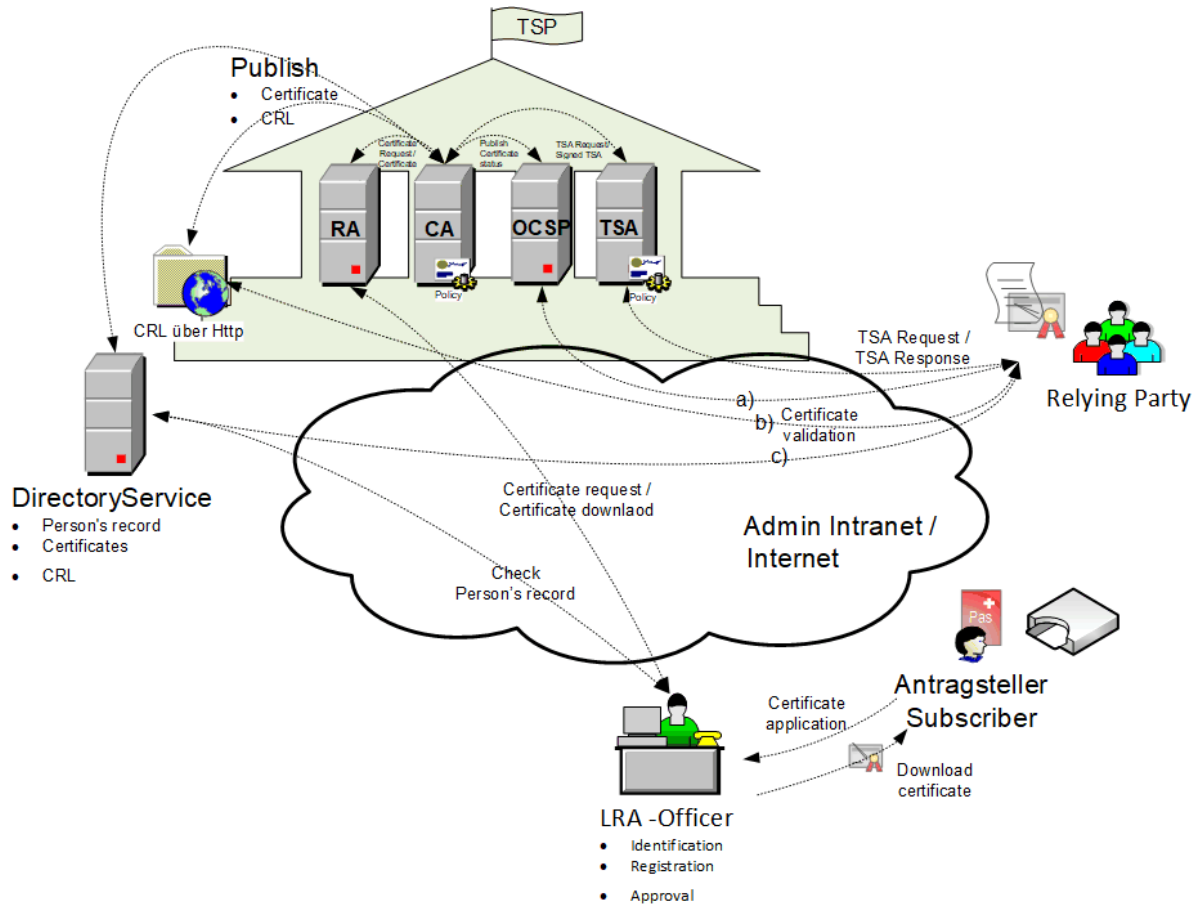

Figure 2 : Overview of PKI participants BV

1.3.1 Certification authorities

1.3.1.1 Root Authorities

1.3.1.1.1 Swiss Government Root CA I

Serial Number	00 fd 75 04 8d 7a 60 86 93 69 4c aa 00 3c 65 d3 3d
Subject DN	CN = Swiss Government Root CA I OU = Certification Authorities OU = Services O = The Federal Authorities of the Swiss Confederation C = CH
Subject Alternative Name	none
Validity Period	From Tuesday, February 15 2011 10:00:00 UTC+1 To Thursday, February 15 2035 09:59:59 UTC+1

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

Public Key	30 82 02 0a 02 82 02 01 00 c8 0e 72 f4 01 2f 86 7b 0b c2 63 b0 8d 68 ed 1f 3d de b9 83 9b 5c a1 5d ba 0f 36 27 11 04 ad 06 54 20 b7 1e a0 e6 ce be f0 99 69 72 19 35 64 66 31 8d 2c bd 8e 42 0a 9f c6 ca a9 90 2c da bc 85 30 03 d9 32 96 96 f0 be a0 22 0d 24 6c d4 c6 7f 5a 4c 51 24 2d 54 72 08 7c 33 e9 cc 28 c7 66 65 23 69 6b 95 b4 eb be e3 87 e7 63 d7 e4 fb 07 ad 12 92 eb e7 e4 0a 43 b2 a9 df c7 90 bc 26 5b 91 f9 a3 b7 87 9c 94 b9 10 8d 88 c5 58 5c 32 bc 16 ec 0e 57 4f fe a7 93 78 8f e0 c5 39 bb 07 88 60 c1 54 65 eb 87 be 9f 31 97 71 3c fa 8b c8 83 6c 52 96 e0 ac c0 ef cb 69 08 95 5b e0 e0 bb af 27 a4 c2 17 f1 51 9f 84 76 61 d8 24 e2 fe 61 6d 64 35 49 ea 39 c4 21 62 bd cc e2 02 ff 48 6b 38 af 69 c7 b9 92 2d 82 11 8d bd 0b 89 85 2a ea b7 b4 b2 cd 4b eb d1 fa aa f0 e0 4c 09 3c 4d df f6 31 1d 86 30 a8 41 88 57 70 2c 27 51 de cf 8b 4e 3f 02 f2 50 a5 17 e0 67 1b 72 0c 41 31 1f 01 a2 96 3e 3c db 02 b6 9d 94 e6 02 4e f3 f0 19 82 b2 08 23 13 eb 91 cd 51 d3 aa 46 c2 73 98 98 3f ba c3 ee 9a fc fa cd af 72 0a 37 13 8f f9 a0 50 b3 ea fb 3f 2c bc fa 63 55 35 f4 d2 bc b8 71 d2 91 eb e9 ca ca 5c ec 51 66 a8 9e 59 05 22 2f a3 1a db 4f e0 45 62 23 3c 5d 55 fb 30 95 2b 34 a2 cf a7 b4 4b c0 33 c9 34 51 9d d3 b3 2b df c5 ea 2c 2c c7 df 44 1f b6 8d b9 fe f3 5c cd 37 2f b0 6c 9c 4a 08 bd e8 f5 d6 fa 70 e5 69 32 37 5c 5f 0b cb 3f e4 88 02 cc ca b3 78 2f 7d bf 48 b3 21 b0 1f 88 79 9b 5a 8a 71 d8 21 84 29 0f 4a 04 31 2a bd 0d 21 44 ce 74 9d 26 d3 49 1d f8 86 a8 e5 12 77 c5 c0 73 0c 50 83 6a 90 6b a1 ca f8 d0 95 d9 35 86 c7 11 a3 3b 14 c7 cb 86 58 56 0d fb 83 f7 01 02 03 01 00 01
Signature Algorithm	sha256RSA
Fingerprint(SHA1)	a1 58 51 87 15 65 86 ce f9 c4 54 e2 2a b1 5c 58 74 56 07 b4

Table 3 : Certificate Swiss Government Root CA I

Swiss Government Root CA I is the top level CA constituting the basis of trust for enhanced certificates. Its Root CA key and certificate have been generated on 15th February 2011 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 I'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, re-keying and revocation of certificates issuing CA.
- Issue initial and rekeyed certificates for second level issuing CAs as requested.
- Revoke CA certificates where necessary.
- Generate and publish ARLs to always support validation of CA certificates.
- 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 I is operated by SG-PKI staff appointed to the task.

