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

Swiss Government PKI

Certification Practice Statement / Certificate Policy

for the issuance of

Publicly-Trusted Certificates

Version 1.0

Document OID: 2.16.756.1.17.3.61.0

Involved Persons	
Authors:	Michael von Niederhäusern Felix Brönnimann Robert Dietschi
Approval:	Swiss Government PKI Management Board
User:	Subscribers, Swiss Government PKI, Assessors, Third Parties
For information / knowledge:	-

Document History

Changes			
Date	**Version**	**Who**	**Description**
2015-03-31	X0.1		Initial Version
2015-05-17	X0.2	MvN	Modifications
2015-08-18	X0.3	MvN	Restructuring
2016-02-29	X0.4	MvN	Adaptations for Root III
2016-04-12	X0.5	MvN	Restructuring for finalization
2016-05-04	X0.6	MvN/BFe	Review Chapters 1-4
2016-05-10	X0.7	MvN/BFe/DR	Review Chapters 4-6
2016-05-12	X0.8	MvN/BFe/DR	Review Chapters 6-8
2016-05-13	X0.9	MvN/BFe	Full Review
2016-05-13	1.0	SG PKI Management Board	Approved version

Table of Contents

1 Introduction 10
1.1 Overview 10
1.2 Document name and identification 11
1.3 PKI participants 12
1.3.1 Certification authorities 12
1.3.1.1 Root Authorities 12
1.3.1.1.1 Swiss Government Root CA III 12
1.3.1.2 Issuing Subordinate Certification Authorities 13
1.3.1.2.1 Swiss Government Public Trust Server CA01 13
1.3.1.2.2 Swiss Government Public Trust EV Server CA01 14
1.3.1.2.3 Swiss Government Public Trust Codesign CA01 15
1.3.1.2.4 Swiss Government Public Trust EV Codesign CA01 15
1.3.2 Registration authorities 16
1.3.2.1 Registration Agent 16
1.3.2.1.1 Registration Agent tasks 16
1.3.2.1.2 Registration Agent contractual requirement 16
1.3.2.1.3 Registration Agent - Identification 16
1.3.3 Subscribers 16
1.3.4 Relying parties 17
1.3.5 Other participants 17
1.4 Certificate Usage 17
1.4.1 Appropriate certificate uses 17
1.4.2 Prohibited certificate uses 18
1.5 Policy administration 18
1.5.1 Organization administering the document 18
1.5.2 Contact persons 18
1.5.2.1 PKI Operations 18
1.5.2.2 PKI Service & Design 19
1.5.3 Person determining CP/CPS suitability for the policy 19
1.5.4 CP/CPS approval procedures 19
1.6 Definitions and acronyms 19
1.6.1 Definitions 19
1.6.2 Acronyms 23

2 Publication and Repository Responsibilities 26
2.1 Repositories 27
2.2 Publication of certification information 27
2.3 Time or frequency of publication 28
2.4 Access controls on repositories 28

3 Identification and Authentication 29
3.1 Naming 29
3.1.1 Types of names 29
3.1.2 Need for names to be meaningful 29
3.1.3 Anonymity or pseudonymity of subscribers 29
3.1.4 Rules for interpreting various name forms 29
3.1.5 Uniqueness of names 29
3.1.6 Recognition, authentication, and role of trademarks 29
3.2 Initial identity validation 30
3.2.1 Method to prove possession of private key 30
3.2.2 Authentication of organization and Domain Identity 30
3.2.2.1 Identity 30
3.2.2.2 DBA/Tradename 30
3.2.2.3 Verification of Country 31
3.2.2.4 Authorization by Domain Name Registrant 31

3.2.2.5 Authentication for an IP Address 31
3.2.2.6 Wildcard Domain Validation 31
3.2.2.7 Data Source Accuracy 31
3.2.3 Authentication of individual identity 31
3.2.4 Non-verified subscriber information 31
3.2.5 Validation of authority 31
3.2.6 Criteria for interoperation 32
3.3 Identification and authentication for re-key requests 32
3.3.1 Identification and authentication for routine re-key 32
3.3.2 Identification and authentication for re-key after revocation 32
3.4 Identification and authentication for revocation request 32
4 Certificate Life-Cycle Operational Requirements 33
4.1 Certificate application 33
4.1.1 Who can submit a certificate application 33
4.1.1.1 Server Certificates 33
4.1.1.2 Codesigning Certificates 33
4.1.2 Enrollment process and responsibilities 33
4.1.2.1 DV Server Certificates 33
4.1.2.2 OV Server Certificates 33
4.1.2.3 EV Server Certificates 33
4.1.2.4 Codesigning Certifiates 34
4.2 Certificate application processing 34
4.2.1 Performing identification and authentication functions 34
4.2.2 Approval or rejection of certificate applications 35
4.2.3 Time to process certificate applications 35
4.3 Certificate issuance 35
4.3.1 CA actions during certificate issuance 35
4.3.2 Notification to subscriber by the CA of issuance of certificate 36
4.4 Certificate acceptance 36
4.4.1 Conduct constituting certificate acceptance 36
4.4.2 Publication of the certificate by the CA 36
4.4.3 Notification of certificate issuance by the CA to other entities 36
4.5 Key pair and certificate usage 36
4.5.1 Subscriber private key and certificate usage 36
4.5.2 Relying party public key and certificate usage 36
4.6 Certificate renewal 37
4.7 Certificate re-key 37
4.7.1 Circumstance for certificate re-key 37
4.7.2 Who may request certification of a new public key 37
4.7.3 Processing certificate re-keying requests 37
4.7.4 Notification of new certificate issuance to subscriber 37
4.7.5 Conduct constituting acceptance of a re-keyed certificate 37
4.7.6 Publication of the re-keyed certificate by the CA 37
4.7.7 Notification of certificate issuance by the CA to other entities 38
4.8 Certificate modification 38
4.9 Certificate revocation and suspension 38
4.9.1 Circumstances for revocation 38
4.9.1.1 Reasons for Revoking a Subscriber Certificate 38
4.9.1.2 Reasons for Revoking a Subordinate CA Certificate 39
4.9.2 Who can request revocation 39
4.9.3 Procedure for revocation request 39
4.9.4 Revocation request grace period 40
4.9.5 Time within which CA must process the revocation request 40
4.9.6 Revocation checking requirement for relying parties 40
4.9.7 CRL issuance frequency 40
4.9.7.1 CRL issuance frequency for the Status of Subscriber Certificates 40
4.9.7.2 CRL issuance frequency for the Status of Subordinate CA Certificates 40

4.9.8 Maximum latency for CRLs 40
4.9.9 On-line revocation/status checking availability 41
4.9.10 On-line revocation checking requirements 41
4.9.11 Other forms of revocation advertisements available 41
4.9.12 Special requirements re key compromise 41
4.9.13 Circumstances for suspension 41
4.9.14 Who can request suspension 41
4.9.15 Procedure for suspension request 41
4.9.16 Limits on suspension period 41
4.10 Certificate status services 42
4.10.1 Operational characteristics 42
4.10.2 Service availability 42
4.10.3 Optional features 42
4.11 End of subscription 42
4.12 Key escrow and recovery 42
4.12.1 Key escrow and recovery policy and practices 42
4.12.2 Session key encapsulation and recovery policy and practices 42

5 Management, Operational, and Physical Controls 43
5.1 Physical Security Controls 43
5.1.1 Site location and construction 43
5.1.2 Physical access 43
5.1.3 Power and air conditioning 43
5.1.4 Water exposures 43
5.1.5 Fire prevention and protection 43
5.1.6 Media storage 43
5.1.7 Waste disposal 44
5.1.8 Off-site backup 44
5.2 Procedural Controls 44
5.2.1 Trusted roles 44
5.2.2 Number of persons required per task 45
5.2.3 Identification and authentication for each role 45
5.2.4 Roles requiring separation of duties 46
5.3 Personnel Controls 46
5.3.1 Qualifications, experience and clearance requirements 46
5.3.2 Background check procedures 46
5.3.3 Training requirements 46
5.3.4 Retraining frequency and requirements 46
5.3.5 Job rotation frequency and sequence 46
5.3.6 Sanctions for unauthorized actions 47
5.3.7 Independent contractor requirements 47
5.3.8 Documentation supplied to personnel 47
5.4 Audit Logging Procedures 47
5.4.1 Types of events recorded 47
5.4.2 Frequency of processing log 47
5.4.3 Retention period for audit log 47
5.4.4 Protection of audit log 47
5.4.5 Audit log backup procedures 48
5.4.6 Audit collection system 48
5.4.7 Notification to event-causing subject 48
5.4.8 Vulnerability assessments 48
5.5 Records Archival 48
5.5.1 Types of records archived 48
5.5.2 Retention period for archive 49
5.5.3 Protection of archive 49
5.5.4 Archive backup procedures 49
5.5.5 Requirements for time-stamping of records 49
5.5.6 Procedures to obtain and verify archive information 49

5.5.7 Archive collection system ..... **Fehler! Textmarke nicht definiert.**
5.6 Key Changeover 49
5.7 Compromise and Disaster Recovery 49
5.7.1 Incident and compromise handling procedures 49
5.7.2 Computer resources, software and/or data are corrupted 50
5.7.3 Entity private key compromise procedures 50
5.7.4 Business continuity capabilities after a disaster 50
5.8 CA or RA termination 50

6 Technical Security Controls 52
6.1 Key pair generation and installation 52
6.1.1 Key pair generation 52
6.1.1.1 Root Key par generation 52
6.1.1.2 Subordinate Key pair generation 52
6.1.1.3 Key Pair Generation location 52
6.1.2 Private Key delivery to subscriber 52
6.1.3 Public key delivery to certificate issuer 52
6.1.4 CA public key delivery to relying parties 53
6.1.5 Key sizes 53
6.1.6 Public key parameters generation and quality checking 53
6.1.7 Key usage purposes 53
6.2 Private key protection and cryptographic module engineering controls 53
6.2.1 Cryptographic module standards and controls 53
6.2.2 Private key (n out of m) multi-person control 53
6.2.3 Private key escrow 54
6.2.4 Private key backup 54
6.2.5 Private key archival 54
6.2.6 Private key transfer into or from a cryptographic module 54
6.2.7 Private key storage on cryptographic module 54
6.2.8 Method of activating private key 54
6.2.9 Method of deactivating private key 54
6.2.10 Method of destroying private key 55
6.2.11 Cryptographic module rating 55
6.3 Other aspects of key pair management 55
6.3.1 Public key archival 55
6.3.2 Certificate operational periods and key pair usage period 55
6.4 Activation data 55
6.4.1 Activation data generation and installation 55
6.4.2 Activation data protection 56
6.4.3 Other aspects of activation data 56
6.5 Computer security controls 56
6.5.1 Specific computer security technical requirements 56
6.5.2 Computer security rating 56
6.6 Life cycle technical controls 56
6.6.1 System development control 56
6.6.2 Security management controls 56
6.6.3 Life cycle security controls 56
6.7 Network security controls 57
6.8 Time-stamping 57

7 Certificate, CRL and OCSP Profiles 58
7.1 Certificate profile 58
7.1.1 Version number(s) 58
7.1.2 Certificate extensions 58
7.1.2.1 Root CA Certificate 58
7.1.2.2 Subordinate CA Certificates 59
7.1.2.2.1 Swiss Government Public Trust Standard CA 02 Extension 59
7.1.2.2.2 Swiss Government Public Trust EV CA 02 Extensions 61

7.1.2.2.3 Swiss Government Public Trust Code Signing Standard CA 02 Extensions .. 62
7.1.2.2.4 Swiss Government Public Trust Code Signing EV CA 02 Extensions 64
7.1.2.3 Subscriber Certificates 66
7.1.2.4 All Certificates 66
7.1.3 Algorithm object identifiers 66
7.1.4 Name forms 66
7.1.5 Name constraints 67
7.1.6 Certificate policy object identifier 67
7.1.7 Usage of policy constraints extension 67
7.1.8 Policy qualifiers syntax and semantics 67
7.1.9 Processing semantics for the critical certificate policies extension 67
7.2 CRL profile 67
7.2.1 Version number(s) 67
7.2.2 CRL and CRL entry extensions 67
7.3 OCSP profile 68
7.3.1 Version Number(s) 68
7.3.2 OCSP Extensions 68

8 Compliance Audit and other Assessments 69
8.1 Frequency or circumstances of assessment 69
8.2 Identity/qualifications of assessor 69
8.3 Assessor's relationship to assessed entity 69
8.4 Topics covered by assessment 69
8.5 Actions taken as a result of deficiency 69
8.6 Communication of results 70

9 Other Business and Legal Matters 70
9.1 Fees 71
9.2 Financial responsibility 71
9.2.1 Insurance coverage 71
9.2.2 Other assets 71
9.2.3 Insurance or warranty coverage for end-entities 71
9.3 Confidentiality of business information 71
9.3.1 Scope of confidential information 71
9.3.2 Information not within the scope of confidential information 72
9.3.3 Responsibility to protect confidential information 72
9.4 Privacy of personal information 72
9.5 Intellectual property rights 72
9.6 Representations and warranties 72
9.6.1 CA representations and warranties 72
9.6.2 RA representations and warranties 73
9.6.3 Subscriber representations and warranties 73
9.6.4 Relying party representations and warranties 73
9.6.5 Representations and warranties of other participants 73
9.7 Disclaimers of warranties 73
9.8 Limitations of liability 73
9.8.1 Swiss Government PKI limitation of liability 73
9.8.2 Registration Agent's limitation of liability 73
9.8.3 Subscriber limitation of liability 74
9.9 Indemnities 74
9.10 Term and termination 74
9.10.1 Term 74
9.10.2 Termination 74
9.10.3 Effect of termination and survival 74
9.11 Individual notices and communications with participants 74
9.12 Amendments 74
9.13 Dispute resolution procedures 75
9.14 Governing law 75

9.15 Compliance with applicable law 75
9.16 Miscellaneous provisions 75
9.17 Other provisions 75
9.17.1 Legally binding version of CP/CPS 75
Annexes 76
9.18 Annex A – References 76
9.19 Annex B – Glossary ..... **Fehler! Textmarke nicht definiert.**

1 Introduction

1.1 Overview

1.1.1 Swiss Government PKI

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 Swiss authorities 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 users having a need for securing the document exchange with those administrations.

