Swiss Government's PKI - Root CA II

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

Document OID : 2.16.756.1.17.3.21.1

Project Name: **Swiss Government Root CA II**

Project Number: **-**

Version: **V0.1g**

Status	At Work	Verify	Approved
	☒	☐	☐

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

Changes			
Date	**Version**	**Who**	**Description**
2011/10/19	0.1a	J. Spörndli	1st 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	0.1g	J. Weber	Updates of 0.1e approved. Additional updates included

Management summary

The current CP/CPS describes in sufficient detail how Swiss Government's 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's PKI in the FOITT to act as the trust basis for its subordinated CAs (presently just one CA - Swiss Government's Regular CA 01) issuing end user certificates to be used primarily for authentication and, in some environments, also for encryption 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's Root CA I), the certificates are issued and used as soft tokens.
- Swiss Government Regular CA 01 issues certificates for machines (servers) operated by the administration to ensure authenticity and privacy of the data accessed there. Certificates are also issued to persons within the administration having a need to access protected data or to encrypt their e-mail exchanges. Employees of companies interacting electronically with their partners in the administration regularly may also get issued certificates.
- The different types of certificates issued are: machine certificates (e.g. SSL server certificates), certificates for encryption with shared mailboxes, Sedex and e-Dec authentication certificates and code signing certificates.
- To ensure the appropriate level of trust in the certificates, there is a strict registration process followed: Requests for certificates are acceptable only if the requester's identity is confirmed by a matching Entry in Admin Directory, and each request must be approved by Registration Agents authorized by the management of the department. Similarly, requests for machine certificates are exclusively accepted by the CA in case the Registration Agent submitting the request has been authorized accordingly by the owner of the domain name(s) to be certified
- Certificates issued are valid for two years then the certificate holders have to request a re-key of their certificates 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's PKI staff must initiate the revocation process to invalidate the certificates concerned.
- Encryption certificates are published by the CA to appropriate directories (e.g. Admin Directory) to enable e-mail originators to find the public encryption keys of the addressees.
- The high security of CA operation and certificate issuance is guaranteed by employing specialized and permanently re-trained staff for the purpose, by operating the exposed hardware in specially protected, permanently supervised environments and by regular audits.
- Each party concerned bears its own costs, there are no charges payable – neither for the CA's services nor for the contribution of the individual departments supporting registration for or publication or certificates.
- Swiss Federal Department of Finance (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 frame contract with Swiss Government's PKI.

Table of Contents

1 Introduction 9
1.1 Overview 9
1.2 Document name and identification 10
1.3 PKI participants 11
1.3.1 Certification authorities 11
1.3.2 Registration authorities 13
1.3.3 Subscribers 13
1.3.4 Relying parties 14
1.3.5 Other participants 14
1.4 Certificate Usage 14
1.4.1 Appropriate certificate uses 14
1.4.2 Prohibited certificate uses 15
1.5 Policy administration 15
1.5.1 Organization administering the document 15
1.5.2 Contact person 15
1.5.3 Person determining CPS suitability for the policy 15
1.5.4 CPS approval procedures 15
1.6 Definitions and acronyms 16

2 Publication and Repository Responsibilities 18
2.1 Repositories 18
2.2 Publication of certification information 18
2.3 Time or frequency of publication 18
2.4 Access controls on repositories 18

3 Identification and Authentication 19
3.1 Naming 19
3.1.1 Types of names 19
3.1.2 Need for names to be meaningful 19
3.1.3 Anonymity or pseudonymity of subscribers 19
3.1.4 Rules for interpreting various name forms 19
3.1.5 Uniqueness of names 20
3.1.6 Recognition, authentication, and role of trademarks 20
3.2 Initial identity validation 20
3.2.1 Method to prove possession of private key 20
3.2.2 Authentication of organization identity 20
3.2.3 Authentication of individual identity 20
3.2.4 Non-verified subscriber information 21
3.2.5 Validation of authority 21
3.2.6 Criteria for interoperation 21
3.3 Identification and authentication for re-key requests 21
3.3.1 Identification and authentication for routine re-key 21
3.3.2 Identification and authentication for re-key after revocation 21
3.4 Identification and authentication for revocation request 21