1.3.1.2 Issuing Subordinate Certification Authorities

There are four issuing CAs subordinated to Swiss Government Root CA I. The tasks of these issuing CAs 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, re-key and revocation of end-user certificates.
- Issue initial and rekeyed end-user certificates as requested.
- Revoke end-user certificates on user-request or in case they are misused.
- Generate and publish CRLs to always support validation of end-user certificates.

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

1.3.1.2.1 Swiss Government Enhanced CA 02

Serial Number	54 0c d9 62 7e 1b 22 61 eb 10 30 14 b2 d0 8a 5a
Subject DN	CN = Swiss Government Enhanced CA 02 OU = Certification Authorities OU = Services O = Admin C = CH
Subject Alternative Name	None
Validity Period	From Wednesday, May 28 2015 14:22:21 UTC+1 To Tuesday, May 28 2030 14:22:21 UTC+1
Public Key	30 82 02 0a 02 82 02 01 00 e3 8d 51 8a 3c 23 6b 47 30 fc 07 09 38 1c b8 59 2d 79 fa 53 96 4f b0 ee ef 6f 1f ea 45 01 ad ab b3 b6 92 40 18 65 0c cf 60 fb 02 c9 bc 50 cb 77 08 05 06 d8 7a bf 87 fc fc ab 3c 60 a8 20 84 af 2e 5c 0d 19 14 78 01 ef ff 49 a5 16 af 9f 17 25 44 04 e2 04 0e 75 df e3 fd 32 2c 3d 02 f1 a3 61 c2 67 85 e2 09 01 00 ab c6 1f 3d b3 1b 2f 17 a0 19 4a 8c b0 d3 78 17 c0 0a 23 c2 1c bc a8 df 15 b8 44 86 dc 63 5b e9 21 31 fb 3f 8f 03 85 9e 43 48 3b 0f fd 17 0a 83 5b 43 3a 3e 81 ad f1 b2 78 e6 d5 d5 34 3b 05 e4 4d d4 59 25 a0 65 65 e4 e9 00 0b f4 f4 2b dd 44 6c a2 a9 42 5c 50 93 fd c7 c4 3c 75 33 63 2a 30 19 b9 8b 58 ad c1 45 2e 41 7b cf 21 90 a5 16 53 1c d5 60 6f b3 fe 57 43 89 b8 d4 d6 1e 7a ac c2 46 d7 85 e2 8e 9f 07 cb 59 01 25 97 81 92 c0 81 8c ee 2a 8c 81 e0 ee d9 4c 21 b1 b4 17 e6 24 40 6e 4c 0e ae ef ee 4a 92 c0 4d 98 ac ec f0 d9 58 89 1e da 6d 30 93 33 ef 76 dc 37 5f 20 94 18 33 f1 c8 2d a7 56 dd 1f 53 e2 4b ed 01 7f 8f 93 b3 06 74 b2 ee 8d 7e b9 66 c0 4b c1 fe b9 7e 97 54 69 7a 85 d1 bb b6 e5 07 f4 08 8e 87 a0 36 e4 28 24 ab 6a 74 8c c9 3f 32 0e ec 4e a3 8d 43 4b 75 2a c5 fe 39 c5 7c f0 d6 c9 f1 de 4a e3 42 9e 67 09 d6 96 3a c7 53 d8 88 fb 98 a5 fd d7 28 ac 7d fb 62 66 4a 74 61 36 48 26 fb b8 68 66 5e 82 b0 ad 6d 81 f6 dc e7 43 89 ec ec c4 1e 9b ef 97 ff d8 1a 35 4d ce e4 a9 a6 89 28 7b f9 4c 75 7f 3d fc e3 0a 65 84 69 ee a4 43 66 f4 61 44 58 07 2c 3d 47 45 d0 d0 a2 34 cd e3 f1 bd 94 41 72 a8 8d 3d 9a f6 42 81 cc 5e 43 3e 42 38 f2 4f 92 09 0c 7d 4b b2 2f 5f d6 23 39 41 ec fa aa 18 e5 6f ce be 27 d8 51 19 83 c3 95 59 02 03 01 00 01
Signature Algorithm	sha256RSA
Fingerprint (SHA1)	72 14 77 cf 4c 78 4b a3 44 07 f6 ec 55 bd b0 5a db c3 1b a2

Table 4: Certificate Swiss Government Enhanced CA 02

The CA *Swiss Government Enhanced CA 02* issues certificates for natural persons. The certificates are issued exclusively on hard tokens pre-staged by SGPKI.

1.3.1.2.2 Swiss Government Enhanced CA 03

Serial Number	57a66760af372556fcf3623d35a81d95
Subject DN	CN = Swiss Government Enhanced CA 03 OU = Swiss Government PKI O = Bundesamt fuer Informatik und Telekommunikation (BIT) OI= NTRCH-CHE-221.032.573 C = CH
Subject Alternative Name	None
Validity Period	From Tuesday, 1. December 2020 13:44:18 To Thursday, 15. February 2035 09:59:59
Public Key	30 82 02 0a 02 82 02 01 00 bf 54 fa 31 ee c4 aa 6a 0c af ea 93 98 b6 6a 41 9c bb 7d da 16 48 1b 97 73 3b 6d 93 9b 0b 6b d9 b9 30 74 28 1b e1 8a fb 74 40 f5 2f ea c3 ff 95 77 e1 15 72 6b 11 e4 9a 53 c8 6c 4e d0 ca 7a aa 2f ce 47 f4 c8 7a 25 c3 33 bd fe 41 57 59 0f d4 c7 c3 3b f8 81 56 a0 f4 56 65 9c db 0a 76 87 91 67 25 55 43 8f 0d 05 7f d1 1e ed 37 47 1c e5 2c 81 f8 80 20 2d fe 5a ab 2a c8 d9 cc 6b 7f c9 9f f9 86 7e 97 c6 d4 8b ca 16 a5 38 fe c7 ba 40 95 d4 5f 35 b1 71 bd 84 24 8f e1 de df d5 2a 70 21 c7 d8 c0 23 be f8 0e b3 83 37 fa 8f 36 ad 0d f2 72 67 ed 69 2c b7 be 88 ba 51 0e 7d cd a3 e0 74 6c 10 3f 55 5b b4 84 8a 2d 3b 96 bc 16 ac eb b1 cf a0 60 28 43 c3 ad 0e 90 7c 83 76 78 05 f1 a7 57 6f 51 ee fd 54 b1 c9 a7 dc 8b 00 f8 a1 1d 2b 31 dc ec db b1 ac 79 7a e9 55 21 9f 1c 54 7c b3 f7 f8 6a 96 a4 b3 44 d8 32 f5 ab c4 eb c3 0d c8 6c 26 4b 4f 80 85 0b 77 9a cb 73 1b 75 c1 bd 96 19 20 c0 c1 78 5f fa a1 cd f5 73 cd 93 f2 80 f8 d3 e4 8c 76 f8 59 f4 bf 31 c8 ec d3 0f 13 19 90 81 7b 46 35 fa 50 15 0d d7 9d 33 66 ba b0 da 5f 8a af 4e f0 91 f2 42 0d e8 d1 2c 47 62 7e 88 d3 8a f1 13 f9 ad cd 2b e5 ab 7d 8c d0 65 6b d6 3e f0 91 75 39 bc 46 e1 86 a1 3f 57 fa e5 79 75 da ba ca 16 6e 5b d4 a1 f2 9a 04 34 23 9d cd 36 3f 79 4d 94 cd f7 43 a1 fa cc d3 23 00 94 2a 22 b9 3b 63 1a c9 8c d4 17 bd 7a 40 95 4f d1 31 8a f4 18 7a 88 a1 17 a7 21 59 38 ee 37 b4 1a 0f 84 6a b1 fb b3 53 dc cb 5f 39 83 03 e7 d4 f9 d1 41 15 2d da 19 2a 64 08 83 68 5b ab 87 db 30 b5 56 c2 0d c5 e8 1f ab a3 c9 b2 e9 eb 64 64 d6 3f 36 ad 7a f8 8e ba 0f 73 3e 70 2b 37 ff 1d 9c 51 d5 b5 02 03 01 00 01
Signature Algorithm	sha256RSA
Fingerprint (SHA1)	5743b6b2524a64e9d9300138592f782f1ef94dc9

