

End-user Certificates

Swiss Government PKI - Root CA II

Certificate Policy and Certification Practice Statement (CP/CPS)

Document OID: 2.16.756.1.17.3.21.1

Project Name: Swiss Government Root CA II

Project Number: -

Version: V1.0

Status At Work Verify Approved

Involved Persons	
Authors:	Jürgen Weber, Jürg Spörndli, Karolina Kohout
Approval:	Responsible Swiss Government PKI
User:	Subscribers, Employees Swiss Government PKI, Auditors, Third Parties
For information / knowledge:	-

Changes			
Date	Version	Who	Description
2011/10/19	0.1a	J. Spörndli	1 st Draft on the basis of the draft CP/CPS for Root CA I and the CP/CPS 'Swiss Government Regular CA 01', V 1.1
2011/12/22	0.1b	J. Spörndli	Updated per feedback P. Joye + R. Jusufi
2012/11/30	0.1c	J. Spörndli	Updated per the input D. Stich/J. Weber/A. Zürcher
2013/02/20	0.1d	J. Weber	Updated
2013/03/20	0.1e	J. Spörndli	Updated per further input J. Weber and D. Stich, in particular on processes
2013/03/26	0.1e	J. Weber	Updates of 0.1e approved. Additional updates included
2013/05/03	0.1f	J. Spörndli	Updated on basis of walkthrough of 2013/04/25 by J. Weber and J. Spörndli
2013/05/15	0.1g	J. Weber	Updates of 0.1f approved. Additional updates included
2014/04/01	0.1h	R. Leu	Added documentation for the OCSP service.
2014/04/03	0.1h	J. Weber	Updates of 0.1h approved
2014/06/05	0.1i	J. Weber	Added additional validation procedures for Extended Validation SSL certificates. Minor other changes
2014/06/12	0.1iRel2	J. Weber	Update for Extended Validation SSL Certificates
2014/07/11	0.1iRel3	J. Weber	Adjustments to the CA/Browser Forum Baseline Requirements
2014/07/23	0.1iRel4	J. Weber	Adjustments to the CA/Browser Forum EV Guidelines

Management summary

The current CP/CPS describes in sufficient detail how SG Root CA II and its subordinate CAs are operated, what certificates they issue, for what purposes and how these are to be handled throughout their lifetime. The essential points made are:

- Swiss Government Root CA II is operated by Swiss Government PKI (SG PKI) in the FOITT to act as the trust basis for its subordinated CAs (presently 3 different CA's) issuing SSL servers certificates or end user certificates to be used primarily for authentication, encryption and signature in the message and data exchange within the federal and cantonal/communal administrations. The level of trust is moderate (as opposed to the qualified and advanced certificates issued by CAs subordinated to Swiss Government Root CA I). Most of the certificates are issued and used as soft tokens, except from Code Signing Certificates with Extended Validation, which are issued and used as hard tokens.
- Swiss Government EV SSL CA 01 only issues certificates after performing Extended Validation according to the guidelines of CA/Browser Forum. Certificates are issued either for servers to ensure authenticity and privacy of the data accessed, or for the purpose of signing code.
- Swiss Government SSL CA 01 issues certificates after performing organization validation. Certificates are issued for servers to ensure authenticity and privacy of the data accessed. In addition this CA issues certificates for the purpose of code signing which do not require Extended Validation.
- Swiss Government Regular CA 01 certificates are issued to persons/organizations within the administration having a need to access protected data or to encrypt their e-mail exchange. Persons/organizations that need regular access to data or services provided by the federal authorities of Switzerland or related parties may also acquire certificates.
- To ensure the appropriate level of trust, a strict registration process is followed: Requests for certificates are only accepted if the requester's identity has been verified and confirmed by a matching entry in AdminDir. Each request must be then approved by Registration Agents that have been authorized through the an authorized representative of the employing department, office, canton or according instance. Requests for server certificates are accepted by the CA only if the Registration Agent submitting the request has been authorized by the owner of the domain name(s) to be certified.
- Certificates issued are valid for up to three years, then the certificate holders has to request a new certificate with new key pairs and pass the registration process again. In case certificates have been illegitimately issued or are no longer appropriate, the holders, the responsible Registration Agents or Swiss Government PKI staff must initiate the revocation process to invalidate the certificates concerned.
- Encryption certificates are published by the CA to the appropriate directories (e.g. AdminDir) enabling e-mail originators to find public encryption keys of the addressees.
- The high security of CA operation and certificate issuance is additionally ensured by:employing specialized and permanently re-trained staff for the purpose, operating the exposed hardware in specially protected, permanently supervised environments and regular audits.
- FDF is liable for potential damages caused by FOITT's operating the CA, limited to the extent permitted by the applicable laws. Registration Agents and Subscribers ensure they are adequately covered against damages they may cause by mishandling or misusing certificates, Registration Agents' liability is limited by a framework contract with Swiss Government PKI.

Table of Contents

1	Introduction	9
1.1	Overview	10
1.2	Document name and identification	12
1.3	PKI participants	13
1.3.1	Certification authorities	13
1.3.2	Registration authorities	15
1.3.3	Subscribers	15
1.3.4	Relying parties	16
1.3.5	Other participants	16
1.4	Certificate Usage	16
1.4.1	Appropriate certificate uses	16
1.4.2	Prohibited certificate uses	18
1.5	Policy administration	18
1.5.1	Organization administering the document	18
1.5.2	Contact person	18
1.5.3	Person determining CPS suitability for the policy	18
1.5.4	CPS approval procedures	18
1.6	Definitions and acronyms	18
2	Publication and Repository Responsibilities	21
2.1	Repositories	21
2.2	Publication of certification information	21
2.3	Time or frequency of publication	21
2.4	Access controls on repositories	22
3	Identification and Authentication	23
3.1	Naming	23
3.1.1	Types of names	23
3.1.2	Need for names to be meaningful	23
3.1.3	Anonymity or pseudonymity of subscribers	23
3.1.4	Rules for interpreting various name forms	23
3.1.5	Uniqueness of names	23
3.1.6	Recognition, authentication, and role of trademarks	24
3.2	Initial identity validation	24
3.2.1	Method to prove possession of private key	24
3.2.2	Authentication of organization identity	24
3.2.3	Authentication of individual identity	24
3.2.4	Non-verified subscriber information	25
3.2.5	Validation of authority	25
3.2.6	Criteria for interoperation	25
3.3	Identification and authentication for re-key requests	26
3.3.1	Identification and authentication for routine re-key	26
3.3.2	Identification and authentication for re-key after revocation	26
3.4	Identification and authentication for revocation request	26
4	Certificate Life-Cycle Operational Requirements	27
4.1	Certificate application	27
4.1.1	Who may submit a certificate application	27
4.1.2	Enrollment process and responsibilities	27
4.2	Certificate application processing	30
4.2.1	Performing identification and authentication functions	30
4.2.2	Approval or rejection of certificate applications	30
4.2.3	Time to process certificate applications	31
4.3	Certificate issuance	32
4.3.1	CA actions during certificate issuance	32

4.3.2	Notification to subscriber by the CA of issuance of certificate.....	32
4.4	Certificate acceptance	32
4.4.1	Conduct constituting certificate acceptance	32
4.4.2	Publication of the certificate by the CA	32
4.4.3	Notification of certificate issuance by the CA to other entities.....	32
4.5	Key pair and certificate security rules	32
4.5.1	Subscriber private key and certificate usage	32
4.5.2	Relying party public key and certificate usage.....	33
4.6	Certificate renewal.....	33
4.7	Certificate re-key	33
4.7.1	Circumstance for certificate re-key	33
4.7.2	Who may request certification of a new public key	33
4.7.3	Processing certificate re-keying requests	34
4.7.4	Notification of new certificate issuance to subscriber.....	34
4.7.5	Conduct constituting acceptance of a re-keyed certificate	34
4.7.6	Publication of the re-keyed certificate by the CA	34
4.7.7	Notification of certificate issuance by the CA to other entities.....	34
4.8	Certificate modification	34
4.9	Certificate revocation and suspension	34
4.9.1	Circumstances for revocation	34
4.9.2	Who can request revocation.....	35
4.9.3	Procedure for revocation request	35
4.9.4	Revocation request grace period.....	35
4.9.5	Time within which CA must process the revocation request	35
4.9.6	Revocation checking requirement for relying parties	35
4.9.7	CRL issuance frequency	36
4.9.8	Maximum latency for CRLs	36
4.9.9	On-line revocation/status checking availability	36
4.9.10	On-line revocation checking requirements	36
4.9.11	Other forms of revocation advertisements available	36
4.9.12	Special requirements re key compromise.....	36
4.9.13	Circumstances for suspension	37
4.9.14	Who can request suspension	37
4.9.15	Procedure for suspension request.....	37
4.9.16	Limits on suspension period.....	37
4.10	Certificate status services	37
4.10.1	Operational characteristics.....	37
4.10.2	Service availability.....	37
4.10.3	Optional features.....	37
4.11	End of subscription	37
4.12	Key escrow and recovery.....	38
4.12.1	Key escrow and recovery policy and practices	38
4.12.2	Session key encapsulation and recovery policy and practices	38
5	Management, Operational, and Physical Controls.....	39
5.1	Physical Controls	39
5.1.1	Site location and construction	39
5.1.2	Physical access	39
5.1.3	Power and air conditioning	39
5.1.4	Water exposures.....	39
5.1.5	Fire prevention and protection.....	39
5.1.6	Media storage	39
5.1.7	Waste disposal.....	40
5.1.8	Off-site backup.....	40
5.2	Procedural Controls and System Access Management	40
5.2.1	Trusted roles	40
5.2.2	Number of persons required per task	41
5.2.3	Identification and authentication for each role	41