SG PKI's Certification Authorities (CAs) offer distinct classes of subscriber certificates. The distinction between these classes of Certificates is the level of Subscriber identification and authentication performed (See section 3.2.2). In addition, specific types of certificates within these classes have specific intended uses (See section 1.4) and certificate profiles (See section 7.1).

The SG PKI operates different CA hierarchies for different purposes:

1. Swiss Government Root CA I hierarchy (SG Root CA I) responsible for high assurance qualified and enhanced certificates, i.e. issuing qualified and enhanced certificates according to the Swiss federal administrations' terminology (see: www.pki.admin.ch).

   Qualified and enhanced certificates are issued on hard-tokens exclusively.

2. Swiss Government Root CA II hierarchy (SG Root CA II) issuing certificates at a lower security level for persons, organizations/organizational units, Shared Mailbox and Sytems.

3. Swiss Government Root CA III hierarchy (SG Root CA III) supporting certificates of a high, medium and low assurance level for Publicly-Trusted Authentication and Code Signing Certificates

1.1.2 Subscriber Certificates issued under this CP/CPS

The following subscriber certificates are issued under this CP/CPS:

Certificate Policy (CP)	OID
Public Trust Standard Server Authentication	2.16.756.1.17.3.62.1
Public Trust Standard Client Authentication	2.16.756.1.17.3.62.2
Public Trust EV Server Authentication	2.16.756.1.17.3.62.3
Public Trust EV Client Authentication	2.16.756.1.17.3.62.4
Public Trust EV Server/Client Authentication	2.16.756.1.17.3.62.5
Public Trust Standard OCSP Responder Signing	2.16.756.1.17.3.62.6
Public Trust EV OCSP Responder Signing	2.16.756.1.17.3.62.7
Public Trust Code Signing	2.16.756.1.17.3.62.8
Public Trust EV Code Signing	2.16.756.1.17.3.62.9
Public Trust Standard CS OCSP Responder Signing	2.16.756.1.17.3.62.10
Public Trust EV CS OCSP Responder Signing	2.16.756.1.17.3.62.11
	2.16.756.1.17.3.62.12

1.2 Document name and identification

This document is the SG Root CA III Certificate Policy and Certification Practice Statement.

The object identifier (OID) exclusively used for this document is: OID 2.16.756.1.17.3.61.0

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

The OID components have the meaning given in Table 1.

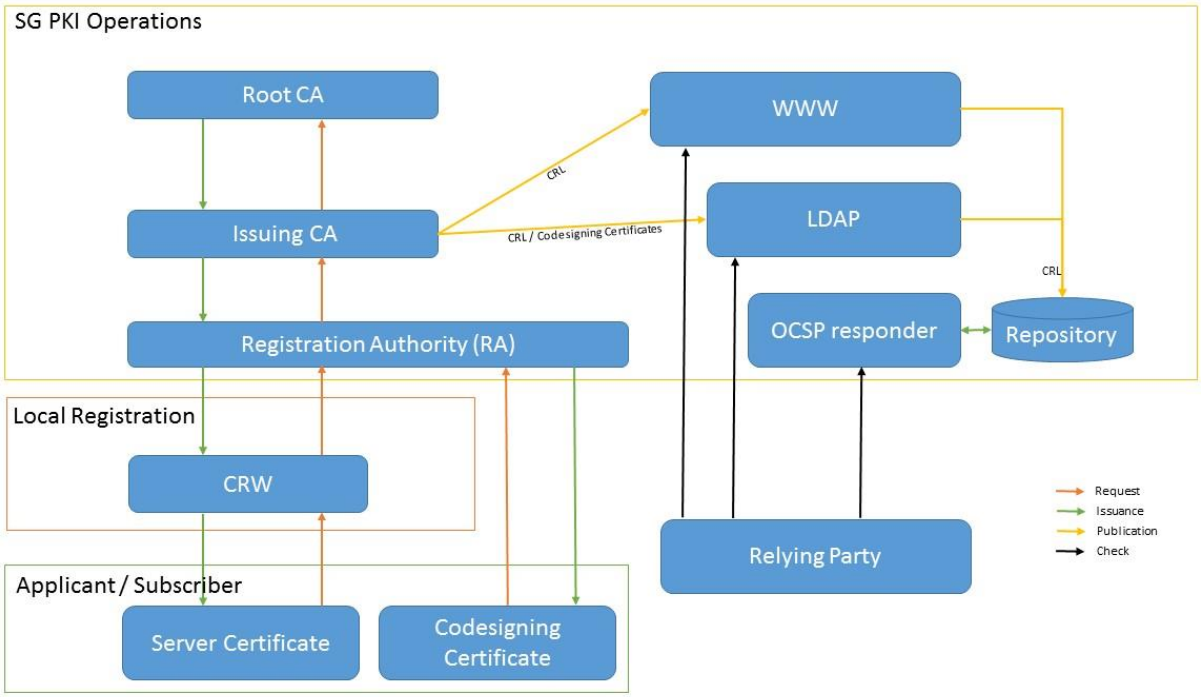
Position	OID Component	Meaning of OID Component
1	2	joint-iso-itu-t
2	16	country
3	756	ch
4	1	organization[1]
5	17	Bundesamt für Informatik und Telekommunikation
6	3	AdminPKI
7	61	SG Root CA III
8	0	CP/CPS

Table 1: SG Root CA III CP/CPS OID Components

[1] Allocated by the Federal Office of Communications (OFCOM). A search function of object identifiers allocated by OFCOM is available under: http://www.eofcom.admin.ch/eofcom/public/searchEofcom_oid.do

1.3 PKI participants

Figure 1: Overview over the PKI Participants



1.3.1 Certification authorities

SG Root CA III operating at first – root – level acts as the common trust reference for all subordinated CAs and subscriber certificates. It issues CA certificates to the CAs operating at second level exclusively, while these CAs in turn issue subscriber certificates.

SG Root CA III and all subordinated CAs are operated exclusively by Swiss Government PKI staff appointed to the task.

1.3.1.1 Root Authorities

This CP/CPS covers the following Root Certification Authority operated by Swiss Government PKI:

1.3.1.1.1 Swiss Government Root CA III

Serial Number	00 fb 1f 0b 42 2b a8 41 3e 57 d1 ee 2a 6e 5a 4f bb
Subject DN	CN = Swiss Government Root CA III OU = www.pki.admin.ch O = Swiss Government PKI C = CH
Subject Alternative Name	none
Validity Period	From Friday, April 15 2016 09:00:00 UTC+1 To Monday, April 15 2041 08:59:59 UTC+1

Public Key	30 82 02 0a 02 82 02 01 00 e1 43 86 8e 4f 18 94 ba d3 c2 39 70 6d 5d 69 51 84 59 bc bb c8 7f 2f fd 17 a3 78 9c bd d8 92 e3 d8 78 21 3e bb 9a 5f fb b2 65 50 72 b6 a7 ec a5 e7 c1 c5 00 04 e3 cc b3 02 4a f9 00 db 6f 6d bb 93 17 44 f9 23 c2 56 3a 30 1f 81 79 fb 64 bf f5 54 85 bf 3b 2b 6f 95 04 06 5d 68 0a c3 8f b8 2b 66 12 be a2 d8 5a 94 05 7d af c1 13 06 a6 91 3a 3f 19 0b 85 83 c0 96 5d f3 81 c8 13 8a f5 10 4b a0 75 3a 5b a3 40 07 bd a1 66 18 65 84 54 79 91 9a d3 72 84 66 d5 0d e6 3b 5a ea fa db a1 54 fd 00 23 59 e8 57 ea 9c b7 f4 8f 41 0b 69 b1 47 b0 9a 2f 62 da 9a 19 ad a0 95 30 cd 2e ad 67 bb 6d f9 36 43 b7 94 79 c9 90 09 00 69 5f 97 a6 d3 6f 25 e8 ef 62 87 77 d7 a6 d9 4e 1c 5f 61 66 d0 b1 70 d5 e0 62 20 36 d8 96 40 f8 5e 31 de 41 99 69 10 d6 a0 ee 3d ad 13 2e d2 94 4a 8d 80 1d dc 8c 46 21 56 8b 49 5b de a1 d8 03 ca ce d8 65 b4 b0 05 3d 26 69 4a 6d a5 8c 79 2f a4 8f 12 78 10 e9 b2 09 08 43 c3 c6 04 bb 33 3e 47 35 a5 5c 20 20 0a e2 36 f8 63 86 e4 0d f4 3e 14 79 be 45 07 b4 8b 09 93 f5 f6 2a 26 a1 bd 44 c7 f3 50 0d 0d 61 9b 3b 11 df a8 83 ea 22 2c 95 44 0d 39 41 63 4d a8 2b 6d 68 a5 4b 9f 40 87 6a 3c 45 0a be 72 a7 88 be f0 39 2a 5b ef 59 a4 20 ef b4 dc c3 da 41 db 41 a5 ba 22 5f 97 a3 c8 63 a1 24 2d 4e 25 a0 c3 17 28 c5 88 41 93 96 64 66 37 43 05 9b 15 7c b6 be 9e fb 1b c8 66 18 ba 14 ef b9 18 cf 84 69 9b 9f bd 82 07 12 6d 1b 19 bf 30 7e f1 92 0e c0 4c 16 ff d1 3e 6f f8 ab b2 61 9a 68 43 e2 0a 54 c7 01 a3 57 8e f3 44 06 22 c3 70 a6 bb a5 b3 cc 82 18 d8 40 8e bd ea 70 41 6f 94 57 0c be 07 74 6e 8e 93 7a 19 8f c6 68 fc 1b a5 45 b3 b9 85 a9 02 03 01 00 01
Signature Algorithm	sha256RSA

Table 2: Swiss Government Root CA III

1.3.1.2 Issuing Subordinate Certification Authorities

This CP/CPS covers the following Subordinate Certification Authorities operated by Swiss Government PKI:

1.3.1.2.1 Swiss Government Public Trust Standard CA 02

Serial Number	51 fc 89 49 2b 49 68 c0 9e c3 21 60 76 b6 56 63
Subject DN	CN = Swiss Government Public Trust Standard CA 02 OU = Certification Authorities OU = Services O = Swiss Government PKI C = CH
Subject Alternative Name	none
Validity Period	From Wednesday, May 11 2016 10:36:42 UTC+1 To Sunday, May 11 2031 10:36:41 UTC+1