Table 5: Certificate Swiss Government Enhanced CA 03

All certificates are issued only to natural persons.

Swiss Government Enhanced CA 04

Serial Number	2c2bb3f05ea8adf3549b4e34ea49e993
Subject DN	CN = Swiss Government Enhanced CA 04 OU = Swiss Government PKI O = Bundesamt fuer Informatik und Telekommunikation (BIT) OI = NTRCH-CHE-221.032.573 C = CH
Subject Alternative Name	None
Validity Period	From Tuesday, 1. December 2020 15:40:40 To Thursday, 15. February 2035 09:59:59
Public Key	30 82 02 0a 02 82 02 01 00 d2 3d 25 fe e5 df b3 53 f6 0c 2d 73 13 15 0f c5 21 1d 9c 5c 8d 62 49 bf 61 5d 32 1e 0e 50 ed 26 a7 db fa 1c d4 46 1d 89 2e 01 01 d9 71 cc da af 0b a4 7d 8e 30 24 aa 2e a8 da d6 56 2b 03 cb 1d 26 a6 ff bb 30 fb a3 b7 cb 6b ed d0 6d 42 e9 ba 97 30 5f 19 30 69 2c 32 0a 71 6f 58 37 21 a2 ad 31 0e d3 8d bd aa 87 4b 16 95 47 ad 25 96 57 d4 50 42 3e 20 96 3f 66 70 29 7b 71 af 52 c9 80 e1 73 df c7 69 de 6e 95 dd 5e f7 90 0e 60 71 78 99 55 a6 69 0e f8 18 27 7e d6 03 f5 bf 81 71 e4 7c 2d 80 f1 d2 0b 16 83 36 da 11 af 86 bc e6 73 08 f2 b5 c7 45 dd ab e0 53 be d1 e4 ce 07 71 77 09 0e a9 78 35 fe fc 9c 0f 99 06 dd 7f 6e 08 17 ec fc bf 5b 4b 33 10 54 21 57 99 c5 cc 5d 54 de 84 7a 41 e6 e2 99 31 ec 2e de 59 0c 82 4b 5f d6 aa c6 1d 12 66 cd 2d dd ff 0c ef 11 6e b6 a2 0b cd 29 ba fa 57 c6 42 6f 62 5d 7c 1d 21 17 25 29 8c ef 23 c0 9d 13 94 df e9 83 17 06 b0 b9 fc 51 ac ce 72 d0 46 c0 10 d9 22 72 b0 b8 26 d5 50 5d 47 c0 f6 7b 6c f6 5d e2 28 83 82 44 ca 91 04 c1 23 2d 13 12 15 9d ad f3 03 d8 12 db 22 a9 ae 81 0d 2c 75 61 5a 46 dd 2c 26 a7 4a c7 3e 5e b4 69 ff af 32 15 b9 32 eb 42 e7 0f af e3 3f 8d 46 a3 f8 a7 2f ed 6b 3b 19 62 be e8 6a b6 13 3b 3e 74 84 af 17 62 0c 21 e2 f4 8b f9 cd 41 cf 29 78 14 07 f2 9d 7e 68 81 72 43 e9 fd 48 00 2c 43 8f f7 4f 06 6f 60 e2 3e 5a 87 be 11 0d c8 4e 6c b3 4a a0 d4 08 c8 59 db 28 a7 2e be a4 4a a3 a5 2b dc 95 03 de 6a 11 c0 bc 6b 08 48 ff 05 8d 5d 07 46 d3 6d c4 d0 90 ce 04 ea c6 0c 1b 11 48 d1 13 36 11 f4 b4 db 6c ff fe a1 f9 77 be 3f ba 7b 06 61 a5 ca d2 43 24 91 18 33 73 b7 3c 6f a6 e6 c7 04 61 02 03 01 00 01
Signature Algorithm	sha256RSA
Fingerprint (SHA1)	a6041c821dfa224a99211e6e19aeceda03d3eee6

Table 6: Certificate Swiss Government Enhanced CA 04

The CA *Swiss Government Enhanced CA 04* issues certificates for natural persons of the Swiss Federal Administration only. The certificates are issued exclusively on hard tokens pre-staged by SGPKI.

1.3.1.2.3 Swiss Government Enhanced CA 05

Serial Number	50cabd19df6d4002ad2793b7d8d060c2
Subject DN	CN = Swiss Government Enhanced CA 05 OU = Swiss Government PKI O = Bundesamt fuer Informatik und Telekommunikation (BIT) OI = NTRCH-CHE-221.032.573 C = CH
Subject Alternative Name	None
Validity Period	From Wednesday, 2. Dezember 2020 14:19:17 To Thursday, 15. February 2035 09:59:59
Public Key	30 82 02 0a 02 82 02 01 00 e6 26 cb dc 81 58 c8 d1 46 37 a1 82 67 12 c8 57 31 af b0 72 5b a6 11 7b a8 20 2b 07 69 4c bf 7a f3 ba 17 8c ff b7 04 1a 1b 77 62 22 45 ca 74 48 a1 49 f9 29 83 82 bf db dc 6e 38 98 06 de e3 ee 6f c1 b3 bf 7c 5e 35 0e 33 54 aa 4a c3 bf 47 4d 8d db 6b 1d 82 26 1c 67 8a 4a 70 28 c9 da b4 9d 46 1f c7 16 b9 ea e3 b2 41 de 76 f3 53 ba 31 93 ea f2 29 9a be 69 c2 30 46 12 5d d1 f2 75 7f dc fc db 5e ca a7 cd db ff 5a a6 8c ee d9 9f a0 72 54 71 26 17 fa 47 36 63 0b 73 e0 28 b2 26 2f 72 d0 9a 8a 24 00 6e 40 44 49 2a db 9b 36 d4 64 7f f0 2f f3 12 32 76 d2 5f 40 72 85 29 03 56 ce 65 38 68 54 3f 72 60 34 81 da d8 49 a5 a4 07 de 23 4c 98 b8 8e 3a d5 49 7d 60 e9 70 57 0d 0a ed bd ec 44 62 9f 39 8f ba a9 72 55 3f 7e b5 9e f3 57 ee f5 2e 09 c3 66 04 f0 ac 42 b6 38 af 18 fb 0f fa 29 ee 76 26 e5 ab e6 38 6a 33 8e 12 95 cf 78 34 61 c3 43 4b 75 b3 b9 c3 ee 1e 1f 02 c8 8c 74 d1 09 54 44 f4 77 58 0b 5e bd 6e 2f 1b 86 4b bd 03 be 1b 09 c5 73 66 08 51 71 9d 41 1d 60 b3 47 91 42 7e a6 e8 18 98 5f 46 f1 d1 42 5a db 85 e4 c3 5c 10 67 b4 bb f7 20 51 9c 13 8b 65 c9 ef 0e f8 b6 ef 04 05 86 44 b3 a6 6f 50 33 3c a7 db 21 be e9 af 4e cc 57 d6 ba df fe be e3 77 60 4e 47 86 ab 26 cd ce 84 55 1f 94 ff 97 56 bb 33 a7 60 c7 b9 47 f5 94 be 93 e0 ab a9 d1 32 53 78 79 d3 2c 9d c5 a0 77 14 09 90 eb 54 51 e0 96 6c 1a 7a ab 68 a1 b7 28 09 40 bd 90 1f 6e 42 07 76 0f 8b 03 e1 c7 4c 39 37 ea 56 58 ae 7d 9f 2b b3 82 70 25 9f c5 be e6 3e 34 38 8e db 8f 63 c4 5a e8 a0 0b d4 45 32 31 f7 28 4c b7 4b b6 3e 25 fd 1a 10 00