5.2.4	Roles requiring separation of duties	41
5.3	Personnel Controls	42
5.3.1	Qualifications, experience and clearance requirements	42
5.3.2	Background check procedures	42
5.3.3	Training requirements	42
5.3.4	Retraining frequency and requirements.....	42
5.3.5	Job rotation frequency and sequence	42
5.3.6	Sanctions for unauthorized actions	42
5.3.7	Independent contractor requirements.....	42
5.3.8	Documentation supplied to personnel	43
5.4	Audit Logging Procedures.....	43
5.4.1	Types of events recorded.....	43
5.4.2	Frequency of processing log	43
5.4.3	Retention period for audit log	43
5.4.4	Protection of audit log	43
5.4.5	Audit log backup procedures.....	43
5.4.6	Audit collection system.....	43
5.4.7	Notification to event-causing subject	44
5.4.8	Vulnerability assessments.....	44
5.5	Records Archival Procedures	44
5.5.1	Types of records archived.....	44
5.5.2	Retention period for archive	44
5.5.3	Protection of archive	44
5.5.4	Archive backup procedures.....	44
5.5.5	Requirements for time-stamping of records.....	44
5.5.6	Procedures to obtain and verify archive information	45
5.5.7	Archive collection system	45
5.6	Key Changeover.....	45
5.7	Compromise and Disaster Recovery	45
5.7.1	Incident and compromise handling procedures	45
5.7.2	Computer resources, software and/or data are corrupted.....	45
5.7.3	Entity private key compromise procedures.....	45
5.7.4	Business continuity capabilities after a disaster.....	46
5.8	CA or RA termination.....	46
5.8.1	Termination of Swiss Government PKI.....	46
5.8.2	Termination of a certificate using application.....	46
6	Technical Security Controls	47
6.1	Key pair generation and installation	47
6.1.1	Key pair generation	47
6.1.2	Private Key delivery to subscriber	47
6.1.3	Public key delivery to certificate issuer	47
6.1.4	CA public key delivery to relying parties	47
6.1.5	Key sizes	47
6.1.6	Public key parameters generation and quality checking	48
6.1.7	Key usage purposes	48
6.2	Private key protection and cryptographic module engineering controls	48
6.2.1	Cryptographic module standards and controls	48
6.2.2	Private key (n out of m) multi-person control	48
6.2.3	Private key escrow	48
6.2.4	Private key backup.....	48
6.2.5	Private key archival.....	48
6.2.6	Private key transfer into or from a cryptographic module.....	49
6.2.7	Private key storage on cryptographic module.....	49
6.2.8	Method of activating private key	49
6.2.9	Method of deactivating private key	49
6.2.10	Method of destroying private key.....	49
6.2.11	Cryptographic module rating	49

6.3	Other aspects of key pair management	49
6.3.1	Public key archival	49
6.3.2	Certificate operational periods and key pair usage period	50
6.4	Activation data	50
6.4.1	Activation data generation and installation	50
6.4.2	Activation data protection	50
6.4.3	Other aspects of activation data	50
6.5	Computer security controls	51
6.5.1	Specific computer security technical requirements	51
6.5.2	Computer security rating	51
6.6	Life cycle technical controls	51
6.6.1	System development control	51
6.6.2	Security management controls	51
6.6.3	Life cycle security controls	51
6.7	Network security controls	51
6.8	Time-stamping	51
7	Certificate, CRL and OCSP Profiles	53
7.1	Certificate profile	53
7.1.1	Version number(s)	53
7.1.2	Certificate extensions	54
7.1.3	Algorithm object identifiers	55
7.1.4	Name forms	55
7.1.5	Name constraints	56
7.1.6	Certificate policy object identifier	56
7.1.7	Usage of policy constraints extension	56
7.1.8	Policy qualifiers syntax and semantics	56
7.1.9	Processing semantics for the critical certificate policies extension	56
7.2	CRL profile	57
7.2.1	Version number(s)	57
7.2.2	CRL and CRL entry extensions	57
7.3	OCSP profile	57
7.3.1	Version Number(s)	57
7.3.2	OCSP Extensions	57
8	Compliance Audit and other Assessments	58
8.1	Frequency or circumstances of assessment	58
8.2	Identity/qualifications of assessor	58
8.3	Assessor's relationship to assessed entity	58
8.4	Topics covered by assessment	58
8.5	Actions taken as a result of deficiency	58
8.6	Communication of results	58
9	Other Business and Legal Matters	59
9.1	Fees	59
9.2	Financial responsibility	59
9.2.1	Insurance coverage	59
9.2.2	Other assets	59
9.2.3	Insurance or warranty coverage for end-entities	59
9.3	Confidentiality of business information	59
9.3.1	Scope of confidential information	59
9.3.2	Information not within the scope of confidential information	60
9.3.3	Responsibility to protect confidential information	60
9.4	Privacy of personal information	60
9.5	Intellectual property rights	60
9.6	Representations and warranties	61
9.6.1	CA representations and warranties	61
9.6.2	RA representations and warranties	61
9.6.3	Subscriber representations and warranties	61

9.6.4	Relying party representations and warranties.....	61
9.6.5	Representations and warranties of other participants.....	61
9.7	Disclaimers of warranties.....	61
9.8	Limitations of liability.....	61
9.8.1	Swiss Government PKI limitation of liability.....	61
9.8.2	Registration Agent's limitation of liability.....	62
9.8.3	Subscriber limitation of liability.....	62
9.9	Indemnities.....	62
9.10	Term and termination.....	62
9.10.1	Term.....	62
9.10.2	Termination.....	62
9.10.3	Effect of termination and survival.....	62
9.11	Individual notices and communications with participants.....	62
9.12	Amendments.....	63
9.13	Dispute resolution provisions.....	63
9.14	Governing law.....	63
9.15	Compliance with applicable law.....	63
9.16	Miscellaneous provisions.....	63
9.17	Other provisions.....	63
9.17.1	Legally binding version of CP/CPS.....	63
10	Annexes.....	64
10.1	Annex A – References.....	64

1 Introduction

Swiss Government PKI (hereinafter referred to as "SG PKI") operates a specific public key infrastructure on behalf of the Swiss government to enable certificate based authentication, data integrity and confidentiality protection in the administration's IT networks as well as its electronic document exchange. The service is primarily available for the users of the federal, cantonal and communal administrations, but is also extended to external users having a need for securing the document exchange with administrative bodies.

The SG PKI comprises two different two-level hierarchies of CAs to cater for the many different needs:

- A group of CAs responsible for high assurance qualified and enhanced certificates (Swiss Government Root CA I), i.e. issuing qualified and enhanced certificates according to the federal administrations' terminology (see: <https://www.pki.admin.ch>). Qualified and enhanced certificates are issued on hard-tokens exclusively.
- A group of CAs supporting certificates at a lower security – regular – level for persons, organizations/organizational units, high assurance with Organization Validation SSL certificates and high assurance with Extended Validation SSL/Code-Signing certificates (Swiss Government Root CA II, hereinafter referred to as "SG Root CA II"). These certificates are usually issued as soft-tokens, except for the EV Code-Signing certificates, which are issued on hard-tokens exclusively.

This document describes the CA architecture of SG Root CA II.

The architecture consists of the following CAs:

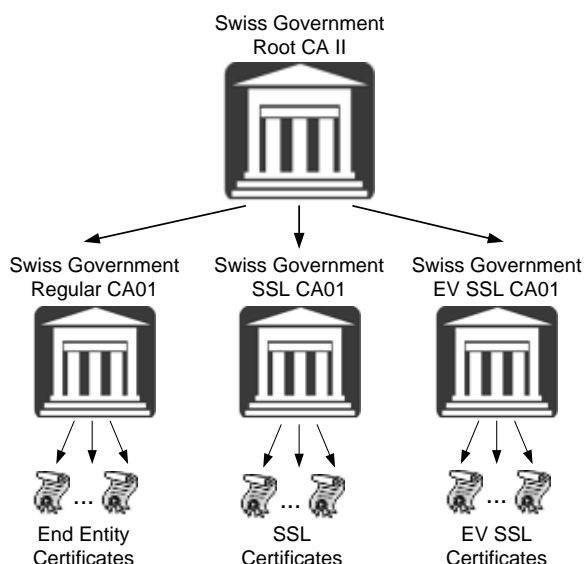


Figure 1.1 - CA hierarchy 'SG Root CA II'

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

The SG PKI issues certificates under this CP/CPS identified by the following object identifier (OID) values:

- Swiss Government EV SSL CA 01 2.16.756.1.17.3.21.3
- Swiss Government SSL CA 01 2.16.756.1.17.3.21.2
- Swiss Government Regular CA 01 2.16.756.1.17.3.21.1

The SG PKI operating under this CPS conforms to the current version of the CA/Browser Forum (CABF) requirements including:

- Guidelines for the Issuance and Management of Extended Validation (EV) Certificates
- Guidelines for the Issuance and Management of Extended Validation (EV) Code-Signing Certificates
- Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates

These requirements are published at www.cabforum.org. In the event of any inconsistency between this document and those requirements, those requirements take precedence over this document.

As the above CAs all comply with equivalent security requirements this particular document serves two purposes:

- It details the policies governing and practices followed by the Root CA's issuance of CA certificates for the subordinated CAs, i.e. it is certificate policy [CP] and certification practice statement [CPS] for the SG Root CA II.
- It details also the policies and practices of the subordinated CAs, i.e. serves as CP and CPS for the CAs issuing certificates to end-users as well.