Public Key	30 82 02 0a 02 82 02 01 00 a7 ea 0c 28 f1 59 f6 d2 34 1d 5b d3 d3 08 9d cd 12 f2 68 dc f6 b5 3e 6a c0 64 36 52 cf ec 22 36 b8 26 47 61 e0 84 6a 0d b2 54 7a 28 6f 0b 60 a4 25 81 71 32 56 c9 04 b1 df 1c bc 31 94 8e a7 23 e7 8b 58 a6 74 57 5e 3e a3 aa 75 87 42 96 f9 72 07 a0 60 ff 94 dd 47 78 7d 19 fb 0c e5 53 df 49 9b 75 95 aa f3 0e df 52 c0 67 09 33 0c 57 10 53 09 f3 e4 2c db 67 b4 20 69 27 35 16 12 d4 1e 0e 23 f7 4c 2d 14 61 ed 9a d5 03 71 c8 25 32 d9 45 aa 0f 42 a6 4b 18 7f b5 b1 45 8c b5 fd 37 7c ee b4 43 b7 7a 70 d0 86 94 50 5c 85 87 39 e3 69 b5 09 25 e8 a9 31 85 2f 55 bf 29 14 34 68 59 ac 91 98 f7 5e 9b 06 3e ef 03 0f 99 fc 04 fc 2e aa 8e 67 05 db 73 33 c7 9a 90 b0 02 85 2f e1 f7 6d ad 95 39 1c b1 b8 4f 87 8c dc 5c b5 f4 5f 35 55 c5 91 e7 a0 fa 63 7c c4 39 6d 33 25 7c 72 94 11 e5 2a cf 15 12 1b 86 5c e8 8f b5 0e e2 db 83 61 93 c8 3b fa 67 9e 97 a7 f3 19 e8 5d 0a 0a 76 78 e7 86 d8 91 61 d7 8d f4 b7 ec ef 47 c3 3b c4 9a 8d a2 88 87 d2 07 78 24 c0 db 4c 22 2e e4 02 9f 11 cf cf 13 68 22 db 8a 57 7b 22 3a cc 39 f8 3d 37 b9 f8 fe 36 84 28 83 ca a2 56 12 32 a2 1e 2d bf a3 93 8d 86 fd d7 dc ca 67 cb 7c a6 9d 7c f5 ef 92 af 79 e9 62 16 14 de 68 d2 94 74 0e 88 c1 52 5e 94 07 8a 36 e1 77 bc ea 19 af f8 19 e1 1f 15 e5 da 48 06 bc b6 43 63 c3 00 57 51 73 e1 08 5f 6f af 33 f1 61 6d bc df 9b 81 11 24 e7 cd 51 7d e1 5e 21 60 77 3f e0 f7 13 4f 82 9b bb 58 71 65 0a c5 10 44 a3 e9 85 2f 96 7e 2e 96 54 fe 50 a5 a3 15 82 e4 fe f5 11 8c bb 66 08 6a 95 35 e3 20 1e ac 8b 2d ad c6 f9 be 8c cf 53 7d ae 2c 8d 64 ab 1f 6a 97 bf 65 ec 31 a5 43 5e f1 97 32 f2 7f 02 03 01 00 01
Signature Algorithm	sha256RSA

Table 3: Swiss Government Public Trust Standard CA 02

1.3.1.2.2 Swiss Government Public Trust EV CA 02

Serial Number	63 8b 4b d1 42 77 a6 67 fc 4a 80 af e9 6a 95 ba
Subject DN	CN = Swiss Government Public Trust EV CA 02 OU = Certification Authorities OU = Services O = Swiss Government PKI C = CH
Subject Alternative Name	none
Validity Period	From Wednesday, May 11 2016 13:33:59 UTC+ 1 To Sunday, 11. May 11 2031 13:33:59 UTC+1
Public Key	30 82 02 0a 02 82 02 01 00 e1 4f f2 e2 b6 24 9e 20 01 b8 45 51 25 2a b6 8d 18 0f 17 39 94 9f ea b8 cc 5b 19 f1 61 24 2c b2 17 52 65 cb 2c 3e a2 d0 d0 cb af 33 42 9e d0 55 6d 3a 54 63 87 50 13 f1 9a 2b 5e 66 0d b5 40 14 a5 ab b6 16 27 bb 24 99 fb 07 83 91 7d e6 c0 a3 00 18 7e 09 97 a1 c8 ab b6 56 c6 44 65 ad c4 42 70 1f 9d 34 3c 1c 92 4d b0 fa ab 71 f8 fb

	49 1a ed a0 10 67 36 55 1b 86 04 fc e0 da 7a ea 17 69 c2 16 76 c6 ca 42 ee b8 5d b1 b8 37 4c 4c 3d 65 7b 94 61 d5 ef e5 8f f2 fe da 74 06 17 47 96 4d 24 e9 a3 9d 70 1a 0e 36 a7 53 00 96 52 e0 a9 c8 4d 86 5e 51 b6 cf 60 4f c5 e4 fe 9e 4f c4 bd 4c b1 d2 9c 81 a5 71 d3 93 9c 1d 95 4e a4 2a 62 45 52 ad f2 33 c3 0a 16 84 7b cd 03 a4 1e 9c 0f 7a 4c 5e 06 ee 5b d1 c3 84 04 f7 4a a9 3b 9e 6e a8 66 1e 1f 15 a3 d7 6d 4a dc 11 1d 14 14 fa b2 31 35 f4 cb eb 6f 1f 5d f7 78 47 e4 08 ba 6c 9e 4d 16 26 c1 21 c9 16 cc b4 e0 90 92 48 be d8 b4 95 25 ff 91 dd da 69 18 42 ab 78 ba c3 50 24 b4 59 75 71 ef 99 89 5e e4 39 ab b7 8c df 1f a1 c4 be 82 c1 92 26 e5 d2 4b 10 1f ab a9 26 29 98 3c 01 61 c1 b1 a6 6f 16 59 ca 04 8c 46 ea a0 cb 1e 7d 2c 74 d2 a7 8e c4 b9 d4 9d 53 7e e6 37 a5 b5 fa 93 e1 71 98 fa 97 b0 ee 8d 8a 47 81 87 d3 68 3b 5d c7 04 3d 06 a1 3a 5d 41 66 a1 a8 15 42 14 db 1a 20 83 3f aa e5 61 b3 10 c1 8f f4 c4 e0 b6 85 e6 25 68 06 c9 c5 91 95 54 17 a7 2a e6 29 20 8d fe f1 15 fe 00 b2 3b 5d d1 fe 87 e8 bb c0 d4 58 77 de e7 ba da 85 79 ee c1 16 92 4d 20 10 ca 07 18 4a 82 c7 39 08 7b 31 2b 1b 16 4c ba fe 32 ac 52 1f 9b 1c 21 03 f5 45 a4 1f 24 67 00 86 05 2b fd eb 02 8c 1e 11 e4 84 da 13 83 2e 16 f8 ef d3 02 03 01 00 01
Signature Algorithm	sha256RSA

Table 4: Swiss Government Public Trust EV CA 02

1.3.1.2.3 Swiss Government Public Trust Codesign CA 02

Serial Number	
Subject DN	
Subject Alternative Name	
Validity Period	
Public Key	
Signature Algorithm	
Fingerprint	

Table 5: Swiss Government Public Trust Codesign CA 02

1.3.1.2.4 Swiss Government Public Trust EV Codesign CA 02

Serial Number	
Subject DN	
Subject Alternative Name	
Validity Period	
Public Key	
Signature Algorithm	
Fingerprint	

Table 6: Swiss Government Public Trust EV Codesign CA 02

1.3.2 Registration authorities

To cope with the variety of certificates issued by the CA's subordinated to SG Root CA III, the submission of requests as well as the registration of applicants and requests MAY be done by individual Registration Agents.

1.3.2.1 Registration Agent

1.3.2.2 Registration Agent tasks

- Generate and submit certificate requests.
- Certificate requests have to be supplied using a tool provided by SG PKI.
- Transfer the certificates to the applicants once their certificates have been issued by CA's subordinated to SG Root CA III.
- Generate and submit revocation requests.
- Verify and approve revocation requests

1.3.2.3 Registration Agent contractual requirement

SG PKI requires Registration Agents by contract to:

- 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 SG PKI Root III CP/CPS
- Agree to accept regular audits to validate compliance with SG PKI Root III CP/CPS
- Supply appropriate information for the requested Fully-Qualified Domain Name(s) as specified in Section 3.2.2.4. (Domain Authorization Letter)

SG PKI is keeping record of all contracts and annually verifies the Registration Agents audit and domain authorization status.

1.3.2.4 Registration Agent - Identification

To act as Registration Agent, a valid Certificate of type "Klasse B" issued by a Subordinate CA to Swiss Government Root CA I [20] is required as means of identification.

1.3.3 Subscribers

As defined in 1.6.1 definitions

1.3.4 Relying parties

Relying parties are:

- All subscribers, i.e. holders of subscriber certificates issued by any of the CA's subordinated to SG Root CA III.
- Any natural person or Legal Entitiy that relies on a valid certificate issued under this CP/CPS.
- An application software supplier is not considered a relying Party when software distributed by such supplier merely displays information relating to a certificate.

The applications used for verifying signatures/validating certificate chains must adhere to the procedures as per ITU-T recommendation X.509.

1.3.5 Other participants

No stipulation

1.4 Certificate Usage

The issuance, distribution and usage of all certificates issued by the SG Root CA III and its subordinated CAs MUST comply with this CP/CPS. Any usage, however, shall be limited to such entities and subject to section 9.8.1, 9.8.2, and these entities shall be solely responsible for any harm or liability caused by such usage.

1.4.1 Appropriate certificate uses

The following table provides an overview of certificate types issued under this CP/CPS and their appropriate usage.

DV SSL Certificates	Used to secure online communication where the risks and consequences of data compromise are low, including non-monetary transactions or transactions with little risk of fraud or malicious access.
OV SSL Certificates	Used to secure online communication where the risks and consequences of data compromise are moderate, including transactions having substantial monetary value or risk of fraud or involving access to private information where the likelihood of malicious access is substantial.
EV SSL Certificates	Used to secure online communication where risks and consequences of data compromise are high, including transactions having high monetary value, risk of fraud, or where involving access to private information where the likelihood of malicious access is high.
Code Signing Certificates, including EV Code Signing	Establishes the identity of the Subscriber named in the certificate and that the signed code has not been modified since signing.

Table 7: Certificate Types issued under SG Root CA III

Subscribers using Certificates within their own environment may place further restrictions on Certificate use within these environments. SG PKI and other SG PKI Participants, however, are not responsible for monitoring or enforcing any such restrictions in these environments.

All SG PKI Certificates are explicit in function and have the respective EKU specified. For example, SSL Server Authentication Certificates may not be used for any functions except Server Authentication.

Also, with respect to SG PKI Certificates, the key usage extension is intended to limit the technical purposes for which a private key corresponding to the public key in a Certificate may be used. See section 6.1.7. In addition, Subscriber Certificates shall not be used as CA Certificates. This restriction is confirmed by the absence of a Basic Constraints extension. See section 7.1.2. The effectiveness of extension-based limitations, however, is subject to the operation of software manufactured or controlled by entities other than SG PKI

Certificates shall be used only to the extent where use is consistent with applicable law. Key usage and extended key usage combinations shall be strictly limited.

1.4.2 Prohibited certificate uses

Certificates issued under this CPS may not be used for MITM, network traffic management or similar.

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 of this document).

1.5.2 Contact persons

1.5.2.1 PKI Operations

Contact person for all operative inquiries is the SG PKI Operations Manager

Swiss Government
Federal Office of Information Technology, Systems and Telecommunication FOITT
PKI Operations Manager
BTR-BFS-BFO
Monbijoustrasse 74
3003 Berne
Switzerland

1.5.2.2 PKI Service & Design

Contact person for all security related inquiries is the SG PKI Service & Design Manager

Swiss Government
Federal Office of Information Technology, Systems and Telecommunication FOITT
PKI Service & Design Manager
BTR-BFS-BFK
Monbijoustrasse 74
3003 Berne
Switzerland

1.5.3 Person determining CP/CPS suitability for the policy

The PKI Management Board (PKI Operations Manager and the PKI Service & Design Manager) determines the document's suitability for the purposes of the accepted policies.

1.5.4 CP/CPS approval procedures

See section 9.12 of this document.