4 Certificate Life-Cycle Operational Requirements 23
4.1 Certificate application 23
4.1.1 Who may submit a certificate application 23
4.1.2 Enrollment process and responsibilities 23
4.2 Certificate application processing 25
4.2.1 Performing identification and authentication functions 25
4.2.2 Approval or rejection of certificate applications 25
4.2.3 Time to process certificate applications 26
4.3 Certificate issuance 26
4.3.1 CA actions during certificate issuance 26

4.3.2 Notification to subscriber by the CA of issuance of certificate 26
4.4 Certificate acceptance 26
4.4.1 Conduct constituting certificate acceptance 26
4.4.2 Publication of the certificate by the CA 27
4.4.3 Notification of certificate issuance by the CA to other entities 27
4.5 Key pair and certificate security rules 27
4.5.1 Subscriber private key and certificate usage 27
4.5.2 Relying party public key and certificate usage 27
4.6 Certificate renewal 28
4.7 Certificate re-key 28
4.7.1 Circumstance for certificate re-key 28
4.7.2 Who may request certification of a new public key 28
4.7.3 Processing certificate re-keying requests 28
4.7.4 Notification of new certificate issuance to subscriber 28
4.7.5 Conduct constituting acceptance of a re-keyed certificate 28
4.7.6 Publication of the re-keyed certificate by the CA 28
4.7.7 Notification of certificate issuance by the CA to other entities 28
4.8 Certificate modification 29
4.9 Certificate revocation and suspension 29
4.9.1 Circumstances for revocation 29
4.9.2 Who can request revocation 29
4.9.3 Procedure for revocation request 29
4.9.4 Revocation request grace period 30
4.9.5 Time within which CA must process the revocation request 30
4.9.6 Revocation checking requirement for relying parties 30
4.9.7 CRL issuance frequency 30
4.9.8 Maximum latency for CRLs 30
4.9.9 On-line revocation/status checking availability 30
4.9.10 On-line revocation checking requirements 30
4.9.11 Other forms of revocation advertisements available 31
4.9.12 Special requirements re key compromise 31
4.9.13 Circumstances for suspension 31
4.9.14 Who can request suspension 31
4.9.15 Procedure for suspension request 31
4.9.16 Limits on suspension period 31
4.10 Certificate status services 31
4.10.1 Operational characteristics 31
4.10.2 Service availability 31
4.10.3 Optional features 31
4.11 End of subscription 32
4.12 Key escrow and recovery 32
4.12.1 Key escrow and recovery policy and practices 32
4.12.2 Session key encapsulation and recovery policy and practices 32
5 Management, Operational, and Physical Controls 33
5.1 Physical Controls 33
5.1.1 Site location and construction 33
5.1.2 Physical access 33
5.1.3 Power and air conditioning 33
5.1.4 Water exposures 33
5.1.5 Fire prevention and protection 33
5.1.6 Media storage 33
5.1.7 Waste disposal 34
5.1.8 Off-site backup 34
5.2 Procedural Controls and System Access Management 34
5.2.1 Trusted roles 34
5.2.2 Number of persons required per task 35
5.2.3 Identification and authentication for each role 35

5.2.4 Roles requiring separation of duties 36
5.3 Personnel Controls 36
5.3.1 Qualifications, experience and clearance requirements 36
5.3.2 Background check procedures 36
5.3.3 Training requirements 36
5.3.4 Retraining frequency and requirements 36
5.3.5 Job rotation frequency and sequence 36
5.3.6 Sanctions for unauthorized actions 37
5.3.7 Independent contractor requirements 37
5.3.8 Documentation supplied to personnel 37
5.4 Audit Logging Procedures 37
5.4.1 Types of events recorded 37
5.4.2 Frequency of processing log 37
5.4.3 Retention period for audit log 37
5.4.4 Protection of audit log 37
5.4.5 Audit log backup procedures 38
5.4.6 Audit collection system 38
5.4.7 Notification to event-causing subject 38
5.4.8 Vulnerability assessments 38
5.5 Records Archival Procedures 38
5.5.1 Types of records archived 38
5.5.2 Retention period for archive 38
5.5.3 Protection of archive 38
5.5.4 Archive backup procedures 39
5.5.5 Requirements for time-stamping of records 39
5.5.6 Procedures to obtain and verify archive information 39
5.5.7 Archive collection system 39
5.6 Key Changeover 39
5.7 Compromise and Disaster Recovery 39
5.7.1 Incident and compromise handling procedures 39
5.7.2 Computer resources, software and/or data are corrupted 39
5.7.3 Entity private key compromise procedures 40
5.7.4 Business continuity capabilities after a disaster 40
5.8 CA or RA termination 40
5.8.1 Termination of Swiss Government's PKI 40
5.8.2 Termination of a certificate using application 41