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

1.1 Overview

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

SG PKI SSL/Code-Signing with Extended Validation Certificates are certificates issued by SG PKI in conformance with the Guidelines for Extended Validation Certificates published by the CA/Browser Forum consisting of major certification authorities and browser vendors.

SG PKI SSL with Organization Validation Certificates for servers (SSL Web Server Certificates, SSL Wildcard Certificates and SAN Certificates) also provide 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.

SG PKI Regular Certificates are Non-Public-trusted Certificates issued to organizations and individuals to provide authentication, message-, data and software- (code-) signing, and content integrity and confidentiality. SG PKI Regular certificates provide assurance of the identity of the Subscriber based on a confirmation that the subscriber organization does in fact exist, that the organization has authorized the certificate application, and that the person submitting the certificate application on behalf of the subscriber was authorized to do so.

Within these classes of certificates, SG PKI issues the following specific types of certificates to end user subscribers in accordance with this CPS:

Certificate Type	Assurance Level	Issued to	Description and Benefit
EV SSL Web Server Certificates (including SAN Certificates)	High with extended validation	Organizations	High Assurance with extended validation secure SSL Certificates issued by SG EV SSL CA 01 in conformance with the Guidelines for Extended Validation Certificates. Capable of 256-bit encryption used to support SSL sessions between web browsers and servers. In case of SAN Certificates secure multiple hosts on a single domain on the same server.
EV Code Signing Certificates	High with extended validation	Organizations	Certificates which secure delivery of code and content to browsers over the Internet issued by SG EV SSL CA 01. Issued on hard-token.
SSL Web Server Certificates (including Wildcard and SAN Certificates)	High	Organizations	High Assurance with organization validation secure SSL Certificates issued by SG SSL CA 01. Capable of 256-bit encryption used to support SSL sessions between web browsers and servers. In case of Wildcard/SAN Certificates secure multiple hosts on a single domain on the same server.
Code Signing Certificates	Medium	Organizations	Certificates which secure delivery of code and content to browsers over the Internet issued by SG SSL CA 01. Issued on soft-token.
Non-public Client	Medium	Organizations and Individuals	Medium Assurance Client Certificates for authentication,

Certificates			encryption and digital signature issued by SG Regular CA 01.
--------------	--	--	--

Table 1.1: Certificate Types within the Swiss Government PKI under the SG Root CA II

1.2 Document name and identification

This document is entitled 'Certificate Policy and Practice Statement of the SG Root CA II' and is identified by the object identifier (OID) **2.16.756.1.17.3.21.1** whose components have the meaning given in Table 1.2.

OID Component	Meaning of OID Component
2	joint-iso-itu-t
16	country
756	ch
1	organization ¹
17	Bundesamt für Informatik und Telekommunikation
3	AdminPKI
21	SG Root CA II
1	CP/CPS

Table 1.2: CP-OID of SG Root CA II

¹ Allocated by the Federal Office of Communications (OFCOM)

1.3 PKI participants

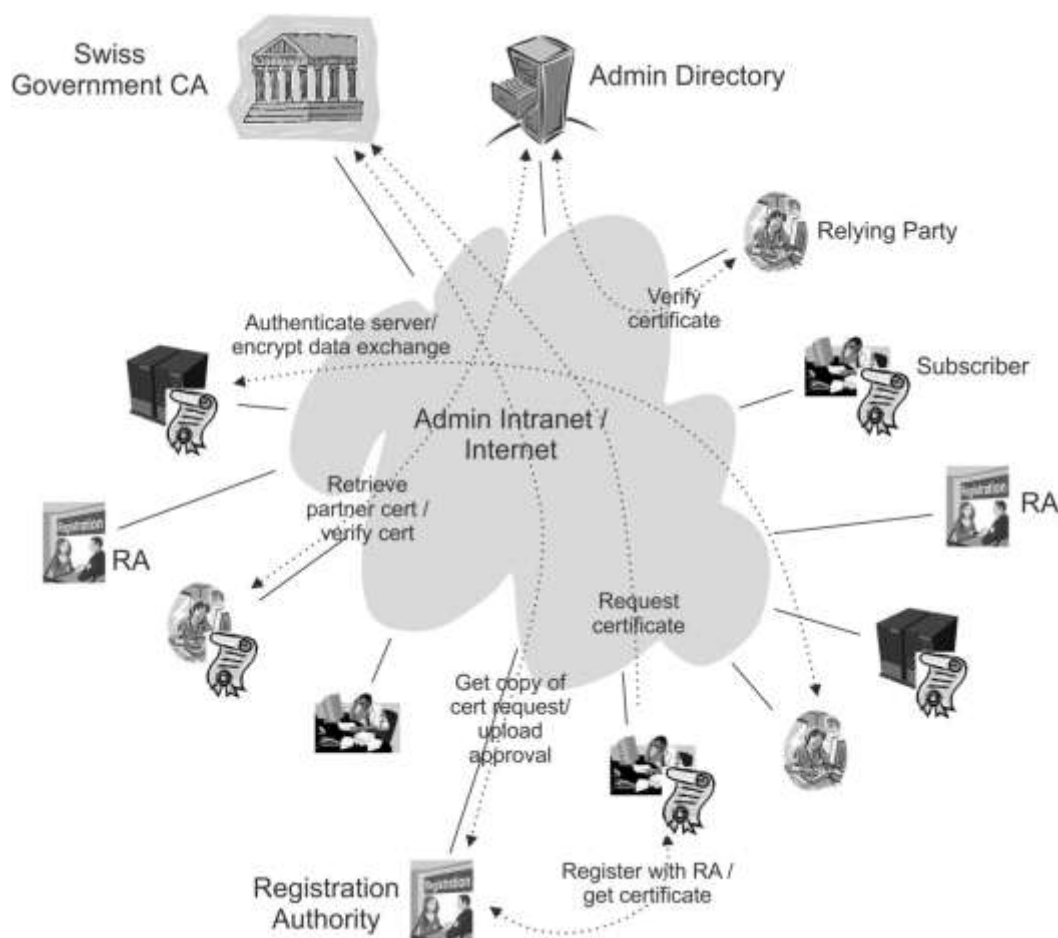


Figure 1.2 – Overview of PKI participants

1.3.1 Certification authorities

SG Root CA II is the first level CA constituting the basis of trust for all regular certificates. Its Root CA key and certificate have been generated February 16, 2011, and minutes have been taken [ref. 1]. The Root CA II certificate is formally distributed as 'trust anchor' to all participants in the Swiss Federal Administration.

SG Root CA II's tasks are:

- Ensure adherence to the processes defined for registration, certificate issuance, certificate revocation and distribution of status information by all parties concerned.
- Validate requests for the issuance, renewal and revocation of second level CA certificates.
- Issue initial and renewed second level CA certificates as requested.
- Revoke CA certificates where necessary.
- Generate and publish ARLs to support validation of CA certificates at all times.
- Publish/distribute the Root CA certificate fingerprint, thereby enabling interested parties to manually validate the Root CA certificate – Root CA certificates are self-signed and

thus cannot be chained back to any other reference for electronic validation.

SG Root CA II is operated by Swiss Government PKI staff appointed to the task, reporting to the PKI Manager.

Swiss Government subordinated CAs

At the moment there are 3 second level CAs subordinated to SG Root CA II:

- *Swiss Government EV SSL CA 01,*
- *Swiss Government SSL CA 01 and*
- *Swiss Government Regular CA 01.*

The tasks of each of the subordinate CA's are:

- Ensure adherence to the processes defined for registration, certificate issuance, certificate revocation and distribution of status information by all parties concerned.
- Validate requests for the issuance, re-key and revocation of certificates.
- Issue initial and re-keyed certificates as requested.
- Revoke certificates on user-request or in case they are misused.
- Generate and publish CRLs to support validation of end-user certificates at all times.
- Provide updated status information via an OCSP responder.

Swiss Government CAs subordinated to SG Root CA II are operated by Swiss Government PKI staff appointed to the task, reporting to the PKI Manager.

Swiss Government EV SSL CA 01

Swiss Government EV SSL CA 01 issues 'SSL Server Certificates' and 'Code Signing Certificates' after performing Extended Validation according to the Guidelines of CA/Browser Forum.

Issued Certificate Types are:

- 'EV SSL Server Certificates' issued for Web-servers, servers and network components operated by administrative bodies to support SSL (including SAN certificates).
- 'EV Code signing certificates' – certificates for signing pieces of code, e.g. applets, issued to employees of the administration responsible for web services and/or applications which must be able to prove their authenticity. Issued on a hard-token only.

Swiss Government SSL CA 01

Swiss Government Regular CA 01 issuing 'SSL Server Certificates' after performing Domain Validation.

Issued Certificate Types are:

- 'SSL Server Certificates' issued for Web-servers, servers and network components operated by administrative bodies to support SSL (including SAN- and wildcard-certificates).
- 'Code signing certificates' – certificates for signing pieces of code, e.g. applets, issued to employees of the administration responsible for web services and/or applications which must be able to prove their authenticity. Usually issued on a soft-token.

Swiss Government Regular CA 01

Swiss Government Regular CA 01 issuing 'regular' certificates to individuals/organizations to be used for authentication, signing and encryption.