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
Applicant	The natural person or Legal Entity that applies for (or seeks renewal of) a Certificate. Once the Certificate issues, 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
Applicant Representative	A natural person or human sponsor who is either the Applicant, employed by the Applicant, or an authorized agent who has express authority to represent the Applicant: (i) who signs and submits, or approves a certificate request on behalf of the Applicant, and/or (ii) who signs and submits a Subscriber Agreement on behalf of the Applicant, and/or (iii) who acknowledges and agrees to the Certificate Terms of Use on behalf of the Applicant when the Applicant is an Affiliate of the CA.	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
Attestation Letter	A letter attesting that Subject Information is correct written by an accountant, lawyer, government official, or other reliable third party customarily relied upon for such information.	BR

Term	Definition	Source
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
CAA	From RFC 6844 (http:tools.ietf.org/html/rfc6844): "The Certification Authority Authorization (CAA) DNS Resource Record allows a DNS domain name holder to specify the Certification Authorities (CAs) authorized to issue certificates for that domain. Publication of CAA Resource Records allows a public Certification Authority to implement additional controls to reduce the risk of unintended certificate misissue."	BR
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 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
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
Cross Certificate	A certificate that is used to establish a trust relationship between two Root CAs	BR
Delegated Third Party	A natural person or Legal Entity that is not the CA but is authorized by the CA to assist in the Certificate Management Process by performing or fulfilling one or more of the CA requirements found herein.	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 B" certificate, issued under Swiss Government Root CA I [20]	SG PKI
Domain Authorization Document	Documentation provided by, or a CA's documentation of a communication with, a Domain Name Registrar, the Domain Name Registrant, or the person or entity listed in WHOIS as the Domain Name Registrant (including any private, anonymous, or proxy registration service) attesting to the authority of an Applicant to request a Certificate for a specific Domain Namespace.	BR
Domain Name	The label assigned to a node in the Domain Name System	BR
Domain Namespace	The set of all possible Domain Names that are subordinate to a single node in the Domain Name System.	BR

Term	Definition	Source
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
Fully-Qualified Domain Name	A Domain Name that includes the labels of all superior nodes in the Internet Domain Name System.	BR
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
High Risk Certificate Request	A Request that the CA flags for additional scrutiny by reference to internal criteria and databases maintained by the CA, which may include names at higher risk for phishing or other fraudulent usage, names contained in previously rejected certificate requests or revoked Certificates, names listed on the Miller Smiles phishing list or the Google Safe Browsing list, or names that the CA identifies using its own risk-mitigation criteria.	BR
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. This could be either a Root CA or a Subordinate CA	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 B	Swiss Government issued Certificates of type “Klasse B” are combining the government identity directory (AdminDir) and a qualified identification process in combination with a strong authentication token (Smartcard)	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	BR

Term	Definition	Source
	Organization for Standardization's applicable standard for a specific object or object class.	
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 Organziation is a legal entity represented by natural persons	SG PKI
Parent Company	A company that Controls a Subsidiary Company	BR
Private Key	The key of a Key Pair that is kept secret by the holder of the Key Pair, and that is used to create Digital Signatures and/or to decrypt electronic records or files that were encrypted with the corresponding Public Key.	BR
Public Key	The key of a Key Pair that may be publicly disclosed by the holder of the corresponding Private Key and that is used by a Relying Party to verify Digital Signatures created with the holder's corresponding Private Key and/or to encrypt messages so that they can be decrypted only with the holder's corresponding Private Key.	BR
Public Key Infrastructure	A set of hardware, software, people, procedures, rules, policies, and obligations used to facilitate the trustworthy creation, issuance, management, and use of Certificates and keys based on Public Key Cryptography.	BR
Publicly-Trusted Certificate	A Certificate that is trusted by virtue of the fact that its corresponding Root Certificate is distributed as a trust anchor in widely-available application software	BR
Qualified Auditor	A natural person or Legal Entity that meets the requirements of Section 8.3 (Auditor Qualifications)	BR
Registered Domain Name	A Domain Name that has been registered with a Domain Name Registrar	BR
Registration Authority (RA)	Any Legal Entity that is responsible for identification and authentication of subjects of Certificates, but is not a CA, and hence does not sign or issue Certificates. An RA may assist in the certificate application process or revocation process or both. When "RA" is used as an adjective to describe a role or function, it does not necessarily imply a separate body, but can be part of the CA.	BR
Reliable Data Source	An identification document or source of data used to verify Subject Identity Information that is generally recognized among commercial enterprises and governments as reliable, and which was created by a third party for a purpose other than the Applicant obtaining a Certificate	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
Reserved IP Address	An IPv4 or IPv6 address that the IANA has marked as reserved: http://www.iana.org/assignments/ipv4-address-space/ipv4-address-space.xml http://www.iana.org/assignments/ipv6-address-space/ipv6-address-space.xml	BR
Root CA	The top level Certification Authority whose Root Certificate is distributed by Application Software Suppliers and that issues Subordinate CA Certificates	BR

Term	Definition	Source
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
Sovereign State	A state or country that administers its own government, and is not dependent upon, or subject to, another power	BR
Subject	The natural person, device, system, unit, or Legal Entity identified in a Certificate as the Subject. The Subject is either the Subscriber or a device under the control and operation of the Subscriber	BR
Subject Identity Information	Information that identifies the Certificate Subject. Subject Identity Information does not include a domain name listed in the subjectAltName extension or the Subject commonName field.	BR
Subordinate CA	A Certification Authority whose Certificate is signed by the Root CA, or another Subordinate CA.	BR
Subscriber	A natural person or Legal Entity to whom a Certificate is issued and who is legally bound by a Subscriber or Terms of Use Agreement	BR
Subscriber Agreement	An agreement between the CA and the Applicant/Subscriber that specifies the rights and responsibilities of the parties	BR
Subsidiary Company	A company that is controlled by a Parent Company	BR
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
Terms of Use	Provisions regarding the safekeeping and acceptable uses of a Certificate issued in accordance with these Requirements when the Applicant/Subscriber is an Affiliate of the CA	BR
Trustworthy System	Computer hardware, software, and procedures that are: reasonably secure from intrusion and misuse; provide a reasonable level of availability, reliability, and correct operation; are reasonably suited to performing their intended functions; and enforce the applicable security policy.	BR
Unregistered Domain Name	A Domain Name that is not a Registered Domain Name	BR
Valid Certificate	A Certificate that passes the validation procedure specified in RFC 5280	BR
Validation Specialists	Someone who performs the information verification duties specified by these Requirements.	BR
Validity Period	The period of time measured from the date when the Certificate is issued until the Expiry Date.	BR
Wildcard Certificate	A Certificate containing an asterisk (*) in the left-most position of any of the Subject Fully-Qualified Domain Names contained in the Certificate.	BR

1.6.2 Acronyms

Term / Acronym	Full text	Explanation
AdminDir	Admin Directory	A central directory service, used by the Swiss Government. AdminDir is compliant with ITU-T recommendation X.500 (http:// itu.int/ITU-T/X.500)
ARL	Authority Revocation List	A list of revoked Certification Authority certificates.

Term / Acronym	Full text	Explanation
BR	Baseline Requirements	Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates
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	Certification 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.
DV	Domain Validation	Domain validation provides assurance that the subscriber is entitled to use the domain name(s) listed in the certificate application, that the domain owner or technical contact has authorized the certificate application, and that the person submitting the certificate application (Registration Agent) on behalf of the Subscriber was authorized to do so.
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.
EV	Extended Validation	Beyond Organization Validation, Extended Validation procedure carried out by the issuing CA verifies that the web site the user is accessing is controlled by a specific legal entity identified in the EV Certificate by name, address of Place of Business, Jurisdiction of Incorporation or Registration and Registration Number or other disambiguating information. Extended Validation is carried out according to the Guidelines of CA/Browser Forum (cabforum.org)
FCA	Federal Customs Administration	The Swiss Federal Customs Administration
FDF	Federal Department of Finance	The Swiss Federal Department of Finance
FIPS	Federal Information Processing Standards	FIPS are issued by NIST, the U.S. National Institute of Standards and Technology http://www.itl.nist.gov/fipspubs/ .
FOITT	Swiss Federal Office of Information Technology, Systems and Telecommunication	The Federal Office of Information Technology, Systems and Telecommunication (FOITT or BIT for the German name) is one of the internal ICT service providers in the Federal Administration. 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
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.
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 or BAKOM for the German name) handles questions related to telecommunications and broadcasting (radio and television) www.bakom.admin.ch .
OID	Object Identifier	A unique numerical sequence allowing the identification of any "thing", in particular also documents.
OV	Organization Validation	Organization validation provides assurance that the subscriber is entitled to use the domain name(s) listed in the certificate application, that the subscriber organization does in fact exist, that the organization has authorized the certificate application, and that the person submitting the certificate application (Registration Agent) on behalf of the Subscriber was authorized to do so. OV certificates MAY contain one or more domain names. Those MUST be validated to the same or greater degree as DV certificates.
PIN	Personal Identification Number	A personal identification number is a numeric password, that can be used to authenticate the user to the system. A password is a string of characters that people can use to log on to a computer and access files, programs, and other resources.
PKCS	Public-key Cryptography Standards	PKCS are specifications produced by RSA Laboratories in cooperation with secure systems developers worldwide http://www.rsa.com/rsalabs/node.asp?id=2124 .
PKCS#10		Syntax for certification requests. https://tools.ietf.org/html/rfc2986
PKCS#12		The specification of a format for storing and transferring key pairs and certificates securely (encrypted). https://tools.ietf.org/html/rfc7292
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.
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.

Term / Acronym	Full text	Explanation
RFC	Request For Comments	Standards issued by the Internet Engineering Task Force (IETF) http://www.ietf.org/ .
RSA	Rivest-Shamir-Adleman	The most widely used algorithm today supporting public key cryptography.
TLS	A secure communication protocol	http://www.rfc-base.org/txt/rfc-5246.txt
SG PKI	Swiss Government PKI	FOITT operational unit responsible for and operating all PKI services provided by the Swiss federal administration.
SLA	Service Level Agreement	Service contract defining the PKI services formally.
SSL	A secure communication protocol	Actually obsolete, today TLS is used.

Table 8: Definitions and Acronyms

1.6.3 References

References are listed in Annex A (9.18)

1.6.4 Conventions

Terms not otherwise defined in this CP/CPS are defined in applicable agreements, user manuals, Certificate policies or other relevant documentation.

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 SG Root CA III and its subordinated CAs publicly available through SG PKI's web site (www.pki.admin.ch).

2.2 Publication of certification information

SG PKI publishes information related to certificates issued by SG Root CA III and its subordinated certification authorities with the following methods:

- Publication on SG PKI Website:
    - The current version of the CP/CPS for the Root CA and its subordinated certification authorities.
    - A schematic overview of the actual CA structure
    - Certificate(s) of the Root CA
    - Fingerprint of the certificate of the Root CA
    - Certificate(s) of each Sub CA
    - Fingerprint of the certificate(s) of each Sub CA
- Browser Testsites:
    - SG PKI Domain-Validated SSL Certificates
        - VALID https://www.valid-dv.pki.admin.ch
        - REVOKED https://www.revoked-dv.pki.admin.ch
        - EXPIRED https://www.expired-dv.pki.admin.ch
    - SG PKI Organization-Validate SSL Certificates
        - VALID https://www.valid-ov.pki.admin.ch
        - REVOKED https://www.revoked-ov.pki.admin.ch
        - EXPIRED https://www.expired-ov.pki.admin.ch
    - SG PKI Extended Validation (EV) SSL Certificates
        - VALID https://www.valid-ev.pki.admin.ch
        - REVOKED https://www.revoked-ev.pki.admin.ch
        - EXPIRED https://www.expired-ev.pki.admin.ch
- OCSP responder at www.pki.admin.ch/aia/ocsp
- WWW repository providing the CRL and ARL. Path is specified in the respective certificate.
- LDAP repository (optional): Providing the CRL and ARL. Path is specified in the respective certificate.

2.3 Time or frequency of publication

This CP/CPS is published in electronic form (Portable Document Format on the SG PKI's web site at www.pki.admin.ch.

Published information shall be updated at the following intervals:

- Whenever a CA certificate and CRL are issued or re-keyed
- Whenever this CP/CPS is amended

Other Amendments to this CP/CPS are processed in accordance with section 9.12.

Updates to Subscriber Agreements and Relying Party Agreements are published as necessary.

2.4 Access controls on repositories

Information published on the web site of SG PKI is publicly available information.

Read only access to such information is unrestricted.

SG PKI has implemented logical and physical security measures to prevent unauthorized changes on its repositories.

All published documents in Portable Document Format SHALL be a Digitally Signed Document, so the document integrity can be validated.

3 Identification and Authentication

3.1 Naming

3.1.1 Types of names

With all certificates issued, SG PKI as well as the subscriber (certificate holder) are identified by a distinguished name DN. The DN is a non-empty sequence of printable characters as per ITU-T recommendation X.501.

SG Root CA III and its subordinated CAs use a standard form of DN (for details see section 7.1.4).

3.1.2 Need for names to be meaningful

Subscriber names must be meaningful in that they either identify

- an organization
- a natural person
- a system name
- a Trademark/DBA name

3.1.3 Anonymity or pseudonymity of subscribers

No stipulation

3.1.4 Rules for interpreting various name forms

Distinguished names in certificates are interpreted using X.500 standards and ASN.1 syntax. RFC 2253 and RFC 2616 provide further information on how X.500 distinguished names are interpreted as URI and HTTP references.

3.1.5 Uniqueness of names

Subject fields in all certificates must be unique in such a manner that all valid certificates with identical subject fields must belong to the same individual, organization or domain owner.

3.1.6 Recognition, authentication, and role of trademarks

Certificate Applicants are prohibited from using names in their Certificate Applications that infringe upon the intellectual property rights of others. SG PKI, however, does not verify whether a certificate applicant has intellectual property rights in the name appearing in a Certificate Application or arbitrate, mediate, or otherwise resolve any dispute concerning the ownership of any domain name, trade name, trademark, or service mark. SG PKI is entitled, without liability to any Certificate Applicant, to reject or suspend any Certificate Application because of such dispute.