6 Technical Security Controls 42
6.1 Key pair generation and installation 42
6.1.1 Key pair generation 42
6.1.2 Private key delivery to subscriber 42
6.1.3 Public key delivery to certificate issuer 42
6.1.4 CA public key delivery to relying parties 42
6.1.5 Key sizes 42
6.1.6 Public key parameters generation and quality checking 42
6.1.7 Key usage purposes 43
6.2 Private key protection and cryptographic module engineering controls 43
6.2.1 Cryptographic module standards and controls 43
6.2.2 Private key (n out of m) multi-person control 43
6.2.3 Private key escrow 43
6.2.4 Private key backup 43
6.2.5 Private key archival 43
6.2.6 Private key transfer into or from a cryptographic module 43
6.2.7 Private key storage on cryptographic module 44
6.2.8 Method of activating private key 44
6.2.9 Method of deactivating private key 44
6.2.10 Method of destroying private key 44
6.2.11 Cryptographic module rating 44

6.3 Other aspects of key pair management 44
6.3.1 Public key archival 44
6.3.2 Certificate operational periods and key pair usage period 44
6.4 Activation data 45
6.4.1 Activation data generation and installation 45
6.4.2 Activation data protection 45
6.4.3 Other aspects of activation data 45
6.5 Computer security controls 46
6.5.1 Specific computer security technical requirements 46
6.5.2 Computer security rating 46
6.6 Life cycle technical controls 46
6.6.1 System development control 46
6.6.2 Security management controls 46
6.6.3 Life cycle security controls 46
6.7 Network security controls 46
6.8 Time-stamping 47

7 Certificate, CRL and OCSP Profiles 48
7.1 Certificate profile 48
7.1.1 Version number(s) 48
7.1.2 Certificate extensions 48
7.1.3 Algorithm object identifiers 49
7.1.4 Name forms 49
7.1.5 Name constraints 50
7.1.6 Certificate policy object identifier 50
7.1.7 Usage of policy constraints extension 50
7.1.8 Policy qualifiers syntax and semantics 50
7.1.9 Processing semantics for the critical certificate policies extension 50
7.2 CRL profile 50
7.2.1 Version number(s) 50
7.2.2 CRL and CRL entry extensions 50
7.3 OCSP profile 51

8 Compliance Audit and other Assessments 52
8.1 Frequency or circumstances of assessment 52
8.2 Identity/qualifications of assessor 52
8.3 Assessor's relationship to assessed entity 52
8.4 Topics covered by assessment 52
8.5 Actions taken as a result of deficiency 52
8.6 Communication of results 52

9 Other Business and Legal Matters 53
9.1 Fees 53
9.2 Financial responsibility 53
9.2.1 Insurance coverage 53
9.2.2 Other assets 53
9.2.3 Insurance or warranty coverage for end-entities 53
9.3 Confidentiality of business information 53
9.3.1 Scope of confidential information 53
9.3.2 Information not within the scope of confidential information 54
9.3.3 Responsibility to protect confidential information 54
9.4 Privacy of personal information 54
9.5 Intellectual property rights 54
9.6 Representations and warranties 54
9.6.1 CA representations and warranties 54
9.6.2 RA representations and warranties 55
9.6.3 Subscriber representations and warranties 55
9.6.4 Relying party representations and warranties 55
9.6.5 Representations and warranties of other participants 55