Issued Certificate Types are:

- 'Group mailbox certificates' – certificates for signing and encryption, issued for shared mailboxes used by administrative bodies. The certified key pairs are distributed to all users entitled to access the individual mailboxes.
- 'Organization certificates' – certificates for authentication, signing and encryption issued to administrative bodies (federal, cantonal or communal).
- 'e-Dec certificates' – authentication certificates issued to employees of companies/organizations using the electronic goods declaration in their transactions with the Federal Customs Administration.

The above certificates are all issued as single certificates, i.e. there is just one soft-certificate issued in each case, no matter how many different usages (authentication/signing/encryption) are to be supported. The actual certificate usage are explicitly signaled in the certificate's 'key usages' field.

1.3.2 Registration authorities

To cope with the variety of certificates issued by the CA's subordinated to SG Root CA II, the submission of requests as well as the registration of applicants and requests is typically done by 'Registration Agents' of the different departments employing certificates. These agents are formally identified by the respective department's management and conveyed to SG PKI either directly or through entries in suitable directories operated by the Federal Administration. SG PKI personnel is involved in registration tasks only with requests for specific certificates where the entries in the certificates are of crucial importance (e.g. domain names identified in SSL, SAN or wildcard certificates).

The Registration Agents' (see above) tasks² are:

- Generate and submit certificate requests.
- Approve certificate requests electronically by means of the registration application, provided they are complete and technically correct.
- Transfer the encrypted certificate files to the applicants once their certificates have been issued by CA's subordinated to SG Root CA II.
- Generate and submit re-key requests.
- Verify and approve re-key requests.
- Generate and submit revocation requests.
- Verify and approve revocation requests.

A list of all Registration Agents is maintained by the SG PKI Ordermanagement.

1.3.3 Subscribers

Subscribers are natural persons, administrative units or legal entities holding certificates is-

² The different types of certificates require specific registration processes, thus only a subset of the tasks listed is relevant in each case.

sued by the CA's subordinated to SG Root CA II. They fall into one of the following categories:

- System Administrators of administrative units (organizations) representing SSL servers.
- Employees of units within the federal or a cantonal or communal administration.
- Employees of subcontractors of any of the above units, provided they are listed in FOITT's X.500 directory 'admindir.admin.ch'.
- Organizational units of the federal, or a cantonal or a communal administration.
- Employees of companies and organizations having a need for exchanging electronically signed documents, for certificate based authentication or for en-/decrypting documents in the context of their collaboration with one or several of the administration's units.

All subscribers are required to use their keys/certificates in conformance with the law on the organization of government and administration [ref. 2] as well as the regulation on organization of the Federal Department of Finances FDF [ref. 3], and always within the framework of the respective application (see section 1.4).

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

1.3.4 Relying parties

Relying parties are:

- All subscribers, i.e. holders of end-user certificates issued by any of the CA's subordinated to SG Root CA II.
- Third parties having to verify signatures, authenticate remote servers and users or encrypt messages on the basis of the certificates issued and, consequently, validate the certificates.

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 II and its subordinated CAs* MUST comply with this CP/CPS. Each type of Certificate is generally appropriate for use with the applications set forth in CPS section 1.4.1 and section 1.1 (Table 1.1). Any such usage, however, shall be limited to such entities and subject to CPS 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 usage of keys certified by SG Root CA II or one of its subordinated CAs is restricted as

per the following table:

Entity	Private key usage	Certificate usage
<i>SG Root CA II</i>	<ul style="list-style-type: none"> ▪ Sign certificates for subordinated certification authorities ▪ Sign ARLs (Authority Revocation Lists) 	<ul style="list-style-type: none"> ▪ Validate end-entity certificates chaining back to SG Root CA II
<i>Swiss Government EV SSL CA 01</i>	<ul style="list-style-type: none"> ▪ Sign EV certificates ▪ Sign CRLs (Certificate Revocation Lists) 	<ul style="list-style-type: none"> ▪ Validate EV certificates (SSL and Code Signing)
<i>Swiss Government SSL CA 01</i>	<ul style="list-style-type: none"> ▪ Sign organization validated certificates ▪ Sign CRLs (Certificate Revocation Lists) 	<ul style="list-style-type: none"> ▪ Validate organization validated certificates
<i>Swiss Government Regular CA 01</i>	<ul style="list-style-type: none"> ▪ Sign certificates ▪ Sign CRLs (Certificate Revocation Lists) 	<ul style="list-style-type: none"> ▪ Validate certificates
<i>Subscriber (Regular)</i>	<ul style="list-style-type: none"> ▪ Sign, authenticate or decrypt documents/data depending on type of certificate 	<ul style="list-style-type: none"> ▪ Use other subscribers' public keys for encrypting documents/data
<i>Subscriber ((EV) SSL)</i>	<ul style="list-style-type: none"> ▪ Authentication ▪ Code Signing 	<ul style="list-style-type: none"> ▪ Chain certificates back to SG Root CA II
<i>Relying Party</i>	<ul style="list-style-type: none"> ▪ not applicable 	<ul style="list-style-type: none"> ▪ Verify electronic signatures ▪ Verify authenticity of certificate holder ▪ Use subscribers' public keys for encrypting documents/data

Table 1.3 – Authorized usage of private keys and certificates

In general, SG PKI Certificates are general-purpose Certificates. SG PKI Certificates may be used to interoperate with diverse Relying Parties worldwide. Usage of SG PKI Certificates is not generally restricted to a specific business environment.

Nonetheless, such use is permitted and Customers 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.

Nonetheless, certain SG PKI Certificates are limited in function. For example, CA Certificates may not be used for any functions except CA functions. Moreover, individual Certificates are intended for client applications and shall not be used as server or organizational Certificates. In addition, High Assurance organizational Certificates issued to devices are limited in function to web servers, mail servers or web traffic management devices (in the case of SSL Web Server Certificates) and Code Signing (in the case of Code Signing Certificates).

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 within the SG PKI. See CPS section 6.1.7. In addition, end-user Subscriber Certificates shall not be used as CA Certificates. This restriction is confirmed by the absence of a Basic Constraints extension. See CPS 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

More generally, Certificates shall be used only to the extent use is consistent with applicable law.

1.4.2 Prohibited certificate uses

SG PKI signals the key usages it authorizes with every certificate issued. Subscribers must not use their keys for any other purpose than the one specified within the respective certificates.

1.5 Policy administration

1.5.1 Organization administering the document

FOITT is responsible for administering and publishing the current CP/CPS (see also section 9.12 of this document).

1.5.2 Contact person

Contact person is the PKI Manager:

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

1.5.3 Person determining CPS suitability for the policy

The PKI Manager and the PKI Security Manager jointly determine the document's suitability for the purposes of the accepted policies.

1.5.4 CPS approval procedures

See section 9.12 of this document.

1.6 Definitions and acronyms

Term / Acronym	Full text	Explanation
AdminDir	Admin Directory	A directory service compliant with ITU-T recommendation X.500
ARL	Authority Revocation List	A list of revoked Certification Authority certificates.
CA	Certification Authority	An entity that issues certificates.

Term / Acronym	Full text	Explanation
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	
EV	Extended Validation	Extended Validation according to the Guidelines of CA/Browser Forum
FCA	Federal Customs Administration	
FDF	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	www.bit.admin.ch
Hard-token		A portable, user controlled, physical device (e.g. smart-card) used to store cryptographic information and possibly also perform cryptographic functions.
ISBD	Informatiksicherheitsbeauftragter Departement	
ISBO	Informatiksicherheitsbeauftragter Organisation	
ITU-T	International Telecommunication Union, Telecommunication Standardization Sector	www.itu.int/ITU-T The ITU-T X-series recommendations cover data networks, open system communications and security.
LDAP	Lightweight Directory Access Protocol	
OCSP	Online Certificate Status Protocol	Online trusted source of certificate status information. The OCSP protocol specifies the syntax for communication between the OSCP server (which contains the certificate status) and the client application (which is informed of that status).
OFCOM	Federal Office of Communications	The Federal Office of Communication (OFCOM) handles questions related to telecommunications and broadcasting (radio and television) www.bakom.admin.ch .
OID	Object Identifier	A unique numerical sequence allowing the identification of any "thing", in particular also documents.
PIN	Personal Identification Number	
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#12		The specification of a format for storing and transferring

Term / Acronym	Full text	Explanation
		key pairs and certificates securely (encrypted).
PKI	Public Key Infrastructure	
Private key		Data used for creating an electronic signature or data for decrypting a data message.
Public key		Data used for verifying an electronic signature or data for encrypting a data message.
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.
Registration Agent		Employee of the administration with a department using regular certificates and authorized to register applicants, submit and – where appropriate - approve requests for regular certificates.
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.
Sedex	Secure data exchange	A platform enabling the secure (signed and/or encrypted) exchange of statistical data between cantonal/communal population registers with the Swiss Federal Office of Statistics.
SHA2	Secure Hash Algorithm	The algorithm used most widely today for hashing data to be digitally signed.
SLA	Service Level Agreement	Service contract defining the PKI services formally.
Soft-token		A data object that is used to store cryptographic information and possibly also perform cryptographic functions.
Swiss Government PKI		FOITT staff responsible for and operating all PKI services provided by the Swiss Authorities.

Table 1.4 – Definitions and Acronyms

2 Publication and Repository Responsibilities

2.1 Repositories

FOITT makes information related to SG Root CA II and its subordinated CAs publicly available through SG PKI's web site (www.pki.admin.ch) and/or the AdminDir, a directory service compliant with ITU-T recommendation X.500.

AdminDir is a trusted source, i.e. all data therein has been formally verified and may be used within certificates without additional validation. AdminDir is available from the Swiss federal administration's Intranet or using LDAP. The public version of AdminDir is accessible from the Internet using LDAP (admindir.admin.ch).