3.2 Initial Identity Validation

3.2.1 Method to prove possession of private key

SG PKI verifies the Certificate Applicant's possession of a private key through the use of a digitally signed certificate request pursuant to PKCS #10.

3.2.2 Authentication of organization and Domain Identity

SG PKI Root III does not process applications that contain Subject identity Information comprised only of the countryName field.

SG PKI verifies the identity of all Applicants, and the authenticity of the applicant represantative's certificate request using a verification process meeting the requirements of Section 3.2.2.1.

SG PKI will inspect any document relied upon under this Section for alteration or falsification

3.2.2.1 Identity

SG PKI verifies the identitiy and other information to included in the certificate at least by one of the following methods:

- The authenticity of legal persons and represantitives thereof is verified using information identified by the Business Identification Number of the Swiss Federal Statistical Office FSO. [21]
- The authenticity of federal organizations and represantatives thereof is verified by consulting the directories of the Swiss Federal Chancellory [22]
- The authenticity of employees or individuals working as contractors of the federal administration is verified by consulting the directory of Swiss Administrative Employees (AdminDir) [4]
- Other identities or informations thereof are validated in the respective directories SG PKI finds appropriate for use as specified in 3.2.2.7

3.2.2.2 DBA/Tradename

If the Subject Identity is to include a DBA/Tradename, SG PKI will verify the Applicant's right to use the DBA/Tradename using at least one of the following methods;

- Documentation provided by, or in communication with a government agency in the jurisdiction of the Applicant's legal creation, existence, or recognition
- Communication with a government agency responsible for the management of such DBAs or tradenames
- An attestation letter accompanied by documentary support
- A form of identification that SG PKI determines to be reliable

3.2.2.3 Verification of Country

If the subject:countryName field is present, then SG PKI verifies the country associated with the Subject using a mehod identified in Section 3.2.2.1

3.2.2.4 Authorization by Domain Name Registrant

For each Fully-Qualified Domain Name listed in a Certificate, SG PKI confirms that, as of the date the Certificate was issued, the Applicant (or the Applicant's Parent Company, Subsidiary Company or Affiliate, collectively referred to as "Applicant" for the purpose of this Section) either is the Domain Name Registrant or has control over the FQDN by:

- communicating directly with the Domain Name Registrant using the contact information listed in the WHOIS records "registrant", "technical" or "administrative" field.
- Relying upon a Domain Authorization Document approved by the Domain Name Registrant. The document must be dated on or after the certificate request date or used by SG PKI to verify a previously issued certificate and that the Domain Name's WHOIS record has not been modified since the previous certificate issuance.

3.2.2.5 Authentication for an IP Address

SG PKI Root III and its Subordinated CAs do not issue certificates for IP Addresses.

3.2.2.6 Wildcard Domain Validation

SG PKI Root III and its Subordinated CAs do not not issue Wildcard Domain Validation Certificates.

3.2.2.7 Data Source Accuracy

Prior to use any data source as a reliable data source, SG PKI evaluates the source for its reliability, accuracy and resistance to alteration or falsification.

3.2.3 Authentication of individual identity

For individual identity authentication a certificate of type "Klasse B" issued under the "Swiss Government Root CA I" [20] SHALL be used.

Certificates of type "Klasse B" are combining the government identity directory (AdminDir) and a qualified identification process in combination with a strong authentication token (Smartcard)

3.2.4 Non-verified subscriber information

No stipulation.

3.2.5 Validation of authority

Authority is validated according to the procedures defined in 3.2.2 and 3.2.3

3.2.6 Criteria for interoperationor Certification

No stipulation.

3.3 Identification and authentication for re-key requests

3.3.1 Identification and authentication for routine re-key

For re-keying certificates the identical process is used as for obtaining initial certificates.

3.3.2 Identification and authentication for re-key after revocation

For certificate re-key after revocation the process as per section 3.3.1 applies.

3.4 Identification and authentication for revocation request

The detailed process for revoking certificates is documented in section 4.9.3.

Any requester may authenticate a revocation request by

- presenting himself in person to a Registration Agent,
- submitting a message to a Registration Agent that requests revocation and contains a digital signature verifiable with reference to the certificate to be revoked.

Depending on the request verification the Registration Agent decides if the certificate in question is to be revoked.

SG PKI Administrators are entitled to request the revocation of end-entity subscriber certificates. SG PKI authenticates the identity of SG PKI administrators before permitting them to perform revocation functions.

4 Certificate Life-Cycle Operational Requirements

4.1 Certificate application

4.1.1 Who can submit a certificate application

4.1.1.1 Server Certificates

The server certificate application SHALL be submitted to the Registration Agent by a subscriber or an authorized representative of the same organization as that of the subscriber.

4.1.1.2 Codesigning Certificates

Applicants for Code Signing Certificates MUST have a valid “Klasse B” Certificate issued under Swiss Government Root CA I [20] for individual identification purpose.

4.1.2 Enrollment process and responsibilities

4.1.2.1 DV Server Certificates

Prior to the issuance of a DV Server Certificate, SG PKI obtains and approves the following documentation from the Applicant:

- a valid Domain Authorization Letter for the requested FQDN
  (MAY be in form of a Digitally Signed Document)
- a Terms & Conditions Agreement (MAY be in form of a Digitally Signed Document)
- a certificate request in form of a PKCS#10

4.1.2.2 OV Server Certificates

Prior to the issuance of a OV Server Certificate, SG PKI obtains and approves the following documentation from the Applicant:

- a signed Organization Authorization Letter for the requested Organization
  (MAY be in form of a Digitally Signed Document)
- a valid Domain Authorization Letter for the requested FQDN
  (MAY be in form of a Digitally Signed Document)
- a signed Terms & Conditions Agreement (MAY be in form of a Digitally Signed Document)a certificate request in form of a PKCS#10

4.1.2.3 EV Server Certificates

Prior to the issuance of a EV Server Certificate, SG PKI obtains and approves the following documentation from the Applicant:

- a signed Organization Authorization Letter for the requested Organization entry

(MAY be in form of a Digitally Signed Document)

- a valid Domain Authorization Letter for the requested FQDN
  (MAY be in form of a Digitally Signed Document)
- a signed Terms & Conditions Agreement (MAY be in form of a Digitally Signed Document)
- a certificate request in form of a PKCS#10

4.1.2.4 Codesigning Certifiates

Prior to the issuance of a Codesigning or EV Codesigning Certificate, SG PKI obtains the following documentation from the Applicant:

- a signed Confirmation Letter for the requested Organization entry in form of a Digitally Signed Document
- a signed Codesigning Terms & Conditions Agreement in form of a Digitally Signed Document
- a signed Codesigning Certificate Guidelines Agreement in form of a Digitally Signed Document

4.2 Certificate application processing

4.2.1 Performing identification and authentication functions

SG PKI identifies Registration Agents initially and authorizes them to access its registration application for requesting and downloading certificates. The registration application then authenticates the agents with each certificate request they submit.

Registration Agents are authenticated by the registration application on the basis of enhanced certificates of type “Klasse B” issued under Swiss Government Root I [20]

Before issuing a Server Certificate, SG PKI ensures the validity of all subject information. This verification processes consists of the following key elements:

- Verify the organization’s existence and identity
- Verify that the organization is a registered holder or has exclusive control of the domain name to be included in the EV certificate.
- Verify the name and authority of the certificate requester.
- Verify that the certificate requester correctly signed the registration form (check validity of Digitally Signed Document).

The validation process is detailed in a checklist for each certificate type. [25][26][27][28]

4.2.2 Approval or rejection of certificate applications

Certificate type requested	Condition for approval
Server Certificate	1. Request formally correct and complete 2. Request submitted by authorized Registration Agent 3. Domain names within the range assigned to the requesting Registration Agent (as of 3.2.3) 4. Checklist for specific Validation Type a. DV [25] b. OV [26] c. EV [27]
Codesigning Certificate	1. Request formally correct and complete 2. Request submitted personally and valid 3. Checklist for Codesigning Certificates [28]

Table 9: Approval Process and Responsibilities for certificate requests

Requests that don't meet all of the requirements are either held pending to enable amendments or are rejected by the Registration Agents in case a request is clearly invalid.

SG PKI reserves the right to decline certificate requests without giving reasons.

SG PKI Root III and its subordinated CAs do not issue certificates containing a new gTLD under condsideration by ICANN.

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 the approval of the requests.

After receiving the registration form as well as the complete, accurate registration documentation, the time to approve certificate applications is five working days.

4.3 Certificate issuance

4.3.1 CA actions during certificate issuance

Certificate issuance by the SG Root CA III requires an individual authorized by the PKI Management Board to deliberately issue a direct command in order for the Root CA to perform a signing operation.

All CA's subordinated to SG Root CA III issue certificates on-line, i.e. once a valid request has been approved, the CA automatically issues the certificate asked for via the registration

application (CRW), except code signing certificates: they are handed to the requesters in person as these are required to present themselves in person for authentication (see 4.1.2).

4.3.2 Notification to subscriber by the CA of issuance of certificate

CA's subordinated to SG Root CA III do not notify the subscribers identified in the certificates. Where necessary the individual subscribers are informed by the Registration Agents acting on their behalf.

4.4 Certificate acceptance

4.4.1 Conduct constituting certificate acceptance

SG PKI doesn't require a formal acceptance of the certificates it issues. SG PKI assumes acceptance of the certificate if the subscriber doesn't notify the RA about a problem.

4.4.2 Publication of the certificate by the CA

Codesigning certificates issued under SG Root CA III are published in AdminDir [23], publicly accessible.

Server Certificates are not published.

4.4.3 Notification of certificate issuance by the CA to other entities

All other entities are not actively notified of certificate issuance by any of the CA's subordinated to SG Root CA III.

4.5 Key pair and certificate usage

4.5.1 Subscriber private key and certificate usage

Subscribers must use their private keys and certificates strictly as stipulated in section 1.4. and as defined in the Subscriber Agreement and in section 9.6.3

4.5.2 Relying party public key and certificate usage

When trusting and using public keys and certificates, the relying party of the server certificate and the code signing certificate is obliged to:

- Check the use purpose of the certificate.
- Check that the certificateis not tampered.
- Verify the validation of the certificate.

4.6 Certificate renewal

Certificate renewal is not supported by any of the CA's subordinated to SG Root CA III.

Certificates that must no longer be used – because they expire or their contents are no longer adequate – are re-keyed (see 4.7).

4.7 Certificate re-key

4.7.1 Circumstance for certificate re-key

Certificates of all types SHOULD be re-keyed in case:

- they are about to expire,
- they have been revoked,
- their contents (typically subscriber identifying data) are obsolete.

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.

4.7.3 Processing certificate re-keying requests

Registration Agents and CA process re-keying requests in the same way as requests for original certificates (see 4.1.1 through 4.2.1).

4.7.4 Notification of new certificate issuance to subscriber

CA's subordinated to SG Root CA III do not notify the subscribers identified in the re-keyed certificates. Where necessary the individual subscribers are informed by the Registration Agents acting on their behalf.

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).

4.7.6 Publication of the re-keyed certificate by the CA

Once Codesigining Certificates have been re-keyed, they are published through the processes used with the original certificates (see section 4.4.2), replacing these in the respective directories.

Server Certificates are not published.

4.7.7 Notification of certificate issuance by the CA to other entities

no stipulation

4.8 Certificate modification

CA's subordinated to SG Root CA III 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

SG PKI revokes a Subscriber certificate if one or more of the following occurs:

- The Subscriber 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;
- SG PKI obtains evidence that the Subscriber'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 and 6.1.6;
- 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 or Terms of Use Agreement;
- SG PKI is made aware of any circumstance indicating that use of a Fully-Qualified Domain Name or IP address in the Certificate is no longer legally permitted (e.g. a court or arbitrator has revoked a Domain Name Registrant's right to use the Domain Name, a relevant licensing or services agreement between the Domain Name Registrant and the Applicant has terminated, or the Domain Name Registrant has failed to renew the Domain Name);
- SG PKI is made aware of a material change in the information contained in the Certificate;
- 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 determines that any of the information appearing in the Certificate is inaccurate or misleading;
- SG PKI ceases operations for any reason 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;
- The technical content or format of the Certificate presents an unacceptable risk to Application Software Suppliers or Relying Parties (e.g. the CA/Browser Forum might determine that a deprecated cryptographic/signature algorithm or key size presents an unacceptable risk and that such Certificates should be revoked and replaced by CAs within a given period of time).