	88 3c b8 d2 84 f5 71 59 db 2c fc c1 bb 68 f5 02 03 01 00 01
Signature Algorithm	sha256RSA
Fingerprint (SHA1)	795a22b56d016fc238ab4f087f212e28a2d83e34

Table 7: Certificate Swiss Government Enhanced CA 05

The CA *Swiss Government Enhanced CA 04* issues certificates for natural persons of the Swiss Federal Administration only. The certificates are issued exclusively on hard tokens pre-staged by SGPKI.

1.3.2 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 based on a frame contract [12] with the FOITT and a service level agreement (SLA) stipulated with SG-PKI.

1.3.2.1 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 applicant for a personal certificate according to the rules set up in the document 'Rules for Identification of Applicant' [20].
- '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 I CP/CPS
- Inform certificate applicants of their rights and duties as detailed in the 'Terms and Conditions' [18].
- Verify role in Admin-Directory with requests for role certificates.
- Verify and approve certificate requests (RIO process).
- Inform applicants that their certificates have been issued and will be published in the Admin-Directory.
- Verify and carry out re-key requests.
- Approve or carry out unblocking of certificate tokens (by resetting PINs).
- Approve or carry out requests for key recovery (encryption)

1.3.2.2 LRAO contractual requirement

SG-PKI requires LRAOs by contract to:

- Fully comply with this Swiss Government Root CA I 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
- Fully comply with the regulations and procedures as laid down in the Swiss Government PKI Registrierrichtlinien Klasse B [17]

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

1.3.2.3 LRAO Authentication

For the above tasks the LRA Officers must apply for and be granted the appropriate rights by the PKI security officer according to the processes described in [17] 'Administration der SG-PKI LRA-Officer und RIO'.

1.3.2.4 Registration Identification Officer (RIO)

For certificates issued by the Swiss Government Enhanced CA 02 the identification of the applicant can be delegated to a Registration Identification Officer (RIO). The tasks of the RIO are:

- Identify certificate applicants according to the rules set up in the document 'Rules for Identification of Applicant' [20].
- Inform certificate applicants of their rights and duties as detailed in the 'Terms and Conditions' [18].
- Hand out a pre-staged hard token to the applicant.
- Send the signed application together with copies of the identification documents to the LRA Officer.
- Assist the applicant in unsealing his hard token and loading the certificates.

1.3.2.5 PIN Reset Super User

For certificates issued by the Swiss Government Enhanced CA 02 the PIN of the hard token can be reset in case it was forgotten, or the card is blocked after more than 4 unsuccessful attempts to enter the correct PIN. The subscriber must place the request for PIN reset with a PIN Reset Super User. The tasks of the PIN Reset Super User are:

- Identify the subscriber with the help of personal questions/answers stored in the subscriber's data record.
- Initialize a system PIN reset request for the subscriber.
- Authorize the PIN reset request.

The authorization to act as PIN Reset Super User must be explicitly granted by SG-PKI.

1.3.2.6 PIN Reset User

Prerequisite: The user has done a PIN Reset Request using the PIN Reset Request Wizard on his workstation.

The approved PIN-reset request can be carried out on every workstation. Any employee in possession of a valid Class B of the Swiss Government PKI can act as a PIN Reset User. His tasks are:

- Start the PIN Reset Wizard.
- Identify the subscriber face to face.
- Provide the subscriber with a second card reader to set a new PIN on the smartcard.

1.3.2.7 Key Recovery Agent

For certificates issued by the Swiss Government Enhanced CA 02 the encryption keys are archived and can be restored to a hard token of the subscriber. The Key Recovery function can be carried out by either an LRA Officer or a Key Recovery Agent. The tasks of the KRA are:

- Start the Key Recovery Wizard.
- Identify the subscriber.

- Recover the required encryption keys onto the subscriber's hard token.

The authorization to act as a Key Recovery Agent must be explicitly granted by SG-PKI.

1.3.3 Subscribers

Subscribers are natural persons holding enhanced certificates issued by one of the CAs subordinate to Swiss Government Root CA I. 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, for certificate based authentication or for en-/decrypting 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 1.4 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 except for employees of the FOITT Swiss Federal Office of Information Technology, Systems and Telecommunication.

1.3.4 Relying parties

Relying Parties are individuals or organizations that use certificates of this CAs to validate the electronic signatures and verify the identity of Subscribers or to secure communication 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, 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.

1.3.5 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 who chooses the auditors for the certification of CSPs in Switzerland.

1.4 Certificate Usage

1.4.1 Appropriate certificate uses

The usage of keys certified by Swiss Government Root CA I or one of its issuing CAs is restricted to

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

the actions detailed in the following table (Enhanced CA 03/04/05 to come):

Entity	Private key usage	Certificate usage
Swiss Government Root CA I	Sign certificates for subordinated certification authorities (Issuing CAs) Sign ARLs (Authority Revocation List)	Validate end-user certificates chaining back to Swiss Government Root CA I Validate the integrity of ARL and OCSP responses
Swiss Government Enhanced CA 02	Sign enhanced certificates for end-users Sign CRLs (certificate Revocation List)	Validate end-user certificates issued by the CA Validate the integrity of CRL and OCSP responses
Subscriber	Enhanced certificates: sign, authenticate or decrypt documents/data depending on type of certificate	Verify certificate holder's electronic signature and authenticity, enables a remote party and the certificate holder to encrypt holder's data
Relying Party	not applicable	Verify electronic signatures and electronic seals Verify authenticity of certificate holder Verify role of certificate holder Use subscribers' public keys for encrypting documents/data

Table 8 : 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.

1.4.2 Prohibited certificate uses

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

1.5 Policy administration

1.5.1 Organization administering the document

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

1.5.2 Contact person

1.5.2.1 SG-PKI Security & Compliance

The contact person for all security and compliance inquiries is Beat Roth.