2.2 Publication of certification information

FOITT publishes information related to certificates issued by SG Root CA II and its subordinated certification authorities:

- Certificate(s) of the SG Root CA II.
- Fingerprint of the certificate of the SG Root CA II.
- Certificate(s) of the Swiss Government EV SSL CA 01.
- Fingerprint of the Swiss Government EV SSL CA 01.
- Certificate(s) of the Swiss Government SSL CA 01.
- Fingerprint of the Swiss Government SSL CA 01.
- Certificate(s) of the Swiss Government Regular CA 01.
- Fingerprint of the Swiss Government Regular CA 01.
- Encryption certificates issued to end users by Swiss Government Regular CA 01, provided these need be accessible in a given private or public environment.
- The authority revocation list (ARL) for the SG Root CA II.
- The certificate revocation list (CRL) for the SG Root CA II and its subordinated certification authorities.
- An OCSP responder server at <http://www.pki.admin.ch/aia/ocsp> provides notice on the status of a Certificate issued by SG Root CA II, upon request from a Relying Party.
- The current version of the CP/CPS for the SG Root CA II and its subordinated certification authorities.
- Relying Party Agreements

2.3 Time or frequency of publication

This CPS is published in electronic form (Adobe Acrobat format) on the SG PKI's web site at www.pki.admin.ch.

Amendments to this CPS are processed in accordance with CPS section 9.12. Updates to Subscriber Agreements and Relying Party Agreements are published as necessary. Certificates are published upon issuance. Certificate status information is published in accordance with CPS section 4.9.7.

New versions of documents are published as soon as they have been approved.

2.4 Access controls on repositories

The repositories are freely accessible on a read-only basis to all users having access to the respective network, i.e. AdminDir to all users of the intranet of the federal administration and the public version of AdminDir to all Internet users.

Information published on the web site of SG PKI is publicly accessible information. Read only access to such information is unrestricted. SG PKI requires persons to agree to a Relying Party Agreement as a condition to accessing Certificates, Certificate status information, or CRLs. SG PKI has implemented logical and physical security measures to prevent unauthorized persons from adding, deleting, or modifying repository entries.

3 Identification and Authentication

This section concentrates on the identification and authentication of subscribers, i.e. applicants for and holders of end-user certificates. Obviously, requests for the issuance and revocation of CA and Root CA certificates must be authenticated too. However, as the respective processes are all initiated by SG PKI personnel specifically appointed to the tasks, the identities and roles have already been well established and the authentication can be based on high assurance personal certificates (i.e. hard-token certificates).

3.1 Naming

3.1.1 Types of names

With all certificates issued, the issuing CA 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. It must satisfy the requirements specified in the technical directive on AdminDir by the Federal Strategy Unit for IT [ref. 4].

SG Root CA II and its subordinated CAs use a standard form of DN where the fields c, o, ou, and cn are populated (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 organizational unit of the federal, a cantonal or communal administration,
- an employee of any of the above units,
- an employee of a subcontractor to any of the above units,
- a company or organization,
- a natural person as representative of a company or organization, or
- a machine as representative of a web server, server or network component.

3.1.3 Anonymity or pseudonymity of subscribers

No stipulation

3.1.4 Rules for interpreting various name forms

The PKI can handle only characters per ITU-T recommendation T.50, the International Reference Alphabet. DNs containing un-supported characters are thus converted to a compliant form in the certification process.

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 identity

In addition to the procedures below, the Certificate Applicant must demonstrate that it rightfully holds the private key corresponding to the public key to be listed in the Certificate in accordance with CPS section 3.2.1.

Authentication of the Identity of Organizational End-User Subscribers

The authenticity of communities applying for regular organization certificates is verified with the help of the official Swiss commune register (see also section 3.1.1).

Private companies/organizations are authenticated by the administrative units having authorized them for getting issued SG PKI certificates (see section 4.1.1).

CABF Verification Requirements for Organization Applicants

The authenticity of communities applying for organization certificates with Extended Validation is validated according to the Guidelines of CA/Browser Forum³.

Mozilla Verification Requirements for Organization Applicants

For requests for internationalized domain names (IDNs) in Certificates, SG PKI performs domain name owner verification to detect cases of homographic spoofing of IDNs. SG PKI employs a manual process that searches various corresponding 'whois' services to find the owner of a particular domain. If the search is inconclusive, the Certificate Request is rejected by the RA.

3.2.3 Authentication of individual identity

With applications for SSL server certificate SG PKI ensures the requests and the data therein

³ Validation according to chapter 11 of http://cabforum.org/wp-content/uploads/Guidelines_v1_4_3.pdf

are authentic in the following way:

- SSL server certificates are issued to entities that belong to or are closely related to federal, cantonal or communal administration.
- CA's subordinated to SG Root CA II do explicitly not issue certificates for identifying servers not visible to Internet's DNS i.e. using any of the following identifiers
 - hostnames
 - private IP addresses
 - internal domain names
- As a prerequisite, signatories of the departments owning domains need to formally authorize selected system administrators to act as Registration Agents for requesting SSL server certificates identifying the respective domains. SG PKI maintains a list of these particular Registration Agents (forming the 'DomainSSL' group) together with the domains they are responsible for. With each request for a SSL server certificate, the authorization of the requester and the validity of the domain(s) to be identified are verified per the above list
- Requests for domains not supported by the list or not in compliance with the established guidelines for SAN-certificates undergo exception handling wherein the requester is required to give further evidence supporting the request, e.g. on the basis of the Swiss Official Gazette of Commerce 'SHAB' or 'WHOIS' supported by written or verbal assent of the respective domain owner.
- E-mail addresses to be added to SSL server certificates are validated by SG PKI staff through a challenge/response procedure.

Applicants for regular personal certificates are authenticated by means of the corresponding entries in AdminDir. As AdminDir is a trusted database, subscriber identifying data such as e-mail addresses etc. may be retrieved from there without additional verification. Representatives of private companies requiring a certificate first need to get a formal entry established in AdminDir, upon which the data on their identities may be trusted in the same way as with federal employees.

3.2.4 Non-verified subscriber information

No stipulation.

3.2.5 Validation of authority

SG PKI validates the authority of Registration Agents before enabling them to use any of the applications necessary for requesting certificates and approving requests. For that purpose SG PKI consults with the management of the administrative unit or company concerned (see section 4.1.2).

3.2.6 Criteria for interoperation

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

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

4.1 Certificate application

4.1.1 Who may submit a certificate application

Requests for Regular, SSL, EV certificates may be submitted exclusively by server administrators and Registration Agents formally authorized for the task (see section 1.3.2).

4.1.2 Enrollment process and responsibilities

The enrollment processes for the different types of certificates issued by CA's subordinated to SG Root CA II together with the responsible parties are:

Step	Description	Responsible
Apply for SSL server certificate (EV or OV)	1. Using registration application, server administrator submits electronic certificate request generated by server, together with request form specifying the domain names to be confirmed by the certificate.	Server administrator authorized by management of department concerned
Register applicant and domain names, approve request	2. Verify server administrator's authorization and correctness of request. 3. Verify ownership of domain(s). 4. Verify request from domain angle and, if correct, approve in registration application. For EV certificates, steps 2-4 are performed in accordance with the Guidelines of CA/Browser Forum	SG PKI Order Management SG PKI Administrator Domain Owner or delegate
Issue certificate	5. Issue certificate on basis of request, generate soft-token and download to server or send to server administrator. Certificates are issued by Swiss Government EV SSL CA 01 (for EV certificates) or Swiss Government SSL CA 01 (for organization validated certificates)	Registration application / SG PKI Administrator

Table 4.1 – Registration Process and Responsibilities for (EV) SSL server certificate

Step	Description	Responsible
Apply for SSL server certificate (SAN- or wildcard-certificate)	1. Server administrator submits certificate request generated by server by e-mail to PKI Order Management, together with request form specifying the domain names to be confirmed by the certificate.	Server administrator authorized by management of department concerned
Register applicant and domain names, approve request	2. Verify server administrator is authorized for domains in question. 3. Verify ownership of domain(s). 4. Verify request from domain angle and, if correct, approve in registration application. For EV certificates, steps 2-4 are performed in accordance with the Guidelines of CA/Browser Forum	SG PKI Order Management SG PKI Administrator Domain Owner or delegate
Issue certificate	5. Issue certificate on basis of request, generate soft-token and download to server or send to server administrator. Certificates are issued by Swiss Government EV SSL CA 01 (for EV certificates) or Swiss Government SSL CA 01 (for organization validated certificates)	Registration application / SG PKI Administrator

Table 4.2 – Registration Process and Responsibilities for (EV) SAN- or wildcard- certificate

Step	Description	Responsible
Apply for regular shared mailbox certificate	1. Registration Agent generates and submits certificate request through registration application.	Registration Agent or his deputy, authorized by management of administrative body running shared mailbox
Register and approve application	2. Approve request through registration application.	Registration Agent or his deputy
Verify technical correctness	3. PKI Order Management verifies if request and shared mailbox as specified are technically correct. 4. Where requested, have shared mailbox established as specified by requester.	PKI Order Management PKI Order Management
Issue certificate	5. Issue certificate on basis of request, generate soft-token and send to applicant. Certificates are issued by Swiss	Registration application / CA (processes run automatically)

	Government Regular CA 01.	
--	---------------------------	--

Table 4.3 – Registration Process and Responsibilities for shared mailbox certificates