4.9.1.2 Reasons for Revoking a Subordinate CA Certificate

SG PKI revokes a Subordinate 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 and 6.1.6,
- 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
- The Issuing CA's or Subordinate 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;
- Revocation is required by the Issuing CA's Certificate Policy and/or Certification Practice Statement; or
- The technical content or format of the Certificate presents an unacceptable risk to Application Software Suppliers or Relying Parties (e.g. the CA/Browser Forum might determine that a deprecated cryptographic/signature algorithm or key size presents an unacceptable risk and that such Certificates should be revoked and replaced by CAs within a given period of time).

4.9.2 Who can request revocation

Requests for revoking certificates can be requested by:

- Subscribers.
- The Registration Agent having done the registration for the certificate in question.
- The administrative unit employing the subscriber.
- The PKI Security Officer.
- The PKI Manager.

Certificates may also be revoked on the basis of a judicial decision. The ensuing request in writing and adequately founded must be addressed to the PKI Manager as per 1.5.2..

4.9.3 Procedure for revocation request

The procedure for revoking certificates of any type is as follows:

- The Subscriber initiates the process and authenticates with a Registration Agent (as detailed in 3.4).
- The Registration Agent verifies requester's entitlement for launching the request. Provided the result is positive the Registration Agent approves the request and forwards it to the CA subordinated to SG Root CA III, that issued the certificate to be revoked.
- The mentioned CA processes the revocation request automatically and instantaneously. It then informs the Registration Agent on the completed revocation.

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).

4.9.5 Time within which CA must process the revocation request

All CA's subordinate to SG Root CA III revoke certificates without delay as soon as it receives approved requests from a Registration Agent.

SG PKI begins investigation of a Certificate Problem Report within twenty-four hours of receipt, and decide whether revocation or other appropriate action is warranted based on at least the following criteria:

1. The nature of the problem

2. The number of Certificate Problem Reports received about a particular Certificate or Subscriber

3. The entitiy making the complaint (for example, a complaint from a law enforcement official that a Web site is engaged in illegal activities dies carry more weight than a complaint from a consumer alleging that she didn't receive the goods she ordered)

4. Relevant legistaltion

4.9.6 Revocation checking requirement for relying parties

All relying parties must ensure they are in possession of a valid certificate status, provided by the OCSP service, or an actual CRL.

4.9.7 CRL issuance frequency

4.9.7.1 CRL issuance frequency for the Status of Subscriber Certificates

All CA's subordinated to SG Root CA III issue and publish updated CRLs usually every four hours during office hours (see 2.3) but at least once every seven days, and 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

SG Root CA III issues and publishes updated ARLs every year and within 24 hours after revoking a Subordinate CA Certificate. The value of the of the nextUpdate field is never more than twelve months beyond the value of the thisUpdate field.

4.9.8 Maximum latency for CRLs

CRLs updated by SG PKI published via LPAD Protocol in AdminDir [23] and via HTTP as specified in the CDP of the Subscriber Certificate with a maximum latency of twenty-four hours.

4.9.9 On-line revocation/status checking availability

The SG PKI provides an OCSP service confirming with RFC 2560. The certificate status database, used by the OCSP service, is updated every four hours during office hours.

OCSP responses are signed by a 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 are required to check the revocation status of the certificate to be validated, as required in 4.9.6. This includes the use of CRLs in accordance with the certification path validation procedure specified in RFC 5280 and/or RFC 2560 or OCSP.

4.9.11 Other forms of revocation advertisements available

No stipulation

4.9.12 Special requirements re key compromise

There aren’t any special requirements re key compromise in addition to the ones as per 4.7 and 4.9.3.

The compromise of the private key may have implications on the information protected with this key. The subscriber must decide how to deal with the affected information before deleting the compromised key.

4.9.13 Circumstances for suspension

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

4.9.14 Who can request suspension

Not applicable (see section 4.9.13).

4.9.15 Procedure for suspension request

Not applicable (see section 4.9.13).

4.9.16 Limits on suspension period

Not applicable (see section 4.9.13).

4.10 Certificate status services

4.10.1 Operational characteristics

Certificate status information is available via CRL or by requesting certificate status information from the OCSP responder.

The CRLs list the serial numbers of all revoked certificates issued by the CA which haven't expired yet.

4.10.2 Service availability

CRL and OCSP Responder are available 24x7

High-Priority Certificate Problem Reports can be submitted on the SG PKI Homepage 24x7 [24].

4.10.3 Optional features

No stipulation

4.11 End of subscription

End of subscription occurs after:

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

For reasons of legal compliance, the Swiss Government 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

SG PKI does not archive any private keys of Subscriber Certificates issued by SG PKI Root CA III and its Subordinate CAs.

4.12.1 Key escrow and recovery policy and practices

Not applicable

4.12.2 Session key encapsulation and recovery policy and practices

Not applicable

5 Management, Operational, and Physical Controls

5.1 Physical Security Controls

5.1.1 Site location and construction

SG PKI operates its certification infrastructure in an appropriately secured location of the FOITT.

5.1.2 Physical access

Physical access to the certification infrastructure is regulated in SG PKI's access control directive [7].

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

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

5.1.3 Power and air conditioning

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

An air condition system specifically built and run for the secured location ensures constant temperature and humidity control (7x24h.)

5.1.4 Water exposures

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

5.1.5 Fire prevention and protection

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

5.1.6 Media storage

Not applicable, data related to the certification infrastructure 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 disposes of a backup-site from where certification can be upheld in case of an emergency.

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

5.2 Procedural Controls

5.2.1 Trusted roles

To enable the necessary segregation of critical duties with 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 dual-role rule with security critical processes (see 5.2.2).

The trusted roles are:

- **PKI Director**
  The PKI Director represents SG PKI in the FOITT directorate. He is the primary responsible for SG PKI. His main task is to assure the correct operation of the infrastructure.
- **PKI Management Board**
  The PKI Management board consists of the PKI Operations Manager and the PKI Service & Design Manager. Its function is to combine the Strategic, Security and Operational view on the SG PKI. Its main tasks are reviewing and approving security- and certification policies.
  The PKI Management Board reports to the PKI Director.
- **PKI Operations Manager**
  The PKI Operations Manager is responsible to operate SG PKI's services. His tasks include participating in the strategic planning, maintaining relations with clients and providers.
  The PKI Operations Manager is responsible for the following SG PKI teams:
  - PKI Order Management
  - PKI Operating
- **PKI Service & Design Manager**
  The PKI Service & Design Manager is responsible for the strategic planning of SG PKI's services. His tasks include the strategic planning, maintaining relations with clients and providers.
  The PKI Service & Design Manager is responsible for the following SG PKI teams:
  - PKI Security Officers
  - PKI Engineering
- **PKI Engineering**
  PKI Engineering is responsible for the technical support and the improvement of SG PKI's services. PKI Engineering is also responsible for the architecture, the design and the implementation of PKI techniques. It permanently observes the technical developments in the market, ensures SG PKI possesses the latest software versions and has

these installed where appropriate.
PKI Engineering reports to the PKI Service & Design Manager

- **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 Officer is the only role entitled to access and read archives and analyzing activity logs.
  PKI Securitiy Officers report to the PKI Service & Design Manager
- **PKI Order Management**
  PKI Order Management is responsible for the publication of information supporting subscribers and third parties. It is also responsible for SG PKI's website http://www.pki.admin.ch and answers client's questions addressed to pki-info@bit.admin.ch
  PKI Order Management reports to the PKI Operations Manager.
- **PKI Operating**
  PKI Operating is responsible for running all services operated by SG PKI. In particular, its tasks are maintaining support contracts with suppliers, ensure the availability of the certification infrastructure and co-ordinate SG PKI's operational work.
  PKI Operating also maintains the applications and the network supporting registration, issuance and revocation for/of certificates and other services provided by SG PKI.
  PKI Operating reports to the PKI Operations Manager.
- **PKI Repository Officer**
  The Repository Officer is responsible for the operation and the availability of the repository in conformance with the respective SLA.
  The Repository Officer reports to PKI Operating
- **Auditor**
  The Auditor is an auditing company assigned by SG PKI. It conducts reviews at regular intervals of the conformance of the services delivered by SG PKI with this certificate policy and practice statement and SG PKI's detailed manuals and security policy.
  The Auditor is assigned by the PKI Management Board
- **Registration Agent**
  As described in 1.3.2.1

5.2.2 Number of individuals required per task

With the exception of the standard tasks performed by the Operating Team, security critical actions require two individuals having different roles (see 5.2.1) 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 and 5.2.2 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.

5.2.4 Roles requiring separation of duties

The PKI Management Board assigns roles to the different SG PKI employees, ensuring that no conflicts regarding the separation of duties arise, e.g. members of the Operating Team may never be PKI Security Officers and vice versa.

5.3 Personnel Controls

5.3.1 Qualifications, experience and clearance requirements

SG Root CA III and its subordinated CAs are operated by qualified and experienced specialists, employed by the Swiss federal administration. They are appointed for an indefinite period of time, and normally they are posted 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 Officer 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 identified by a Certificate of type "Klasse B" issued under the Swiss Government Root CA I [20] and Background Checks as specified in 5.3.2 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 [8].

5.3.3 Training requirements

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

5.3.4 Retraining frequency and requirements

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

Each SG PKI employee must 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 [9].

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, 5.3.2, 5.3.3 and 5.3.4).

5.3.8 Documentation supplied to personnel

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

- Certificate Policy and Certification Practice Statement of the SG Root CA III (this document)
- SG PKI security policy [10]
- SG PKI manual on operation and organization [11]
- Manuals of 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 requester, name(s) of person(s) approving (where applicable).

5.4.2 Frequency of processing log

Log files are checked as part of a daily verification as per SG PKI's operating manual 'periodic monitoring or functions and activities' [12].

5.4.3 Retention period for audit log

All log files are retained for at least eleven years.

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 Officer, Operating Team and Auditor 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 log accumulation system

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

5.4.7 Notification to event-causing subject

The Operating Team analyzes the log files daily and notifies the security officer and the members of 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 forseeable internal and external threats that could result in unauthorized access, disclosure, misuse, alteration, or destruction of any Certificate Data or Certificate Management Process

- Assesses the likelihood and potential damage of these threats, taking into consideration the sensitivity of the Certificate Data and Certificate Management Process

- Assesses the sufficiency of the policies, procedures, information systems, technology, and other arrangements that SG PKI has in place to counter such threats

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

5.5 Records Archival

5.5.1 Types of records archived

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

- Contractual agreements with clients.
- All certificates issued for Root CA III, subordinated 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.

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 has to be formally authorized by the PKI Managament 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 on base of the central date/time reference provided by FOITT.

5.5.6 Archive Collection System

All data to be archived is integrity protected by hash-values and collected in a specific data-base 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 the 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 SG Root CA III and all its subordinated CA's are backed up off-site in at least two backup tokens at all times. All data related to the issuance and maintenance of subscriber certificates is backed up daily as well.

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

5.7.3 Recovery procedures after key compromise

In case any of the subordinate CA's key should have been compromised or is suspected to be compromised, SG PKI Manager activates the predefined action plan. In particular, this comprises the following steps:

- Informing supervisory authorities
- Informing all subscribers concerned.
- Revoking all subscribers' certificates signed by the compromised key.
- Revoking the CA's certificate (by SG Root CA III) and publishing an updated ARL.
- Generating and certifying a new key pair for the CA.
- Issuing new certificates for the subscribers concerned.
- Informing software vendors supporting SG PKI CA certificates as trust anchors and providing them with the necessary updates.

If the key of SG Root CA III should have been compromised the above measures are carried out for all of the subordinated CA's and all their subscribers as well as for the SG Root CA III itself.

5.7.4 Business continuity capabilities after a disaster

There is an emergency facility available, capable of running SG PKI's SG Root CA III and its subordinated CAs with all necessary processes within seven days after a disaster.

5.8 CA or RA termination

In case SG PKI decides to terminate CA operation[2], it will inform the supervisory authorities and all subscribers at least 30 days in advance before it stops the certification activities in conjunction with SG Root CA III.

All valid certificates, including Root CA III and subordinated CA certificates, will be revoked

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

and a final CRL and ARL published on FOITTs website for a minimum of eleven years. The Root CA III key and the keys of the subordinated CAs including 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.

6 Technical Security Controls

6.1 Key pair generation and installation

6.1.1 Key pair generation

6.1.1.1 Root Key par 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 Staff member, a Qualified Auditor, a Notary and an independent Witness to witness the Root CA Key Pair Generation Ceremony. The Root CA Key Pair Generation Ceremony is documented, logged and videographically recorded.

6.1.1.2 Subordinate Key pair generation

Subordinate CA Key pairs are generated by following a Key Generation Script and have a PKI Security Officer, a PKI Operation 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.

6.1.1.3 Key Pair Generation location

All SG Root CA III and subordinated CAs key pairs are generated in HSMs conformant to FIPS 140-2 level 3 or EAL 4+ within the secured facilities of SG PKI (5.1.1.)