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

1.5.3 Person determining CPS suitability for the policy

The 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) [32].

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

KPMG AG
Badenerstrasse 172
8026 Zürich
Switzerland

1.5.4 CPS approval procedures

The PKI Management Board annually reviews this CP/CPS and its related documentation so that it adheres to applicable law,

See also section '9.12 - Amendments'.

1.6 Definitions and acronyms

1.6.1 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]
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
Ausweis F	Document issued by the State Secretariat for Migration SEM to refugees without valid identity documents.	SEM
Authority Certificate	Behördenzertifikat	

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

Term	Definition	Source
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 re-key	Certificate re-keying is a process where a Subscriber automatically obtains a new certificate, if proof of key possession of the current, valid certificate can be provided. The re-keyed certificate contains new validity information, a new key pair but retains the same subject.	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” or “Klasse B” certificate, issued under Swiss Government Root CA I	SG-PKI
Directory Service	CIS, AIS 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
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
Enterprise RA	An employee or agent of an organization unaffiliated with the CA who authorizes issuance of Certificates to that organization	BR
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

Term	Definition	Source
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
Hard-Token	Also hardware token, a user controlled, physical device (e.g. smart card) used to store cryptographic information and possibly also perform cryptographic functions	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 I.	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 Key (such as a Debian weak key, see http://wiki.debian.org/SSLkeys) 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
Klasse B	Certificates of type “Klasse B” issued by SG-PKI are combining the government identity directory (AdminDir) and a qualified identification process in combination with a strong authentication token (smart card)	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	A group of **public-key cryptography standards** devised and published by RSA Security Inc.	RSA
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

Term	Definition	Source
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
Registered Domain Name	A Domain Name that has been registered with a Domain Name Registrar	BR
Register Smartcard Process	A process with which a non-prestaged token for Klasse B certificates is initialized (if not already in this state), furnished with three key pairs and registered in SG-PKI's central token-database.	SG-PKI
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
Reliable Method of Communication	A method of communication, such as a postal/courier delivery address, telephone number, or email address, that was verified using a source other than the Applicant Representative.	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
Soft-token	A data object that is used to store cryptographic information and possibly also perform cryptographic functions.	SG-PKI
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
Swiss authorities	Entirety 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

Term	Definition	Source
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 measured from the date when the Certificate is issued until the Expiry Date.	BR

1.6.2 Acronyms

Term / Acronym	Full text	Explanation
AIS	Auftragsinformationssystem	The 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.
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.
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/ .
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

Term / Acronym	Full text	Explanation
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.
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.
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.
PUK	PIN Unlock Key	Key used to unlock a blocked certificate token.
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	A widely used algorithm today supporting public key cryptography.

Term / Acronym	Full text	Explanation
SG-PKI	Swiss Government PKI	FOITT operational unit responsible for and operating all PKI services provided by the Swiss federal administration.
SHA2	Secure Hash Algorithm	A class of algorithms used widely today for hashing data to be digitally signed.
SLA	Service Level Agreement	Service contract where the PKI services are formally defined.
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

1.6.3 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 I and its Issuing CA publicly available through SG-PKI's web site (www.pki.admin.ch) and/or over a directory service compliant with ITU-T recommendation X.500.

Directory service is available from within the Swiss federal administration's intranet or using LDAP.

2.2 Publication of certification information

SG-PKI publishes information related to certificates issued by Swiss Government Root CA I 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 I and its issuing certification authorities.
  - A schematic overview of the actual CA structure
  - Certificate(s) of the Swiss Government Root CA I
  - Fingerprint of the certificate of the Swiss Government Root CA I
  - Certificate(s) of each Sub CA
  - Fingerprint of the certificate(s) of each Sub CA
  - Terms and conditions "Klasse B" [18]
- Publication on directories within the federal administration:
  - All certificates for encrypted communication issued by the Swiss Government Root CA I and its Issuing CAs.
  - The Swiss Government Root CA I certificate and the Issuing CAs certificates.
  - The authority revocation list (ARL) for the Swiss Government Root CA I.
  - The certificate revocation list (CRL) for the Swiss Government Root CA I and its Issuing CAs.

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 I - CP_CPS: This document. If updates are required, the new version of this document will be published as soon as it has been approved.

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

- Directory services update data on certificates several times per hour and CRLs every hour.
- **Swiss Government Root CA I** updates its **ARL** at least **once a year** and immediately after revoking a Issuing CA's certificate.
- **Swiss Government Enhanced CA 02** updates its **CRL at least every seven days** with a grace period of one day and maximally eight hours after revoking a subscriber certificate.
- **Swiss Government Enhanced 03/04/05:** Not defined yet**.**

2.4 Access controls on repositories

The Directory Service, 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. Writing 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 basis(i.e. 24/7) 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 must 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 approve 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)
- 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 satisfy the requirements specified in technical directive on Directory Service (CIS) by the Federal IT Steering Unit [5] [6].

‘Standard’ subscribers are employees of the federal, cantonal or communal administration. They are identified by their name, first name and a unique alphanumerical code generated by the CIS (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. The two exceptions to this rule are:

- In case it is essential that a certificate holder’s function or other particulars are visible from the certificates they MAY use the option ‘FreeDN’ and compose their distinguished names freely within the limits set by the above directive. They MUST provide proof of all information that will be part of the certificate based on formal documents.
- With role certificates the DN comprises also the certificate holder’s role assigned by his local administration.

Swiss Government Root CA I and its Issuing CAs use a standard form of DN where the fields c, o, ou, cn are populated (for details see section 7.1.4 Name forms).

Persons from outside the public 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.

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

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

- Subscribers with a record in the Directory Service (see 3.2.2 - Authentication of individual identity) have already a common name on which has been added a unique suffix by the Directory Service. 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 the Directory Service from the date/time they are registered in the administrative database.
- Subscribers with a record in the Swiss Government AIS directory (see 3.2.2 - Authentication of individual identity) have their unique email address incorporated in their record.
- 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.

3.1.6 Recognition, authentication, and role of trademarks

Not relevant. SG-PKI 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

In general, there are two ways to prove possession of private key.

3.2.1.1 Key generation as part of the prestaging process

For Klasse B Prestaged, the keys are generated centrally in a secure location supervised by SG-PKI personnel and then injected into new hard tokens. The tokens are secured with an unseal PIN and then distributed to the local registration office. The applicants receive a pre-staged hard token only after having been identified by an LRA Officer . During the unseal process the certificates are written

onto the card. The established processes ensure that no-one except the intended applicants ever gets access to any token and the corresponding unseal information simultaneously. All keys except the encryption keys are deleted from the central database immediately after being copied to the tokens. The encryption keys are escrowed in a special key recovery database.

3.2.2 Authentication of individual identity

Applicants for certificates MUST prove their identity by personally presenting a valid travel document (valid Swiss passport or identity card or foreign travel document recognized for the entry into Switzerland) The LRA MUST carry out the following checks:

- verify the validity of the presented identification document
- verify the contents of the applicants certificate request form
- verify the applicant is registered in a directory under the control of the authorities of the Swiss Government (e.g. AdminDir. AIS or CIS),
- Verify that the applicant's name in the directory is identical to the one in the identity document presented.