Step	Description	Responsible
Apply for regular Sedex certificate	1. Registration Agent generates and submits certificate request through registration application.	Registration Agent authorized by management of administrative body using Sedex.
Register and approve application	2. Approve request through registration application.	Registration Agent
Verify entries for requester and intended addressees	3. Entries in the applicable directories (OSCI-TV and IDM) are verified.	Automated process
Issue certificate	4. Issue certificate on basis of request, generate soft-token and send to applicant. Certificates are issued by Swiss Government Regular CA 01.	Registration application / CA (processes run automatically)

Table 4.4 – Registration Process and Responsibilities for organization certificate (to be used in conjunction with Sedex)

Step	Description	Responsible
Apply for regular e-Dec certificate	1. Registration Agent generates and submits certificate request through application run by FCA.	Registration Agent authorized by the FCA
Register and approve application	2. Registration application approves request automatically, provided the certificate subject (organization) is listed in AdminDir.	Registration application
Issue certificate	3. Issue certificate on basis of request, generate soft-token and send to FCA application. Certificates are issued by Swiss Government Regular CA 01.	Registration application / CA (processes run automatically)

Table 4.5 – Registration Process and Responsibilities for e-Dec certificate

Step	Description	Responsible
Apply for regular code signing certificate	1. Registration Agent – the intended certificate owner with code signing certificates - submits formal request by e-mail to PKI Order Management.	Registration Agent formally authorized by the head of the administrative body asking for the certificate
Register and approve application	2. Identify Registration Agent face-to-face on the basis of a passport/identity card. 3. Verify Registration Agent's	PKI Security Officer

	<p>authorization.</p> <p>4. Approve request.</p>	
Issue certificate	<p>5. Issue certificate.</p> <p>6. Generate soft-token and hand it personally to requester.</p> <p>If EV generate hard-token and hand it personally to requester.</p> <p>Certificates are issued by Swiss Government EV SSL CA 01 (for EV certificates) or Swiss Government SSL CA 01.</p>	<p>Registration application / CA (processes run automatically)</p> <p>PKI Security Officer</p>

Table 4.6 – Registration Process and Responsibilities for (EV) Code Signing certificate

4.2 Certificate application processing

4.2.1 Performing identification and authentication functions

SG PKI identifies Registration Agents authorized by the management of the administrative unit or company having a need for certificates just initially and authorizes them to access its registration application (or the application run by FCA) for requesting and downloading certificates⁴. The registration application (or the FCA application) then authenticates the agents with each certificate request they submit.

Registration Agents authorized to approve requests autonomously are authenticated by the registration application on the basis of enhanced certificates.

Before issuing an EV certificate, SG PKI ensures that all subject organisation information in the EV certificate conforms to the requirements of, and has been verified in accordance with, the CA/Browser Forum EV Guidelines and matches the information confirmed and documented by the CA pursuant to its verification processes. Such verification processes are intended accomplish the following:

- Verify the organization's existence and identity as a federal or cantonal/communal administrative unit
- 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 signed the registration form in case of SAN- and Wildcard certificate requests.

4.2.2 Approval or rejection of certificate applications

Certificate type	Condition for approval	Responsible
------------------	------------------------	-------------

⁴ Server administrators acting as Registration Agents for SSL server certificates must be identified face-to-face on the basis of a formal identity document.

requested		
(EV) SSL Web Server Certificates (including Wildcard and SAN Certificates)	<ol style="list-style-type: none"> 1. Request formally correct and complete 2. Request submitted by authorized Registration Agent (a server administrator) 3. Domain names within the range assigned to the requesting Registration Agent (see 3.2.3) 4. <i>For EV certificates:</i> Extended validation according to the Guidelines of CA/Browser Forum must be successful 	PKI Order Management PKI Order Management PKI Security Officer
Certificate for shared mailbox	Request formally correct and complete	Registration Agent /PKI Order Management
Organization certificate	Request formally correct and complete	Registration Agent/PKI Order Management
e-Dec certificate	<ol style="list-style-type: none"> 1. Request formally correct and complete 2. Subject DN (i.e. of company to be certified) listed in AdminDir 	Registration Agent/PKI Order Management Registration application
(EV) Code signing certificate	<ol style="list-style-type: none"> 1. Request formally correct and complete 2. Request submitted personally by authorized agent of requesting administrative unit 3. <i>For EV certificates:</i> Extended validation according to the Guidelines of CA/Browser Forum must be successful 	PKI Order Management PKI Security Officer

Table 4.6 – 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. If they are in doubt, Registration Agents consult with SG PKI.

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

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

All CA's subordinated to SG Root CA II issue certificates on-line, i.e. once a valid request has been approved, the CA automatically issues the certificate asked for. The registration application delivers the certificate tokens to the requesting parties either by e-mail (e.g. SSL server certificate tokens) or by download to the requesting application, 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

All CA's subordinated to SG Root CA II notify the subscribers on the issuance of certificates by e-mail, using the e-mail addresses verified in the registration process (see 3.2.3).

4.4 Certificate acceptance

4.4.1 Conduct constituting certificate acceptance

SG PKI doesn't require a formal acceptance of the certificates it issues. Certificates are deemed to be accepted with the successful handover of certificates tokens by the registration application.

4.4.2 Publication of the certificate by the CA

e-Dec- and code signing certificates issued by Swiss Government Regular CA 01 are published in AdminDir, publicly accessible.

Organization certificates to be used for Sedex are published in the Sedex user directory (OSCI-TV, not publicly accessible).

(EV) SSL 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 II. However, the Registration Agents can retrieve data on certificates issued at their convenience from the CA's reporting.

4.5 Key pair and certificate security rules

4.5.1 Subscriber private key and certificate usage

Subscribers must use their private keys and certificates strictly as stipulated in section 1.4.

Beside the adherence to the key usages specified, subscribers are bound to the following

rules when using their keys and certificates:

- Use approved applications only.
- Ensure they alone have access to their private keys, i.e. keep the respective passwords strictly confidential.
- In case they suspect or know a private key has been compromised, subscribers must stop signing or authenticating immediately (depending on the certificated key usage) and report the incident to a Registration Agent either personally or by e-mail or phone.
- In case data confirmed by certificates is no longer valid, certificate holders must see to the revocation of the certificates concerned (see 4.9) and stop using signature and authentication keys.

4.5.2 Relying party public key and certificate usage

Relying parties must use public keys and certificates solely

- by means of approved applications,
- if keys and certificates are valid and active (i.e. not revoked),
- for the purpose(s) indicated in the certificates.

Relying parties must validate certificate chains as per ITU-T recommendation X.509.

Relying parties must read and agree to all terms and conditions of this CP/CPS and End-User Agreement.

4.6 Certificate renewal

Certificate renewal is not supported by any of the CA's subordinated to SG Root CA II. 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 must 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 II 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 regular organization certificates used in Sedex, e-Dec and code signing 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.

4.7.7 Notification of certificate issuance by the CA to other entities

Cantonal and communal administrative bodies having signed the applicable framework contract and concluded the agreement with SG PKI have access to SG PKI's reporting. From there they can retrieve data on re-keyed certificates.

4.8 Certificate modification

CA's subordinated to SG Root CA II do not support certificate modification. In case a certificate's content is obsolete, its holder must request a re-key of the certificate and thus proceed as per section 4.7. The certificate holder must also see to the revocation of the original certificate (see 4.9.1).

4.9 Certificate revocation and suspension

4.9.1 Circumstances for revocation

Certificates of any type must be revoked under the following circumstances:

- A compromise of private key or password of a token is suspected or has actually happened.
- A certificate token has been erased.
- Any part of the certificate subject has changed.
- A certificate has been acquired illegitimately.
- A subscriber has been dismissed or suspended by his employer.

- The contract with a subscriber has expired.
- A subscriber or a Registration Agent has violated the rules set out in this CP/CPS.
- The issuing CA (a subordinate of SG Root CA II) ceases its operation.
- The EV certificate issued does not comply anymore with the terms and conditions of the EV Guidelines .

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.
- The ISBD and ISBO.

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 actual requester (see 4.9.2) 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 II, which 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 II revoke certificates without delay as soon as it receives approved requests from a Registration Agent. During office hours the CA updates its CRL in four-hour intervals (no matter if there have been revocations or not) and uploads it to Admin-Dir and to <http://www.pki.admin.ch> for publication (for details see 2.3).

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 alternatively a valid CRL issued by the CA (a subordinate of SG Root CA II), that issued the affected certificate, at the moment they verify that certificate on the basis of a SG PKI certificate.

4.9.7 CRL issuance frequency

All CA's subordinated to SG Root CA II issue and publish updated CRLs every four hours during office hours (see 2.3).

SG Root CA II issues and publishes updated ARLs every year as a standard. Additionally, if a certificate of one of its subordinated CAs is revoked the SG Root CA II updates its ARL and publishes it immediately.

4.9.8 Maximum latency for CRLs

CRLs updated by the issuing CA are sent to and published in AdminDir and via <http://www.pki.admin.ch> within maximally 24h.

4.9.9 On-line revocation/status checking availability

The SG PKI provides an OCSP service for certificate status validation. The certificate status database, used by the OCSP service, is updated every four hours during office hours.

Within the OCSP response, the fields "This Update" and "Next Update" reflect the validity period of the returned OCSP status. Information regarding requests and responses is retained for a period of 11 years.

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

Beside the publication of CRLs in AdminDir and via <http://www.pki.admin.ch> there aren't any other forms of revocation notifications available.

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 regular certificates.

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 a downloadable CRL or by requesting certificate status information from the OCSP responder.

The certificate status database, used by the OCSP responder, is updated every four hours during office hours.