6.1.2 Private Key delivery to subscriber

As a standard, private keys to be certified by any of the Swiss Government PKI's CAs are generated on subscribers' premises and not submitted to the CA at all, private key delivery is thus not necessary.

If requested by the Applicant, SG PKI MAY generate key pairs on behalf of the Applicant as they lack the necessary technical means. Once the corresponding certificates have been issued SG PKI assembles key pairs and certificates in password-protected PKCS#12 files and sends these to the requesting Registration Agents. The passwords are sent by separate mails or handed over in person.

For EV Codesigning Certificates, the key pair is generated on a FIPS 140-2 level 3 conformant Smartcard as specified in A006 [23]

6.1.3 Public key delivery to certificate issuer

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

6.1.4 CA public key delivery to relying parties

SG PKI publishes the certificates of SG Root CA III and its subordinated CA's

- in AdminDir [4],
- on its Website [24]

6.1.5 Key sizes

SG Root CA III and all of its subordinated CA's use RSA keys of 4096 bits in size.

Subscribers to the subordinated CA's use RSA keys of 2048 bits in size.

6.1.6 Public key parameters generation and quality checking

All CA keys are generated on HSMs conformant to FIPS 140-2 level 3 or EAL 4+ and following the recommendations of NIST SP 800-89.

6.1.7 Key usage purposes

The key usage flags are populated in all SG Root CA III, CA and subscriber certificates issued.

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

SG Root CA III keys are not used to sign certificates except in the following states:

- Self-signed certificates to represent the Root CA itself
- Certificates for Suboardinate CAs and Cross Certificates
- Certificates for Infrastructure purposes

Subscribers are bound by the general agreement 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) conformant to FIPS 140-2 level 3 or EAL 4+ (see also section 6.1).

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

All activities on HSMs require the presence of at least two authorized SG PKI staff members.

In particular these are the generation, backup and recovery, activation and deactivation of the keys and the exchange of HSMs.

6.2.3 Private key escrow

Not applicable

6.2.4 Private key backup

SG Root CA III and subordinate CAs private keys are backed up in at least two encrypted backup tokens stored in separate, secure locations off-site. For recovering backup tokens at least two authorized SG PKI staff members are required.

6.2.5 Private key archival

There aren't any private keys archived.

6.2.6 Private key transfer into or from a cryptographic module

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

6.2.7 Private key storage on cryptographic module

SG Root CA III and subordinated CA's private keys are stored encrypted within the HSMs and are decrypted only when activated.

Subscribers' keys are stored encrypted in the respective soft-tokens and password protected in the workstations where they are used.

6.2.8 Method of activating private key

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

6.2.9 Method of deactivating private key

SG Root CA III and subordinated CA's private keys are deactivated by PKI Security Officers. The deactivation process requires two SG PKI staff members authorized for the task beside a PKI Security Officer.

For Subscriber Certificates, the subscriber is solely responsible for the deactivation of private key.

6.2.10 Method of destroying private key

SG Root CA III and subordinated CA's private keys are destroyed in that the hard-disks of the HSMs concerned as well as the HSMs' backup tokens are shredded and disposed of in compliance with SG PKI's formal concept for waste disposal - the 'BIT Entsorgungskonzept'.[29] The process requires at least two SG PKI staff members authorized for the task.

For Subscriber Certificates, the subscriber is solely responsible for the destruction of private key material.

6.2.11 Cryptographic module capabilities

For ratings and capabilities refer to section 6.2.1.

6.3 Other aspects of key pair management

6.3.1 Public key archival

All public keys – Root CA II's, subordinated CA's 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

Validity periods are:

- 25 years for SG Root CA III.
- 15 years for all subordinated CAs
- A maximum of 36 months for all Subscriber Certificates
    - 36 months for Server Certificates
    - 12 months for EV Server Certificates
    - 36 months for Codesigning Certificates
    - 12 months for EV Codesigning Certificates

6.4 Activation data

6.4.1 Activation data generation and installation

Supervised by a PKI Security Officer, activation data for the HSMs storing SG Root CA III and subordinated CA keys are generated individually by the authorized SG PKI staff members. The passphrases and parameters are then entered as advised by the HSM's provider.

6.4.2 Activation data protection

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

Subscribers must not write down certificate token passwords.

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 [10]

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

6.8 Time-stamping

SG PKI uses a qualified time-stamping service supporting electronic signing under the SG PKI Root CA I. SG PKI operational rules apply likewise for the time-stamping service, for details see the time stamping authority's policy [13].

All SG PKI Systems are time synchronized by using NTP, referring the time source provided by FOITT.

7 Certificate, CRL and OCSP Profiles

All certificates and CRLs issued by SG Root CA III and each of the subordinated CA's conform to the technical and operational requirements specified by the Federal law on the certification services supporting electronic signatures ZertES [14] article 3.4,

7.1 Certificate profile

7.1.1 Version number(s)

Certificates issued by any of the CA's subordinated to SG Root CA III are of version 2 in accordance with recommendation X.509 v3.

7.1.2 Certificate extensions

7.1.2.1 Root CA Certificate

Full specifications of all Root CA Certificates are listed in [30]

Swiss Government Root CA III Certificate Extensions		
authorityKeyIdentifier		
extnId	2.5.29.35	DN + Cert Serial
extnValue	160 bit	OCTET STRING, 160 bit SHA1 of BIT STRING
subjectKeyIdentifier		
extnId	2.5.29.14	
extnValue	160 bit	OCTET STRING, 160 bit SHA1 of BIT STRING
keyUsage		
extnId	2.5.29.15	
critical	TRUE	BOOLEAN
extnValue	'000001100'B	RFC 5280
digitalSignature	0	
nonRepudiation	0	
keyEncipherment	0	
dataEncipherment	0	
keyAgreement	0	
keyCertSign	1	
cRLSign	1	
encipherOnly	0	
decipherOnly	0	
certificatePolicies	NOT SET	

extnId		
extnValue		
crlDistributionPoints	NOT SET	
extnId		
extnValue		
basicConstraints		
extnId	2.5.29.19	
critical	TRUE	BOOLEAN
extnValue	cA TRUE	BOOLEAN

7.1.2.2 Subordinate CA Certificates

Full specifications of all Subordinate CA Certificates are listed in [30]

7.1.2.2.1 Swiss Government Public Trust Standard CA 02 Extension

Swiss Government Public Trust Standard CA 02 Extension		
authorityKeyIdentifier		
extnId	2.5.29.35,	DN +Cert Serial
extnValue	…..,	OCTET STRING, 160 bit SHA1 ofBIT STRING
subjectKeyIdentifier		
extnId	2.5.29.14	
extnValue	…..,	OCTET STRING, 160 bit SHA1 of self subjectPublicKey BIT STRING
keyUsage		
extnId	2.5.29.15,	
critical	TRUE,	BOOLEAN
extnValue	‘000001100,	certSign, crlSign
digitalSignature	0	
nonRepudiation	0	
keyEncipherment	0	
dataEncipherment	0	
keyAgreement	0	
keyCertSign	1	
	1	

cRLSign		
encipherOnly	0	
decipherOnly	0	
certificatePolicies		
extnId	2.5.29.32,	
critical	TRUE	BR 1.3.3 Chap. 7.1.2.2 a.
extnValue	2.16.756.1.17.3.61.1,	
extnId	1.3.6.1.5.5.7.2.1,	
extnValue	http://www.pki.admin.ch/cps/CPS_2_16_756_1_17_3_61_0.pdf,	IA5String, cps
extnId	1.3.6.1.5.5.7.2.2,	
extnValue	Reliance on the SG Root CA III Certificate by any party assumes acceptance of the then applicable standard terms and conditions of use and the SG Root CA III CPS,	VisibleString, id-qt-unotice RFC 5280
basicConstraints		
extnId	2.5.29.19,	
critical	TRUE,	BOOLEAN
extnValue	cA TRUE,	BOOLEAN
pathLenConstraint	0 ,	INTEGER, no child CA
crlDistributionPoints		
extnId	2.5.29.31,	
extnValue	http://www.pki.admin.ch/crl/RootCAIII.crl ldap://admindir.admin.ch:389/cn=Swiss Government Root CA III,ou=Certification Authorities,ou=Services,o=Admin,c=CH,	uri IA5String ldap uri IA5String CA CDPs
authorityInfoAccess		SEQUENCE
extnId	1.3.6.1.5.5.7.1.1,	OCTET STRING
extnValue	SEQUENCE OF	OCTET STRING
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.2,	id-ad-caIssuers
accessLocation	http://www.pki.admin.ch/aia/RootCAIII.crt	uri IA5String
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.1,	id-ad-ocsp
accessLocation	http://www.pki.admin.ch/aia/ocsp ,	uri IA5String

7.1.2.2.2 Swiss Government Public Trust EV CA 02 Extensions

Swiss Government Public Trust EV CA 02 Extensions		
authorityKeyIdentifier		
extnId	2.5.29.35,	DN +Cert Serial
extnValue	…...,	OCTET STRING, 160 bit SHA1 of BIT STRING
subjectKeyIdentifier		
extnId	2.5.29.14	
extnValue	…...,	OCTET STRING, 160 bit SHA1 of self subjectPublicKey BIT STRING
keyUsage		
extnId	2.5.29.15,	
critical	TRUE,	BOOLEAN
extnValue	‘000001100,	certSign, crlSign
digitalSignature	0	
nonRepudiation	0	
keyEncipherment	0	
dataEncipherment	0	
keyAgreement	0	
keyCertSign	1	
cRLSign	1	
encipherOnly	0	
decipherOnly	0	
certificatePolicies		
extnId	2.5.29.32,	anyPolicy
extnValue	2.16.756.1.17.3.61.2,	
extnId	1.3.6.1.5.5.7.2.2,	
extnValue	Reliance on the SG Root CA III Certificate by any party assumes acceptance of the then applicable standard terms and conditions of use and the SG Root CA III CPS,	VisibleString, id-qt-unotice RFC 3280

extnId	1.3.6.1.5.5.7.2.1,	
extnValue	http://www.pki.admin.ch/cps/CPS_2_16_756_1_17_3_61_0.pdf,	IA5String, cps
basicConstraints		
extnId	2.5.29.19,	
critical	TRUE,	BOOLEAN
extnValue	cA TRUE,	BOOLEAN
pathLenConstraint	0 ,	INTEGER, no child CA
crlDistributionPoints		
extnId	2.5.29.31,	
extnValue	http://www.pki.admin.ch/crl/RootCAIII.crl ldap://admindir.admin.ch:389/cn=Swiss Government Root CA III,ou=Certification Authorities,ou=Services,o=Admin,c=CH,	uri IA5String ldap uri IA5String CA CDPs
authorityInfoAccess		SEQUENCE
extnId	1.3.6.1.5.5.7.1.1,	OCTET STRING
extnValue	SEQUENCE OF	OCTET STRING
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.2,	id-ad-caIssuers
accessLocation	http://www.pki.admin.ch/aia/RootCAIII.crt	uri IA5String
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.1,	id-ad-ocsp
accessLocation	http://www.pki.admin.ch/aia/ocsp ,	uri IA5String

7.1.2.2.3 Swiss Government Public Trust Code Signing Standard CA 02 Extensions

Swiss Government Public Trust Code Signing Standard CA 02 Extensions		
authorityKeyIdentifier		
extnId	2.5.29.35,	DN +Cert Serial
extnValue	…..,	OCTET STRING, 160 bit SHA1 ofBIT STRING
subjectKeyIdentifier		
extnId	2.5.29.14	
extnValue	…..,	OCTET STRING, 160 bit SHA1 of self subjectPublicKey BIT STRING
keyUsage		
extnId	2.5.29.15,	

critical	TRUE,	BOOLEAN
extnValue	‘000001100,	certSign, crlSign
digitalSignature	0	
nonRepudiation	0	
keyEncipherment	0	
dataEncipherment	0	
keyAgreement	0	
keyCertSign	1	
cRLSign	1	
encipherOnly	0	
decipherOnly	0	
certificatePolicies		
extnId	2.5.29.32,	
critical	TRUE	BR 1.3.3 Chap. 7.1.2.2 a.
extnValue	2.16.756.1.17.3.61.3,	
extnId	1.3.6.1.5.5.7.2.1,	
extnValue	http://www.pki.admin.ch/cps/CPS_2_16_756_1_17_3_61_0.pdf,	IA5String, cps
extnId	1.3.6.1.5.5.7.2.2,	
extnValue	Reliance on the SG Root CA III Certificate by any party assumes acceptance of the applicable standard terms and conditions of use and the SG Root CA III CPS	VisibleString, id-qt-unotice RFC 5280
basicConstraints		
extnId	2.5.29.19,	
critical	TRUE,	BOOLEAN
extnValue	cA TRUE,	BOOLEAN
pathLenConstraint	0 ,	INTEGER, no child CA
crlDistributionPoints		
extnId	2.5.29.31,	

extnValue	http://www.pki.admin.ch/crl/RootCAIII.crl ldap://admindir.admin.ch:389/cn=Swiss Government Root CA III, ou=Certification Authorities,ou=Services,o=Admin,c=CH,	uri IA5String ldap uri IA5String CA CDPs
authorityInfoAccess		SEQUENCE
extnId	1.3.6.1.5.5.7.1.1,	OCTET STRING
extnValue	SEQUENCE OF	OCTET STRING
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.2,	id-ad-caIssuers
accessLocation	http://www.pki.admin.ch/aia/RootCAIII.crt	uri IA5String
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.1,	id-ad-ocsp
accessLocation	http://www.pki.admin.ch/aia/ocsp ,	uri IA5String