As an exception, applicants for certificates CAN prove their identity by personally presenting an 'Identity card for provisionally admitted foreigners type F' (Ausweis für vorläufig aufgenommene Ausländer F, thereafter, referred to as 'Ausweis F'). In this case, the applicant must also present a special application form duly signed by the person responsible for PKI safety within the applicant's administrative unit (for government offices this is the ISBO), stating that that unit is aware of the fact that the applicant cannot be identified without doubts (Additional Application Form for 'Ausweis F' Holders). In addition to the steps specified above the LRA MUST, in this case, also carry out the following additional check:

- verify the contents of the 'Additional Application Form for 'Ausweis F' Holders',
- verify the authority of the undersigned of this form.

3.2.2.1 Enhanced Certificates

For enhanced certificates, the applicant must be identified in person by an LRA-Officer especially trained and qualified for issuing these certificates.

3.2.2.2 Registration Information Officer (RIO) Process

For enhanced certificates, there exists an additional process to identify applicants, the 'Registration Information Officer' (RIO) process.

The 'Registration Information Officer' (RIO) carries out the checks listed under 3.2.2 Authentication of individual identity in the presence of the applicant instead of the LRA-Officer and documents this identification. The RIO hands out a pre-staged sealed smartcard to the applicant and sends the registration data to an LRA for approval. After approval the LRA-Officer initializes the issuing of the certificate and sends an unseal-PIN back to the RIO or the applicant. Once the requested certificate has been issued, the applicant can unseal his smartcard, downloading and transferring the certificates to his personal token.

After first usage (unseal the token) the system sends an e-mail to the address listed in the certificate instructing the certificate subscriber to immediately revoke the certificate if he did not unseal the token himself.

Independently of how keys and certificates are technically handled, the LRAO or RIO MUST:

- verify the contents of the applicants certificate request form,
- verify the contents of the 'Additional Application Form for 'Ausweis F' Holders' in case of an applicant with 'Ausweis F',
- verify the authority of the undersigned of this form.
- verify the applicant is registered in a directory under the control of the authorities of the Swiss Government (e.g. AdminDir, AIS or CIS),
- verify the applicant's name in the directory is identical to the one in the presented identity document.

3.2.3 Non-verified subscriber information

The LRA verifies all data necessary for identifying an applicant and, like described in '3.2.2 - Authentication of individual identity'. It doesn't do any further verification of requests for certificates.

3.2.4 Validation of authority

With certificate requests from subscribers external to the administration, the LRA validates the authority of the applicant by consulting the administrative unit having authorized the external partner originally.

3.2.5 Criteria for interoperation

Not applicable.

3.3 Identification and authentication for re-key requests

Enhanced certificates which are still valid MAY be re-keyed without registration. The subscriber initiates and authenticates a re-key request on-line on the basis of a valid enhanced authentication certificate (see 4.7.3 Processing certificate re-keying requests). The 'old' signature and authentication keys are erased from the token after the successful download of the re-keyed certificates while encryption keys are kept permanently.

For re-keying role certificates the responsible LRA verifies in the Directory Service that the applicants are still assigned the roles.

3.3.1 Identification and authentication for re-key after revocation

For certificate re-key after revocation the identical process is used as for obtaining initial certificates. This applies for all enhanced certificates.

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 card recognized for entry into Switzerland) at a LRA

- Sending the revocation request by registered mail to the local LRA.
- Electronically sign the revocation request with his signing key, provided the revocation is not done because of a suspected or actual key compromise or because of the loss/theft of the certificate token.
- Contacting FOITT's ServiceDesk which will forward the request to an LRA for approval.

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

As an exception, a requestor MAY present his/her 'Ausweis F' for identification.

4 Certificate Life-Cycle Operational Requirements

This paragraph details all requirements for end-user certificates. For Root CA and subordinate 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- enhanced certificates, provided his/her organization has signed the frame contract [12] and the service level agreement with FOITT.

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

- Terms and conditions for Klasse B certificates Swiss Government PKI (Benutzervereinbarung und Nutzungsbedingungen für die Klasse B [18])

Representatives of companies working closely with one of the administrative units MAY request SG-PKI 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
Centralized Key Generation	1. Stage secure tokens (generate key pairs) and deliver to the LRA	SG-PKI

Process	Description	Responsible
	2. Applicant or his agent initiates request.	Applicant / applicant's agent
	3. Applicant and, when issuing role certificates, applicant's role, is / are identified / authenticated by an LRA officer.	LRAO
	4. Personalization of hard-token is done centrally by SG-PKI (technically: a certificate request generated and uploaded to CA, certificate issued by CA, the generated certificate is downloaded and finally written to token).	SG-PKI / CA
	5. Applicant secures token with personal PIN. LRA officer hands applicant the sealed hard-token and the Unseal PIN. This MUST be done personally or based on two independent trusted ways (e.g. line manager and validated post address).	Applicant
	6. LRA officer hand applicant the hard-token	LRAO
RIO Centralized Key Generation	1. Applicant or Administrative unit initiates request on his behalf.	Administrative unit
	2. Applicant and, when issuing role certificates, applicant's role, is / are identified / authenticated by an RIO.	RIO
	3. RIO hands "pre-staged" token to applicant, identifies applicant and sends proof of identification and token serial number to LRA.	RIO
	4. LRAO approves request of applicant identified by RIO	LRAO
	5. LRA officer 'issues certificates on the CA using the serial number of the token and the therefore in the prestaging process registered keypairs.	CA / LRAO
	6. The Unseal-PIN is sent to applicant.	LRAO
	7. Applicant (at a colleagues workstation) uses unseal-PIN to unlock token and download certificates from CA. These are now written on the hard-token.	Applicant
	8. The applicant sets a PIN on the hard-token and adds the revocation-passphrase into the system.	Applicant

Table 9 : 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 or by RIOs. Independent of the enrollment process (see 4.1.2 Enrollment process and responsibilities) the LRAO or RIO identifies the applicants as follows:

- Applicants present themselves in person to the LRAO or RIO.
- Applicants' identities are verified based on a valid travel document (valid Swiss passport or identity card or foreign travel document recognized for entry into Switzerland)
- Applicants' identities CAN, as an exception, be verified based on a valid 'Ausweis F' and a duly signed 'Additional Application Form for 'Ausweis F' Holders'.
- LRAO or RIO scans the identity documents presented to be stored as evidence by the CAs concerned.

4.2.2 Approval or rejection of certificate applications

LRAOs accept certificate applications provided the following requirements are met:

- The applicant is registered in a directory under the control of the authorities of the Swiss Government (e.g. AdminDir, AIS or CIS) 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).
- The entry in a directory under the control of the authorities of the Swiss Government (e.g. AdminDir, AIS or CIS) confirms that the applicant has truly been assigned the role identified in the application for a role certificate.

Applications that don't meet all 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 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 and within a maximum of three days after registration by an RIO.

4.3 Certificate issuance

4.3.1 CA actions during certificate issuance

The CAs subordinated to Swiss Government Root CA I 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 4.1.2 Enrollment process and responsibilities), the CA either downloads the certificate directly to the LRA having approved the request (to be transferred to the hard-token) or holds it pending for download until the subscriber actively retrieves it from a 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 I send an e-mail notification to 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 hard-tokens or with the successful download of certificates by the applicants.

4.4.2 Publication of the certificate by the CA

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

Certificates with other purposes than encryption (i.e. certificates for signing or authentication) MAY be published in the same way.

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 I. 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 1.4 Certificate Usage.

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 hard tokens, i.e. keep PIN 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. not 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, considering 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 I.