The CRLs list the serial nos. of all revoked certificates issued by the CA which haven't expired yet. The CRLs are published in AdminDir and via <http://www.pki.admin.ch> (see 2.1).

4.10.2 Service availability

Both services (retrieval of CRLs as well as the OCSP responder) are available minimally 99% of the time during office hours. At all other times the availability of the services is not guaranteed. However, outages are shorter than 24h in 80% of all cases.

4.10.3 Optional features

There aren't any optional features to the status service offered.

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

To achieve recovery of encryption keys certified by Swiss Government Regular CA 01, these are escrowed by Swiss Government PKI. The keys are escrowed virtually indefinitely as the original private keys are required for decrypting documents/data until all data protected is no longer used.

4.12.1 Key escrow and recovery policy and practices

A key archive server runs in the background as part of the registration application operated by SG PKI. In the course of the certificate issuance, (see 4.1.2) it stores applicants' encryption key pairs in a secure backup database. These keys may thus be recovered on subscribers' requests.

4.12.2 Session key encapsulation and recovery policy and practices

No stipulation.

5 Management, Operational, and Physical Controls

5.1 Physical 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 [ref. 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 and System Access Management

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 'four eyes' 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 and is the primary responsible for SG PKI. His main tasks are reviewing and approving security and certification policies as well as assure the operation of the infrastructure.

- **PKI Manager**

The PKI Manager is responsible for implementing SG PKI's services. His tasks include participating in the strategic planning, maintaining relations with clients and providers and managing SG PKI personnel.

- **PKI Engineer**

The PKI Engineer of SG PKI is responsible for the technical support and the improvement of SG PKI's services.

He has to achieve the strategic goals set by PKI officer and PKI Manager.

The PKI Engineer is also responsible for the architecture, the design and the implementation of PKI techniques. He permanently observes the technical developments in the market, ensures SG PKI possesses the latest software versions and has these installed where appropriate.

- **PKI Security Officer**

The PKI Security Officer is responsible for enforcing compliance with all legal requirements, for the adherence to physical and functional security policies by SG PKI and its environment. He manages the physical access control to the certification platform. The PKI Security Officer is the only role entitled to access and read archives and analyzing activity logs.

- **Operating Team**

The Operating Team is responsible for the running all services delivered 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.

The Operating Team also maintains the applications and the network supporting registration, issuance and revocation for/of certificates and the other services provided by SG PKI.

- **Repository Officer**

The Repository Officer is responsible for the operation and the availability of the repository in conformance with the respective SLA.

- **Information Officer**

The Information Officer is responsible for the publication of information supporting subscribers and third parties. He is also responsible for SG PKI's website <http://www.pki.admin.ch> and answers client's questions addressed to uki-info@bit.admin.ch.

- **Auditor**

The Auditor is an auditing company assigned by FOITT's legal service. 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.

- **Registration Agent**

Registration Agents are employees of the federal or a cantonal or communal administration working with one of the departments using regular certificates, e.g. server administrators, persons responsible for secure shared mailboxes, etc. They are identified as Registration Agents to SG PKI staff by their superiors to support certificate issuance for the department or the organization concerned. Registration Agents get authorized by SG PKI to use the registration application it runs.

5.2.2 Number of persons required per task

With the exception of the standard tasks performed by the Operating Team, security critical actions require two persons 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 based on qualified certificates. 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 Manager 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 II and its subordinated CAs are operated by qualified and experienced employees of the Swiss federal administration. They are appointed for an indefinite period of time, and normally they are 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.

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 [ref. 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 [ref. 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 II (this document).
- SG PKI security policy [ref. 10].
- SG PKI manual on operation and organization [ref. 11].
- Manuals on the hard- and software being used by the PKI system and applications.

5.4 Audit Logging Procedures

5.4.1 Types of events recorded

All relevant events related to the issuance and maintenance of SG PKI certificates are logged automatically or manually (journals, e.g. for recording entries to/exits from a protected room) for checking purposes, together with date/time, type, reason for and result of action, name of 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' [ref. 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 collection 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

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.

The PKI Security Officer is warned in case there are critical anomalies detected.

5.5 Records Archival Procedures

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, 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.

Only the PKI Security Officer is authorized to access the archived data in the presence of a second SG PKI staff member (four eyes principle).

5.5.4 Archive backup procedures

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

5.5.5 Requirements for time-stamping of records

Each event registered, and subsequently archived, gets time-stamped on the basis of the

central date/time reference provided by FOITT.

5.5.6 Procedures to obtain and verify archive information

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

5.5.7 Archive collection system

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

5.6 Key Changeover

None of the subordinate CA's support key changeover. Instead, the CA re-keys and uses the new CA key for signing end-user certificates early enough for all end-user 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

The PKI Security Officer specifies the procedures for incident and compromise handling and informs all SG PKI staff accordingly.

5.7.2 Computer resources, software and/or data are corrupted

All active keys and certificates used by SG Root CA II 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 end-user certificates is backed up daily as well. Consequently, in case any of SG PKI's important IT resources or data are corrupted the recovery procedures enable the resumption of the full service within maximally two days.

Data on the registration and certification processes are backed up incrementally by the CA's databases. Consequently, only status information may have to be recovered manually in case of DB failures.

5.7.3 Entity private key compromise procedures

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 all subscribers concerned.
- Revoking all subscribers' certificates signed by the compromised key.

- Revoking the CA's certificate (by SG Root CA II) 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 (Microsoft, Mozilla, Adobe, others) supporting SG PKI CA certificates as trust anchors and providing them with the necessary updates.

If the key of SG Root CA II 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 Root CA 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 II and its subordinated Swiss Government CA 01 with all necessary processes starting seven days after a disaster.

5.8 CA or RA termination

5.8.1 Termination of Swiss Government PKI

In case SG PKI decides to terminate CA operation⁵, 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 II.

All valid certificates, including Root CA and subordinated CA certificates, will be revoked and a final CRL and ARL published on FOITT's website for a minimum of eleven years. The Root CA key and the ones of the subordinated CA inclusive of all backup copies will be destroyed.

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

5.8.2 Termination of a certificate using application

In case an application using certificates is to be discontinued – leading to the termination of the registration activities by the responsible Registration Agents – SG PKI updates its lists of operational Registration Agents accordingly and, where necessary, amends its SLA with the administrative unit responsible for the Registration Agents. The respective registration data is archived (by the standard archival process, see 5.5) and will be retained for at least eleven years.

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

6 Technical Security Controls

6.1 Key pair generation and installation

6.1.1 Key pair generation

Root CA and subordinated CA key pairs are generated in HSMs conformant to FIPS 140-2 level 3 or EAL 4+.

6.1.2 Private Key delivery to subscriber

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

With some specific types of certificates issued (e.g. e-Dec certificates) Swiss Government CA Regular 01 also generates key pairs on behalf of the requesters as they lack the necessary technical means. Once the corresponding certificates have been issued the CA 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.

6.1.3 Public key delivery to certificate issuer

Requester's public key is delivered to the CA within the technical certificate request generated by the registration application, signed by the corresponding private key.

6.1.4 CA public key delivery to relying parties

SG PKI publishes the end-user certificates of SG Root CA II and its subordinated CA's

- in AdminDir,
- on its Website <http://www.pki.admin.ch>.

SSL server certificates are not published.

On request FOITT's Service Desk provides a copy of the SG Root CA II certificate's fingerprint for verification.

6.1.5 Key sizes

SG Root CA II and all of its subordinated CA's use keys of 4096 bits.

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

6.1.6 Public key parameters generation and quality checking

All CA keys are generated by HSMs conformant to FIPS 140-2 level 3 or EAL 4+.

6.1.7 Key usage purposes

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

SG PKI ensures Root CA and CA private keys are strictly used as indicated by the flags, i.e. for certificate and CRL signing.

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

6.2 Private key protection and cryptographic module engineering controls

6.2.1 Cryptographic module standards and controls

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

6.2.3 Private key escrow

Where applicable, subscribers' encryption key pairs are escrowed by a key archive server run by SG PKI which encrypts the key pairs for storage. The server is operated in a secure location and accessible to specifically authorized SG PKI staff only.

6.2.4 Private key backup

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

6.2.5 Private key archival

There aren't any private keys archived, except those listed section 6.2.3.

6.2.6 Private key transfer into or from a cryptographic module

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

6.2.7 Private key storage on cryptographic module

Root CA 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

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

Subscribers activate their private keys by entering the respective password.

6.2.9 Method of deactivating private key

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

The subscriber is solely responsible for the deactivation of private key.

6.2.10 Method of destroying private key

Root CA 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 BIT's formal concept for waste disposal - the 'BIT Entsorgungskonzept'. The process requires at least two SG PKI staff members authorized for the task.

The subscriber is solely responsible for the destroying of private key.

6.2.11 Cryptographic module rating

For ratings see section 6.2.1.

6.3 Other aspects of key pair management

6.3.1 Public key archival

All public keys – Root CA's, 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

SG PKI certificate validity periods are:

- 24 years with SG Root CA II.
- 14 years with the subordinated CA.
- 3 years with end-user certificates.

The usage periods for the private signature keys are:

- 10 years with SG Root CA II.
- 12 years with the subordinated CA.
- 2 years with end-user certificates.

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

6.4 Activation data

6.4.1 Activation data generation and installation

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

Activation data for the certificate tokens – the initial passwords – is generated and entered by the registration application automatically in the course of certificate issuance.

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 (see [12]).

In the course of registration the Registration Agents instruct subscribers on how to adequately protect access to their certificate tokens and private keys and the possible consequences of neglect in that respect.