9.7 Disclaimers of warranties 55
9.8 Limitations of liability 55
9.8.1 Swiss Government's PKI limitation of liability 55
9.8.2 Registration Agent limitation of liability 55
9.8.3 Subscriber limitation of liability 56
9.9 Indemnities 56
9.10 Term and termination 56
9.10.1 Term 56
9.10.2 Termination 56
9.10.3 Effect of termination and survival 56
9.11 Individual notices and communications with participants 56
9.12 Amendments 56
9.13 Dispute resolution provisions 57
9.14 Governing law 57
9.15 Compliance with applicable law 57
9.16 Miscellaneous provisions 57
9.17 Other provisions 57
9.17.1 Legally binding version of CP/CPS 57
10 Annexes 58
10.1 Annex A – References 58

1 Introduction

1.1 Overview

Swiss Government's 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 PKI comprises two different two-level hierarchies of CAs to cater for the many different needs:

- A group of CAs responsible for qualified and enhanced certificates, i.e. issuing qualified and enhanced certificates according to the federal administrations' terminology (see: http://www.bit.admin.ch/adminpki/00247/index.html?lang=de). 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 and servers etc. These certificates are issued as soft-tokens.

The current document concentrates on the second group, i.e. on CAs supporting regular certificates. These CAs are:

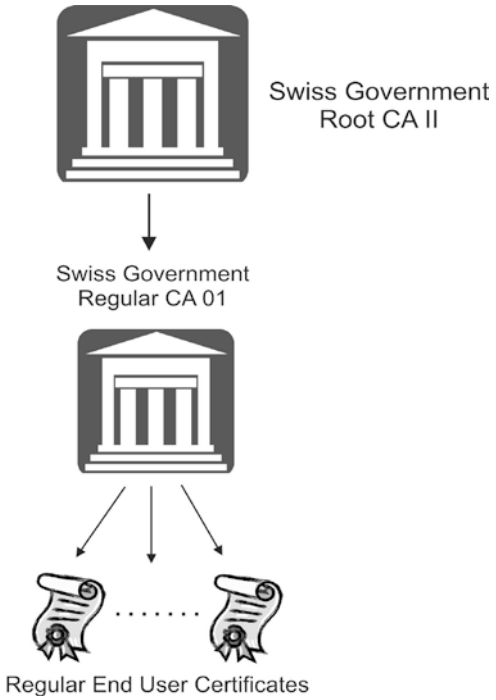

Figure 1.1 - CA hierarchy 'Swiss Government Root CA II'

Swiss Government 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's PKI to easily add additional subor-

dinated 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.).

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

- It details the policies governing and practices followed by the Root CA's issuance of CA certificates for the subordinated CAs, i.e. it is certificate policy [CP] and certificate practices statement [CPS] for the Swiss Government 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 regular certificates to end-users as well.

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

1.2 Document name and identification

This document is entitled 'Certificate Policy and Practice Statement of the Swiss Government Root CA II' and is identified the object identifier (OID) **2.16.756.1.17.3.21.1** whose components have the meaning given in Table 1.

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	Swiss Government Root CA II
1	CP/CPS