4.7 Certificate re-key

Certificate re-keying is a process where a Subscriber automatically obtains a new certificate, if proof of key possession of the current, valid authentication certificate can be provided. The re-keyed certificate contains new validity information, a new key pair but retains the same subject.

4.7.1 Circumstance for certificate re-key

Certificates issued by the CAs subordinated to Swiss Government Root CA I SHOULD be re-keyed (i.e. new certificates are issued based on new key pairs) in case they are about to expire.

4.7.2 Who MAY request certification of a new public key

The applicants entitled to request certificate re-key are identical to the ones entitled to request initial certificates as per section 4.1.1 Who can submit a certificate application.

4.7.3 Processing certificate re-keying requests

Enhanced certificates MUST still be valid to be re-keyed without registration.

The re-keying request is based on unused key pairs that have been generated during the initial token staging procedure. Since card staging generates only three different sets of key pairs, the certificates on pre-staged tokens can only be re-keyed twice without a new registration.

4.7.4 Notification of new certificate issuance to subscriber

After a certificate is re-keyed, the CA sends the respective subscriber an e-mail notification, using the e-mail address indicated in the certificate.

4.7.5 Conduct constituting acceptance of a re-keyed certificate

The conduct constituting acceptance is the same as with the issuance of initial certificates (see section 4.4.1 Conduct constituting certificate acceptance).

4.7.6 Publication of the re-keyed certificate by the CA

Re-keyed certificates are published in the same way as certificates that are issued initially (see 4.4.2 Publication of the certificate by the CA).

With the publication of a re-keyed certificate the responsible CA removes a subscriber’s earlier certificate issued for the same purpose from the Directory Service.

4.7.7 Notification of certificate issuance by the CA to other entities

No stipulation

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 I 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 hard-token has been lost or stolen.
- A hard-token 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 mis-leading;
- 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 I or SG-PKI 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
- A subscriber has been unassigned the role certified by a role 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;

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 employs the subscriber.
- The administrative unit having vouched for 'external' subscribers.
- The SG-PKI Security Officer.
- The SG-PKI Management Board.
- The local administration having unassigned a subscriber's role.
- The Security Officer of the subscriber's Department (ISBD) or Office (ISBO).

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

4.9.3 Procedure for revocation request

The procedure for revoking certificates issued by CAs subordinated to Swiss Government Root CA I 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 the 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 this 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 I revoke certificates without delay as soon as they receive approved requests from a LRA. With every revocation the responsible CA updates its CRL and uploads it to the Directory Service for publication.

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 based on a SG-PKI certificate.

4.9.7 CRL issuance frequency

4.9.7.1 CRL issuance frequency for the Status of Subscriber Certificates

If no certificates are revoked, the CRL is updated and published every day.

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

4.9.8 Maximum latency for CRLs

CRLs updated by the issuing CAs are sent to and published in the Directory Service and on the web site (see 2.1 - Repositories) with a maximum latency of twenty-four hours.

4.9.9 On-line revocation/status checking availability

The SG-PKI provides OCSP services compliant with RFC 6960.

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

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 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 I 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 not be listed in the CRL even if they were revoked for some reason. The CRLs are published both in Directory Service (CIS) and 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.

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 legal compliance reasons, 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

There is no escrow for signature and authentication keys of enhanced certificates by SG-PKI. Encryption keys are handled differently – as the original private keys are required for decrypting documents/data until all data protected is no longer used, escrow is applied to all keys used for en- and decryption.

4.12.1 Key escrow and recovery policy and practices

A key archive server runs in the background as part of the registration application operated by SG-PKI. In the course of the personalization of tokens for enhanced certificates (see 4.1.2 - Enrollment process and responsibilities) it stores the applicants' encryption key pairs in a secure backup database.

A subscriber can have his previous encryption keys recovered from this database onto his valid hard-token via a secure procedure. The request MUST be carried out by a Key Recovery Agent.

4.12.2 Key recovery Foreign keys for trusted third parties

In exceptional cases, it may be necessary to make a person's encryption key(s) available to another user on a separate smartcard. Reasons for this may include:

- The employee is no longer working for the organization.
- The employee is absent for a prolonged period due to illness.
- The employee has died.
- There is a court order against the employee.

Since the restored encryption keys can now be used to read all encrypted data that was encrypted with one of these belonging to the certificate holder, each of these cases must be assessed separately. For this purpose, a detailed request must be submitted to the SG-PKI security officers. The further procedure will then be determined on a case-by-case basis, always in consultation with the FOITT Legal Service.

4.12.3 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 [14].

Only people 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 people 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 are 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

. 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 PKI systems operation can be upheld in case of an emergency.

SG-PKI uses an off-site 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 Management Board.
- **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 BIT Manager they are responsible for the TSP Products. 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 I 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 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 “Class B”, issued under the Swiss Government Root CA I as specified in 1.6.1 - 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 to 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, to the following documents in particular:

- Certificate Policy and Certification Practice Statement of the Swiss Government Root CA I (this document).
- SG-PKI security policy [14].
- SG-PKI manual on operation and organization [15].
- 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' [15].

5.4.3 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 I.

5.4.4 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 Operation Backend are authorized to access server and log files.

5.4.5 Audit log backup procedures

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

5.4.6 Audit collection system

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

5.4.7 Notification to event-causing subject

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

5.4.8 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 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. These are in particular:

- 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 I.

5.5.3 Protection of archive

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

All access to archives must be formally authorized by the PKI Management Board.

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 based on the central date/time reference provided by FOITT.

5.5.6 Archive collection system

All data to be archived is integrity protected by digital signatures 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 I and its Issuing CAs are always backed up off-site in at least two security modules. 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.

5.7.3 Entity private key compromise procedures

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

- 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 I) 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 I 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

An emergency facility is available, capable of running SG-PKI's Swiss Government Root CA I and its Issuing CAs 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 I.

All valid certificates, including Swiss Government Root CA I and Issuing CA certificates, will be revoked and a final CRL and ARL published on FOITTs website for a minimum of eleven years. The Swiss Government Root CA I 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 an 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 the members of PKI Management Board, a PKI Security Officer, a PKI Operation Backend Staff member, a Qualified Auditor and a Notary to witness the Root CA Key Pair Generation Ceremony. The Swiss Government Root CA I Key Pair Generation Ceremony is documented and logged.
- Root CA Key pairs are generated in HSMs conformant to FIPS 140-2 Level 3 or CEN EN 419 221-5 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 3 or CEN EN 419 221-5 within the secured facilities of SG-PKI (5.1.1 - Site location and construction).
- The keys are generated centrally in the SG-PKI backend systems within the secured facilities of SG-PKI and then injected into a new token conformant to FIPS 140-2 Level 2. The token is secured with a random initial PIN and a PUK and distributed to the local registration office.

6.1.2 Private key delivery to subscriber

- Private keys to be certified are delivered to subscribers in one of the following ways:
  - Generated and certified centrally and handed over to applicant either at an LRA after successful registration or by means of two independent trusted ways (see 4.1.2 - Enrollment process and responsibilities).
  - Generated centrally and handed over to applicant during the registration process by a RIO.

6.1.3 Public key delivery to certificate issuer

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

6.1.4 CA public key delivery to relying parties

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

SG-PKI publishes the certificates of Swiss Government Root CA I 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 I certificate's fingerprint for verification.