6.5 Computer security controls

6.5.1 Specific computer security technical requirements

SG PKI uses mandatory access control with all applications making up its PKI service.

With critical processes such as re-keying CA keys, handling HSMs etc., segregation of duties is enforced, requiring typically two authorized SG PKI staff members for a process to execute.

There is a penetration test performed weekly on SG PKI's IT infrastructure, and it is audited yearly by the Auditor (see section 8.2).

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. With priority SG PKI employs reliable products protected against unauthorized changes.

6.6.2 Security management controls

The PKI Security Officer regularly verifies the integrity of the certification service's components.

6.6.3 Life cycle security controls

No stipulation.

6.7 Network security controls

SG PKI's certification infrastructure is operated in a specific network-segment separated from the federal administration's intranet by a gateway acting as a firewall. This blocks all protocols which are not absolutely necessary with SG PKI's operations.

6.8 Time-stamping

SG PKI offers a time-stamping service supporting electronic signing. SG PKI operational rules apply likewise for the time-stamping service, for details see the time stamping authori-

ty's policy [ref. 13].

7 Certificate, CRL and OCSP Profiles

All certificates and CRLs issued by SG Root CA II 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 [ref. 14], article 3.4, although the operation of the CAs is not covered by ZertES.

7.1 Certificate profile

The subsidiaries of this CA issue X.509 Version 3 certificates in accordance with PKIX. The structure of such a certificate is:

Certificate Field	Value	Comment
Version	X.509 Version 3	See section 7.1.1
Serial number	Unique number	Will be used in CRL
Signature algorithm identifier	OID	See section 7.1.3
Validity period	Start date, expiration date	
Subject	According to X.500	See Definitions in section 1.6
Subject Public Key Info	Public Key algorithm, Subject Public Key	See section 7.1.3
Extensions	X509V3 Extensions	See section 7.1.2
Signature	Certificate Signature	

Certificates of the subordinated CA *Swiss Government SSL CA 01* and *Swiss Government EV SSL CA 01* conform to the current version of the CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates.

For EV certificates the following fields must be included in the subject:

- Common Name (FQDN): /CN
- Organizational Unit /OU
- Organizational Unit /OU
- Organization: /O
- Country: /C
- Business Category 2.5.4.15

In accordance with the revised EV Guidelines the field *businessCategory* MUST contain one of the following strings: "Private Organization", "Government Entity", "Business Entity", or "Non-Commercial Entity" depending upon whether the Subject qualifies under the terms of section 7.2.2, 7.2.3, 7.2.4 or 7.2.5 of these Guidelines, respectively.

7.1.1 Version number(s)

Certificates issued by any of the CA's subordinated to SG Root CA II are of version 2 in ac-

cordance with recommendation X.509 v3.

7.1.2 Certificate extensions

Subject of the SG Root CA II certificates

CA Type	Subject	Issuer
Root CA	/CN=SG Root CA II /OU=Certification Authorities /OU=Services /O=The Federal Authorities of the Swiss Confederation /C=CH	/CN=SG Root CA II /OU=Certification Authorities /OU=Services /O=The Federal Authorities of the Swiss Confederation /C=CH
Issuing CA	/CN=Swiss Government Regular CA 01 /OU=Certification Authorities /OU=Services /O=The Federal Authorities of the Swiss Confederation /C=CH	/CN=SG Root CA II /OU=Certification Authorities /OU=Services /O=The Federal Authorities of the Swiss Confederation /C=CH
Issuing CA	/CN=Swiss Government SSL CA 01 /OU=Certification Authorities /OU=Services /O=The Federal Authorities of the Swiss Confederation /C=CH	/CN=SG Root CA II /OU=Certification Authorities /OU=Services /O=The Federal Authorities of the Swiss Confederation /C=CH
Issuing CA	/CN=Swiss Government EV SSL CA 01 /OU=Certification Authorities /OU=Services /O=The Federal Authorities of the Swiss Confederation /C=CH	/CN=SG Root CA II /OU=Certification Authorities /OU=Services /O=The Federal Authorities of the Swiss Confederation /C=CH

Root CA and Subordinate CA Certificate extensions

Certificate extensions used with SG Root CA II's and each of the subordinated CA's certificates:

Extension	Objective	Criticality
Authority Key Identifier	Identifies key used by issuer of certificate.	not critical
Subject Key Identifier	Identifies key used by subject of certificate.	not critical
Key Usage	Lists intended usages of private key.	critical
Certificate Policies	Identifies policy governing the operation of the Root CA (the current CP/CPS).	not critical

Extension	Objective	Criticality
Basic Constraints	<ol style="list-style-type: none"> 1. Indicates type of certificate subject: CA or end-user (here: CA). 2. Indicates how many CA levels may be subordinated to CA (with Root CA II: no limit given, with subordinated CAs: limit is 0). 	critical
CRL Distribution Points	Lists address(es) where status information on certificate may be found.	not critical
Authority Information Access	Lists URIs to access the issuer certificate as well as the OCSP service to request certificate status information from.	not critical

Table 7.1 – Root CA and CA certificate extensions

End-user Certificate extensions

Extension	Objective	Criticality
Authority Key Identifier	Identifies key used by issuer of certificate.	not critical
Subject Key Identifier	Identifies key used by subject of certificate (the end-user).	not critical
Key Usage	Lists intended usages of private key.	critical
Certificate Policies	Identifies policy governing the operation of the Root CA (the current CP/CPS).	not critical
Subject Alternative Name	Shows additional subject identifiers depending on type of certificate and usage, e.g. e-mail address, domain or subdomain name, etc.	not critical
CRL Distribution Points	Lists address(es) where status information on certificate may be found.	not critical

Table 7.2 – End-user certificate extensions

7.1.3 Algorithm object identifiers

There are two algorithms used in conjunction with regular 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 II and the subordinated CAs are identified in the certificates (as issuer and/or subject) as follows:

DN Field	Value
Country (c)	CH
Organization (o)	The Federal Authorities of the Swiss Confederation

Organizational Unit (ou)	Services
Organizational Unit (ou)	Certification Authorities
Common Name (cn)	Swiss Government <Name of individual CA>

Table 7.3 – CA Name forms

Subscribers are identified as certificate subjects in the following way:

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

Table 7.4 – Subscriber name forms

Subscribers are identified as SSL server certificate subjects in the following way:

DN Field	Value
Country (c)	CH
Organization (o)	Swiss Government PKI
Organizational Unit (ou)	Servers
Organizational Unit (ou)	SSL
Common Name (cn)	<fully qualified domain name>

Table 7.5 – Subscriber name forms for (EV) SSL server certificates

7.1.5 Name constraints

Not implemented.

7.1.6 Certificate policy object identifier

The one applicable policy OID is the one of the current document: 2.16.756.1.17.3.21.1

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 II 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 II's and subordinate CAs' certificates are:

CRL Extension	Objective	Criticality
CRL number	No. of CRL (CRLs are sequentially numbered).	not critical
CRL Entry Extension		
Reason Code	Identifies actual reason for revoking certificate.	not critical
Invalidity Date	Indicates known or suspected date a key was compromised.	not critical

Table 7.5 – 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 II 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 II 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 II and it's subordinate CA's as well.

8.2 Identity/qualifications of assessor

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

8.3 Assessor's relationship to assessed entity

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

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

PKI Manager and PKI Security Officer agree with the Auditor 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.

8.6 Communication of results

Audit results are just communicated to PKI Director, PKI Manager and PKI Security Officer as a standard and, where advisable, to other employees/units of the federal administration on a 'need to know' basis, e.g. SG PKI staff, FOITT legal services, etc.

9 Other Business and Legal Matters

9.1 Fees

SG PKI's costs for running the certification services basing on SG Root CA II 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 the 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 2).
- SG PKI documents intended for subscribers, relying parties and third parties, e.g. this CP/CPS.

9.3.3 Responsibility to protect confidential information

All SG PKI staff and Registration Agents are responsible for protecting confidential information. 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 II (this document).
- Directives for registration for regular certificates.
- Contracts and other agreements concluded between SG PKI and its clients (federal, cantonal and communal administrative units).
- Certificates issued by Swiss Government EV SSL CA 01.
- Certificates issued by Swiss Government SSL CA 01.
- Certificates issued by Swiss Government Regular CA 01.

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.

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 (see section 1.3) 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 handing 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 regular 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

As a standard, SG PKI communicates by e-mail with all participants.

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

9.12 Amendments

The PKI Director or the PKI Manager 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.

Material changes to the CP/CPS must be advertised 30 days in advance.

Subscribers will be notified where necessary.

9.13 Dispute resolution provisions

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

9.14 Governing law

This CP/CPS is subject to the applicable Swiss federal laws, particularly the law on data protection DSG [ref. 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.

10 Annexes

10.1 Annex A – References

- [1] Minutes of SG Root CA II root ceremony
- [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] Frame contract between Subscriber and SG PKI
- [6] Subscriber agreement with SG PKI
- [7] SG PKI access control directive
- [8] Ordinance on Security Checks for Persons (OSCP)
- [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
- [11] SG PKI manual on operation and organization
- [12] SG PKI's operating manual 'Periodic Monitoring or Functions and Activities'
- [13] Policy of Time Stamping Authority
- [14] SR 943.03 Federal law on the certification services supporting electronic signatures ZertES
http://www.admin.ch/ch/d/sr/c943_03.html
- [15] SR 235.1 Federal law on data protection DSG
http://www.admin.ch/ch/d/sr/c235_1.html