Table 1.1: CP-OID of Swiss Government Root CA II

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

1.3 PKI participants

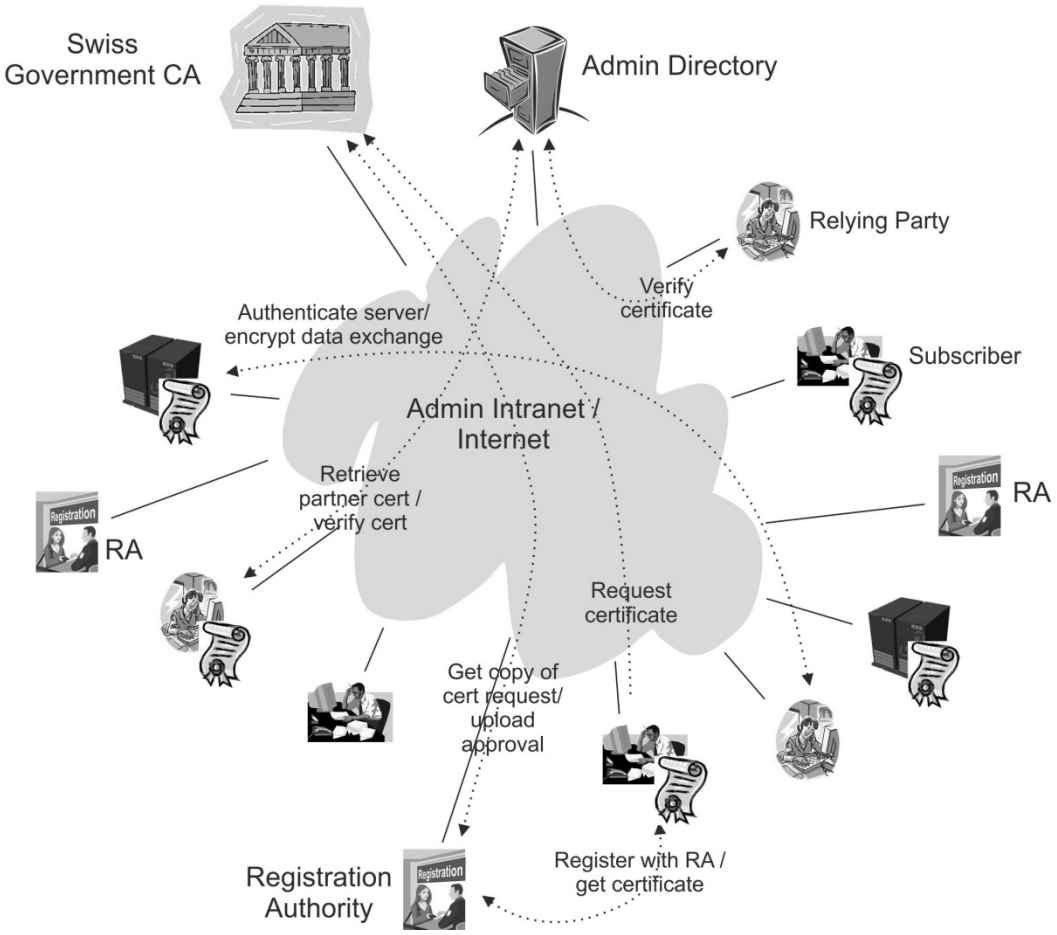

Figure 1.2 – Overview of PKI participants

1.3.1 Certification authorities

Swiss Government 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 administration.

Swiss Government 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.

Swiss Government Root CA II is operated by Swiss Government's PKI staff appointed to the task, responsible the PKI Manager.

Swiss Government subordinated CAs

Presently there is one second level CA subordinated to Swiss Government Root CA II, issuing end-user certificates exclusively:

- *Swiss Government Regular CA 01* issuing 'regular' certificates[2] to be used for authentication, signing and encryption.

The regular certificates issued presently are grouped as follows:

- 'Machine certificates' issued for Web-servers, servers and network components operated by administrative bodies to support SSL (including SAN- and wildcard-certificates).
- '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) as well as to external organizations to support Sedex (primarily intended for ensuring traceability).
- 'e-Dec certificates' – authentication certificates issued to employees of companies/organizations using the electronic goods declaration in their transactions with the Federal Customs Administration.
- '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.

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 usages a certificate is intended for are explicitly signaled in the 'key usages' field.

The tasks of Swiss Government Regular CA 01 are:

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

The Swiss government subordinated CAs are operated by Swiss Government's PKI staff appointed to the task, responsible the PKI Manager.

[2] These certificates replace the 'class C-Trustcenter' and 'class D' certificates issued by the predecessors of Regular CA 01.

1.3.2 Registration authorities

To cope with the variety of certificates issued by Swiss Government Regular CA 01, 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 communicated to Swiss Government's PKI either directly or through entries in suitable directories operated by the Federal Administration. Swiss Government's 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) tasks[3] 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 Swiss Government Regular CA 01.
- Generate and submit re-key requests.
- Verify and approve re-key requests.
- Generate and submit revocation requests.
- Verify and approve revocation requests.

With all institutes a list of Registration Agents in charge of these tasks is maintained by the respective head of institute.

1.3.3 Subscribers

Subscribers are natural persons, administrative units or legal entities holding regular certificates issued by Swiss Government Regular CA 01. These subscribers are

- System Administrators representing machines.
- 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 Admin-Directory.
- 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/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 applications (see section 1.4).