6.1.5 Key sizes

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

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

6.1.6 Public key parameters generation and quality checking

All CA keys are generated by HSMs conformant to FIPS 140-2 level 3 or CEN EN 419 221-5 or by a special procedure designed, approved and supervised for this purpose by the cryptology section of the Swiss federal administration

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

The key usage flags are populated automatically in all Swiss Government Root CA I, 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 I keys are not used to sign certificates except in the following states:

- Self-signed certificates to represent the Swiss Government Root CA I itself
- Certificates for Infrastructure purposes.
- Child issuing CAs.

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 hard-tokens) conformant to FIPS 140-2 Level 3 or ETSI EN EN 419211-5 (see also 6.1 Key pair generation).

Subscribers for enhanced certificates MAY use tokens conformant to FIPS 140-2 Level 2.

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. These are in particular the generation, backup and recovery, activation and deactivation of the keys and the exchange of HSMs.

6.2.3 Private key escrow

Subscribers' en-/decryption key pairs are escrowed by a key archive server run within the secured facilities of SG-PKI which encrypts the key pairs for storage. The server is operated in a secure location and accessible to specifically authorized SG-PKI staff only.

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.

Subscribers' keys will not be backed up in any way, except for clause 6.2.3.

6.2.5 Private key archival

There are no private keys archived, except for clause 6.2.3 and with the exception that, for operational

purposes, private keys are stored in an encrypted representation.

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.

The keys intended for enhanced certificates are either

- generated and written un-encrypted to hard-tokens centrally in a secure location,
- Private keys that are used for encryption and need to be recovered, which are transferred encrypted with a transport key that has been generated by the token.

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', except for keys generated by the special procedure mentioned in clause 6.1.1

Subscribers' keys are stored un-encrypted in a secure container in the hard-tokens.

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 besides the PKI Security Officer.

Subscribers activate their hard-tokens and private keys by entering the token PIN.

6.2.9 Method of deactivating private key

Root CA and Issuing CA's private keys are deactivated with the closure of the certification application by the security officer. The deactivation process requires two SG-PKI staff members authorized for the task beside the PKI Security Officer.

Subscribers' private keys are deactivated when the certificate tokens are powered off, i.e. either with the removal of the tokens or the closing down of the subscribers' workstation.

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.

Subscribers' private keys are destroyed by destroying the respective certificate tokens.

6.2.11 Cryptographic module rating

For ratings see section 6.2.1.

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 I.
- 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.

Hard-tokens:

The PUK is generated, stored and applied to the token during the staging process. The same process sets a random PIN for the card. The individual PIN is entered by the subscriber when the card is activated.

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 always locked, unless there is a HSM to be activated or deactivated.

Subscribers Keys:

Subscribers are obliged to always keep the activation data (PIN or passphrase) secret.

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]).

During registration the LRA officers instruct subscribers on how to adequately protect access to their certificate tokens 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

PKI Engineers 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 are 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 necessary for SG-PKI's operations. All private network communications are protected through integrity checks and encryption mechanisms.

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

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 and utilize the ITU-T X.509 version 3 Digital Certificate standard.

Certificates and CRLs issued by enhanced Issuing CAs conform to same requirements although these CAs are not covered by ZertES.

7.1 Certificate profile

Unless it is explicitly indicated, certificates issued for Swiss Government Root CA I, its subordinate CAs and end-users adhere to the identical profile. A detailed description for all certificate types are documented in 0040-RV-CA Layout and Policies [34].

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 I's and subordinate 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	EnhancedCA02/03/04/05: Policy OID as stated in [33]	not critical
Basic Constraints	1. Indicates type of certificate subject: CA or end-user (here: CA). 2. Indicates how many CA levels MAY be subordinated to CA (with Swiss Government Root CA I: no limit given, with Issuing CAs: limit is 0).	critical
CRL Distribution Points	Lists address(es) where status information on certificate may be found.	not critical

Table 10 : Swiss Government Root CA I 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

Table 11 : End-user certificate extensions

7.1.3 Algorithm object identifiers

There are two algorithms used in conjunction with SG-PKI 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 I 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
Country (c)	CH
Organization (o)	Admin
Organizational Unit (ou)	Services
Organizational Unit (ou)	Certification Authorities
Common Name (cn)	Swiss Government <Name of individual CA>

Table 12 : CA name forms

Subscribers are identified as certificate subjects in the following way:

DN Field	Value
Country (c)	CH
Organization (o)	Admin
Organizational Unit (ou)	Weisse Seiten
Common Name (cn)	<Lastname> <Firstname> <Suffix>

Table 13 : Subscriber name forms

7.1.5 Name constraints

Name constraints are not used by SG-PKI with the issuance of enhanced 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 I are listed in ‘1.1.2 - Subscriber Certificates issued under this CP/CPS’. Usage of policy constraints extension

Policy constraints are not used by SG-PKI with the issuance of enhanced certificates.

7.1.7 Policy qualifiers syntax and semantics

Policy qualifiers are not used by SG-PKI with the issuance of enhanced certificates.

7.1.8 Processing semantics for the critical certificate policies extension

With the issuance of enhanced certificates, the certificate policies extension is set to ‘not critical’, SG-

PKI doesn't expect relying parties to process policy information electronically.

7.2 CRL profile

7.2.1 Version number(s)

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

7.2.2 CRL and CRL entry extensions

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

CRL Extension	Objective	Criticality
CRL number	Number of CRL (CRLs are sequentially numbered).	not critical
CRL Entry Extension		
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

Table 14 : CRL and CRL entry extensions

Expired certificates are not included in the CRL, due to size limitations of the CRL. If you have any questions about an expired certificate, please contact us by e-mail at servicedesk@bit.admin.ch, quoting the certificate serial number and the reason of your request. Revocation status information of expired certificates can be retrieved using OCSP.

7.3 OCSP profile

The SG-PKI OCSP responders implement the RFC 6960 profile.

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, NonRepudiation, CRLSign	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

OCSP Signer Extension	Objective	Criticality
Status	good or revoked or unknown	
This update	Time OCSP response starts to be valid	
Next update	Time OCSP response ends to be valid	

Table 15 : OCSP Signer and OCSP Response extensions

8 Compliance Audit and other Assessments

8.1 Frequency or circumstances of compliance audit and other assessments

Swiss Government Root CA I 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 certification body (see (see 1.3.5. - Other participants).

8.1.1 Self-Audits:

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 Management Board 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 for tracking the necessary actions and reporting to the PKI Management Board the actual status of completion.

8.6 Communication of results

Audit results are only communicated to PKI Director, PKI Management Board 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 based on Swiss Government Root CA I 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.

Since 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 SG-PKI's certification services as liable, and has thereby eliminated 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 internal 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 internal information

All SG-PKI staff and Registration Agents are responsible for protecting confidential information. PKI Security Officers specify the respective requirements and measure and enforce 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 must only collect 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 the owner of the intellectual property rights of the following documents:

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

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 enhanced certificates in compliance to the current CP/CPS.

9.6.2 RA representations and warranties

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

9.6.3 Subscriber representations and warranties

Subscribers commit to acquire, use and maintain their private keys, certificates and tokens in compliance to 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 18 (see [2]). As far as possible the liability of the SG-PKI is limited to the extent permitted by applicable law. SG-PKI is not liable in particular 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 client 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. The Registration Agent is liable in particular 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]., The Subscriber is liable in particular 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 the SG-PKIs 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 Management Board 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 1.3.5 - 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 of the relevant ETSI Standards, SG-PKI will react to a notification of a failure or mis-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 the 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.