7.1.2.2.4 Swiss Government Public Trust Code Signing EV CA 02 Extensions

Swiss Government Public Trust Code Signing EV CA 02 Extensions		
authorityKeyIdentifier		
extnId	2.5.29.35,	DN +Cert Serial
extnValue	…..,	OCTET STRING, 160 bit SHA1 of BIT STRING
subjectKeyIdentifier		
extnId	2.5.29.14	
extnValue	…..,	OCTET STRING, 160 bit SHA1 of self subjectPublicKey BIT STRING
keyUsage		
extnId	2.5.29.15,	
critical	TRUE,	BOOLEAN
extnValue	‘000001100,	certSign, crlSign
digitalSignature	0	
nonRepudiation	0	

keyEncipherment	0	
dataEncipherment	0	
keyAgreement	0	
keyCertSign	**1**	
cRLSign	**1**	
encipherOnly	0	
decipherOnly	0	
certificatePolicies		
extnId	2.5.29.32,	anyPolicy
extnValue	2.16.756.1.17.3.61.4,	
extnId	1.3.6.1.5.5.7.2.2,	
extnValue	Reliance on the SG Root CA III Certificate by any party assumes acceptance of the applicable standard terms and conditions of use and the SG Root CA III CPS	VisibleString, id-qt-unotice RFC 3280
extnId	1.3.6.1.5.5.7.2.1,	
extnValue	http://www.pki.admin.ch/cps/CPS_2_16_756_1_17_3_61_0.pdf,	IA5String, cps
basicConstraints		
extnId	2.5.29.19,	
critical	TRUE,	BOOLEAN
extnValue	cA TRUE,	BOOLEAN
pathLenConstraint	0 ,	INTEGER, no child CA
crlDistributionPoints		
extnId	2.5.29.31,	
extnValue	http://www.pki.admin.ch/crl/RootCAIII.crl ldap://admindir.admin.ch:389/cn=Swiss Government Root CA III,ou=Certification Authorities,ou=Services,o=Admin,c=CH,	uri IA5String ldap uri IA5String CA CDPs
authorityInfoAccess		SEQUENCE
extnId	1.3.6.1.5.5.7.1.1,	OCTET STRING
extnValue	SEQUENCE OF	OCTET STRING

accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.2,	id-ad-caIssuers
accessLocation	http://www.pki.admin.ch/aia/RootCAIII.crt	uri IA5String
accessDescription	SEQUENCE	
accessMethod	1.3.6.1.5.5.7.48.1,	id-ad-ocsp
accessLocation	http://www.pki.admin.ch/aia/ocsp,	uri IA5String

7.1.2.3 Subscriber Certificates

Full specifications of all Subscriber Certificates are listed in [30]

7.1.2.4 All Certificates

SG PKI Root CA III and its subordinate CAs do not issue certificates with:

- Extensions that do not apply in the context of the public Internet
- Semantics that, if included, will mislead a Relying Party about the certificate information verified by SG PKI

7.1.3 Algorithm object identifiers

There are two algorithms used in conjunction with 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

SG Root CA III and the subordinated CAs, subscribers and SSL subscribers identifications in the certificates (as issuer and/or subject) are shown in an annex document (“CA Layout and Policies”) [30].

7.1.5 Name constraints

Not implemented.

7.1.6 Certificate policy object identifier

OID of the current document: **2.16.756.1.17.3.61.0**

A complete list of all Swiss Government PKI issued Object identifiers is listed in the annexed document [31]

7.1.7 Usage of policy constraints extension

Not implemented.

7.1.8 Policy qualifiers syntax and semantics

Not implemented.

7.1.9 Processing semantics for the critical certificate policies extension

PKI client applications must process extensions marked as critical.

7.2 CRL profile

7.2.1 Version number(s)

CRLs generated by any of the CA's subordinated to SG Root CA III are of version 2 in accordance with recommendation X.509 v3 and IETF PKIX RFC 5280.

7.2.2 CRL and CRL entry extensions

CRL and CRL entry extensions used with SG Root CA III's and subordinate CAs' certificates are:

CRL Extension	**Objective**
CRL number	No. of CRL (CRLs are sequentially numbered).
CRL Entry Extension	
Reason Code (optional)	Identifies actual reason for revoking certificate.
Invalidity Date	Indicates known or suspected date a key was compromised.

Table 10: CRL and CRL entry extensions

7.3 OCSP profile

SG PKI offers an OCSP service for relying parties to retrieve information about the status of certificates. The OCSP responder is implemented in accordance with RFC 2560.

7.3.1 Version Number(s)

The OCSP responder implements OCSP Version 1, as defined by RFC 2560.

7.3.2 OCSP Extensions

No stipulation.

8 Compliance Audit and other Assessments

8.1 Frequency or circumstances of assessment

SG PKI Root CA III and each of the subordinate CA's are subject to a verification of their compliance with the requirements of this CP/CPS at least yearly. These audits are done by the Auditor (see 5.2.1).

Additionally, as SG Root CA III and all of the subordinate CA's are operated in the identical environment and subject to the identical security requirements as Swiss Government Root CA I and its subordinated qualified/enhanced CAs, the yearly recertification of the qualified CAs by the Swiss Certification Body essentially covers operation of SG Root CA III and it's subordinate CA's as well.

8.2 Identity/qualifications of assessor

The assessor assigned by FOITT is an independent company carrying out audits in accordance with the statutory and regulatory provisions.

The assessor must be accredited by the Swiss Accreditation Service to perform the specific audits.

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

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 to track the necessary actions and report to the PKI Management Board the actual status of completion.

8.6 Communication of results

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

8.7 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.

9 Other Business and Legal Matters

9.1 Fees

SG PKI's costs for running the certification services basing on SG Root CA III and all subordinated CA's 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 (Registration Agents registering and supporting applicants, etc.) are covered by the administrative units employing the Registration Agents.

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

9.2 Financial responsibility

9.2.1 Insurance coverage

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

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

9.2.2 Other assets

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

9.2.3 Insurance or warranty coverage for end-entities

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

9.3 Confidentiality of business information

9.3.1 Scope of confidential information

The following data is regarded as confidential and treated accordingly:

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

9.3.2 Information not within the scope of confidential information

Explicitly not within the scope of confidential information are:

- All data on subscribers shown in certificates and CRLs are not confidential; these are usually published formally (see section 1.6.3).
- SG PKI documents intended for subscribers, relying parties and third parties, e.g. this CP/CPS.

9.3.3 Responsibility to protect confidential information

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

9.4 Privacy of personal information

All SG PKI staff and Registration Agents must observe the requirements stipulated in the Swiss laws on data protection where applicable.

All SG PKI staff and Registration Agents may collect only subscriber data necessary for registration and certification and use it for these purposes exclusively. In particular, they must not use subscriber data for any commercial purposes.

9.5 Intellectual property rights

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

- Certificate Policy and Certification Practice Statement of SG Root CA III (this document).
- Directives for registration for certificates.
- Contracts and other agreements concluded between SG PKI and its clients
- Certificates issued by Swiss Government Root CA III.
- Certificates issued by subordinated CAs to Swiss Government Root CA III

The reproduction, presentation (inclusive of 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 don't 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 certificates in compliance with the current CP/CPS.

9.6.2 RA representations and warranties

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

9.6.3 Subscriber representations and warranties

Subscribers commit to acquire, use and maintain their private keys, certificates and certificate tokens in compliance with the current CP/CPS and have to accept the SG PKI Subsciber Agreement [7]

9.6.4 Relying party representations and warranties

Relying parties must 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 Swiss Government PKI limitation of liability

The liability of the Swiss Government PKI is limited to the extent permitted by applicable law.

In particular the Swiss Government PKI is not liable for:

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

9.8.2 Registration Agent's limitation of liability

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

9.8.3 Subscriber limitation of liability

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

9.9 Indemnities

SG PKI cannot give explicit information on indemnities in addition to the statements in sections 9.6 through 9.8.

9.10 Term and termination

9.10.1 Term

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

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 a Digitally Signed Document 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

9.12.3 Circumstances under wich OID must be changed

No stipulation

9.13 Dispute resolution procedures

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

9.14 Governing law

This CP/CPS is subject to the applicable Swiss federal laws, particularly the law on data protection DSG [15]. The only place of jurisdiction is Berne.

9.15 Compliance with applicable law

No stipulation.

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.

Annexes

9.18 Annex A – References

[1]	RFC3647, Request for Comments: 3647, Internet X.509 Public Key Infrastructure: Certificate Policy and Certification Practices Framework, Chokhani, et al, November 2003. https://www.ietf.org/rfc/rfc3647.txt
[2]	SR 172.010 Federal law on the Organization of Government and Administration (RVOG) http://www.admin.ch/ch/d/sr/c172_010.html
[3]	SR 172.215.1 Regulation on the Organization of the Federal Department of Finances (OV-EFD) http://www.admin.ch/ch/d/sr/c172_215_1.html
[4]	Technical directive I006 'Structure of the AdminDir' by the Federal Strategy Unit for IT (FSUIT) http://www.isb.admin.ch/themen/standards/alle/03149/index.html?lang=de
[5]	SG PKI Subscriber Agreement
[6]	Minutes of SG Root CA III root ceremony (not publicly available)
[7]	SG PKI access control directive (not publicly available)
[8]	Ordinance on Security Checks for Persons (OSCP) https://www.admin.ch/opc/de/classified-compilation/20092321/index.html
[9]	SR 170.32 Federal Act on the Responsibility of the Swiss Confederation, the Members of its Official Bodies and their Officers http://www.admin.ch/ch/d/sr/17.html#170.32
[10]	SG PKI security policy (not publicly available
[11]	SG PKI manual on operation and organization (not publicly available
[12]	SG PKI's operating manual 'Periodic Monitoring or Functions and Activities'(not publicly available
[13]	Policy of Time Stamping Authority
[14]	SR 943.03 Swiss Federal law on the certification services supporting electronic signatures ZertES, 19 December 2003 http://www.admin.ch/ch/d/sr/c943_03.html
[15]	SR 235.1 Swiss Federal law on data protection DSG http://www.admin.ch/ch/d/sr/c235_1.html
[16]	ETSI TS 102 280 V1.1.1 (2004-03), Technical Specification, X.509 V.3 Certificate Profile forCertificates Issued to Natural Persons. See also Draft ETSI EN 319 412-2 V2.0.15 (2015-06) Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons
[17]	Guidelines for the Issuance and Management of Extended Validation (EV) Certificates https://cabforum.org/extended-validation/

[18]	Guidelines for the Issuance and Management of Extended Validation (EV) Code signing Certificates https://cabforum.org/current-work/code-signing-working-group/
[19]	Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates https://cabforum.org/baseline-requirements-documents/
[20]	Certificate Type “Klasse B” of Swiss Government Root CA I: https://www.bit.admin.ch/adminpki/00240/00367/
[21]	Swiss Business Identitiy Registry - UID Register: https://www.uid.admin.ch
[22]	Swiss Federal Directory – Staatskalender: https://www.staatskalender.admin.ch/welcome.html?dn=top&localeString=Deutsch#
[23]	Swiss Federal IT Steering Unit Smartcard Standard - A006: https://www.isb.admin.ch/isb/de/home/ikt-vorgaben/standards/a006-smartcard.html
[24]	Swiss Government PKI Homepage: www.pki.admin.ch
[25]	Pre-Issuance checklist for DV Server Certificates (not publicly available)
[26]	Pre-Issuance checklist for OV Server Certificates (not publicly available)
[27]	Pre-Issuance checklist for EV Server Certificates (not publicly available)
[28]	Pre-Issuance checklist for Codesigning Certificates (not publicly available)
[29]	FOITT Waste Management Concept – BIT Entsorgungskonzept (not publicly available)
[30]	Swiss Government PKI CA Layout and Policies
[31]	Swiss Government PKI Object Identifiers

Table 11: References