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

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. owners of end-user certificates issued by Swiss Government Regular CA 01.
- 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

There aren’t any other participants involved.

1.4 Certificate Usage

The issuance, distribution and usage of all certificates issued by the *Swiss Government Regular CA 01* MUST comply with this CP/CPS.

1.4.1 Appropriate certificate uses

The usage of keys certified by Swiss Government Root CA II or one of its subordinated CAs is restricted as per the following table:

Entity	Private key usage	Certificate usage
Swiss Government root CA II	▪ Sign certificates for subordinated certification authorities ▪ Sign ARLs (Authority Revocation Lists)	▪ Validate end-user/machine certificates chaining back to Swiss Government Root CA II
Swiss Government Regular CA 01	▪ Sign regular certificates ▪ Sign CRLs (Certificate Revocation Lists)	▪ Validate regular certificates
Subscriber	▪ Sign, authenticate or decrypt documents/data depending on type of certificate	▪ Use other subscribers’ public keys for encrypting documents/data
Subscriber (Machine)	▪ Authentication	▪ Chaining back to Swiss Government Root CA II

Entity	Private key usage	Certificate usage
Relying Party	▪ not applicable	▪ Verify electronic signatures ▪ Verify authenticity of certificate holder ▪ Use subscribers' public keys for encrypting documents/data

Table 1.1 – Authorized usage of private keys and certificates

End-user certificates issued by Swiss Government Regular CA 01 as well as the corresponding keys may be used exclusively in conjunction with applications approved for the purpose by Swiss Government's PKI.

1.4.2 Prohibited certificate uses

Swiss Government Regular CA 01 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
BTR – BFS - BFK
74, Monbijoustrasse
3003 Berne
Switzerland

1.5.3 Person determining CPS suitability for the policy

The PKI Manager and the PKI Security Officer 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
ARL	Authority Revocation List	A list of revoked Certification Authority certificates.
CA	Certification Authority	An entity that issues certificates.
CP	Certificate Policy	A named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements.
CPS	Certificate Practice Statement	A statement of the practices that a CA employs in issuing, managing, revoking and renewing or re-keying certificates.
CRL	Certificate Revocation List	A list of revoked certificates.
DN	Distinguished Name	
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.
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	
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 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.

Term / Acronym	Full text	Explanation
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's PKI		FOITT staff responsible for and operating all PKI services provided by the Swiss Authorities.

Table 2.1 – Definitions and Acronyms

2 Publication and Repository Responsibilities

2.1 Repositories

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

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

2.2 Publication of certification information

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

- certificate(s) of the Swiss Government Root CA II.
- fingerprint of the certificate of the Swiss Government Root CA II.
- 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 Swiss Government Root CA II.
- the certificate revocation list (CRL) for the Swiss Government Root CA II and its subordinated certification authorities.
- the current version of the CP/CPS for the Swiss Government Root CA II and its subordinated certification authorities.

2.3 Time or frequency of publication

Directory services update data on encryption certificates several times per hour and publishes updated CRLs das these are available (see below).

Swiss Government Root CA II updates its ARL at least once a year and immediately after revoking a subordinated certification authority's certificate.

Swiss Government Regular CA 01 updates its CRLs daily in four hour intervalsduring office hours.

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. Admin-Directory to all users of the intranet of the federal administration and the public version of the Admin-Directory to all Internet users.

3 Identification and Authentication

Unless it is explicitly stated, this section concentrates on the identification and authentication of subscribers, i.e. applicants for and holders of regular 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 Swiss Government's PKI personnel specifically appointed to the tasks, the identities and roles have already been well established and the authentication can be based on enhanced personal certificates (i.e. hard-token certificates).

3.1 Naming

3.1.1 Types of names

With all certificates issued the issuer (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 technical directive on Admin-Directory by the Federal Strategy Unit for IT [ref. 4].

Swiss Government 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, or
- a natural person as representative of a company or organization.
- a machine as representative of a web server, server or network component.

3.1.3 Anonymity or pseudonymity of subscribers

The CAs subordinated to Swiss Government Root CA II don't support anonymity or pseudonymity with the certificates they issue.

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

- Names in regular certificates must be unique. In case an applicant's distinguished name should duplicate the DN of an existing subscriber, the Registration Agent invokes Swiss Government's PKI to resolve the conflict.

3.1.6 Recognition, authentication, and role of trademarks

Not relevant. Regular certificates don't convey any data related to trademarks.

3.2 Initial identity validation

3.2.1 Method to prove possession of private key

The applications initiating a certificate request on behalf of the subscribers (individual users, server administrators etc.) also generate a key pair. By signing the public key with the private key and adding the result to the request data, they provide proof of possession of private key.

3.2.2 Authentication of organization identity

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

Private companies/organizations are authenticated by the administrative units having authorized them for getting issued Swiss Government's PKI certificates (see 4.1.1).

3.2.3 Authentication of individual identity

With applications for machine certificate Swiss Government's PKI ensures the requests and the data therein are authentic in the following way:

- Machine certificates are issued exclusively for domains owned by the federal or a cantonal or communal administration.
- Swiss Govnerment's Regular CA 01 does explicitly not issue certificates for identifying servers not visible to Internet's DNS i.e. using any of the following identifiers
  . host names
  . 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 machine certificates identifying the respective domains. Swiss Government's 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 machine certificate, the authorization of the requester and the validity of the domain(s) to be identified are verified per the above list.
- E-mail addresses to be added to machine certificates are validated by Swiss Government's PKI staff through a challenge/response procedure.
- Requests for domains not supported by the list or not in compliance with the estab-

lished guidelines for SAN-certificates undergo an exceptional process 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 an oral or e-mail statement of the domain owner identified.

Applicants for regular personal certificates are authenticated by means of the corresponding entries in Admin-Directory. As Admin-Directory 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 Admin-Directory, 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

The parties registering certificate requests verify all data necessary for identifying an applicant and the administrative unit or organization he may represent. With requests for machine certificates they also verify the domain names to be signaled in the certificates (see 3.2.3). They don't do any other verifications with requests for certificates.

3.2.5 Validation of authority

Swiss Government's 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 Swiss Government's PKI either verifies the function has been formally assigned in the appropriate directory or consults with the management of the administrative unit concerned (see section 4.1.2).

3.2.6 Criteria for interoperation

Not applicable. Swiss Government's Regular CA 01 must not interoperate with any other PKIs.

3.3 Identification and authentication for re-key requests

3.3.1 Identification and authentication for routine re-key

For re-keying regular 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 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,
- sending the revocation request by mail to a Registration Agent,
- sending the revocation request by e-mail, signed with the signature key, to a Registration Agent.

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

4 Certificate Life-Cycle Operational Requirements

This section details all requirements for regular end-user 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 Swiss Government's 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 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 Swiss Government Regular CA 01 together with the responsible parties are:

Step	Description	Responsible
Apply for machine certificate (SSL, SAN or wildcard certificate)	1. Server administrator submits electronic certificate request generated by server through registration application, together with request form specifying the domain names to be confirmed by the certificate.	Server administrator authorized by IT management of department concerned
Register applicant and domain names, approve request	2. Verify server administrator's authority and correctness of request. 3. Verify ownership of domain(s). 4. Verify request from domain angle and, if correct, approve in registration application.	PKI Order Management PKI Security OfficerDomain Owner or delegate
Issue certificate	5. Issue certificate on basis of request, generate soft-token and download to server / send to server administrator.	Registration application / CA (processes run automatically)

Table 4.1 – Registration Process and Responsibilities for machine certificates

Step	Description	Responsible
Apply for regular 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 ap-	2. Approve request through reg-	Registration agent or his deputy

prove application	istration application.	
Issue certificate	3. Issue certificate on basis of request, generate soft-token and send to applicant.	Registration application / CA (processes run automatically)

Table 4.2 – Registration Process and Responsibilities for shared mailbox certificates

Step	**Description**	**Responsible**
Apply for regular 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
Issue certificate	3. Issue certificate on basis of request, generate soft-token and send to applicant.	Registration application / CA (processes run automatically)

Table 4.3 – Registration Process and Responsibilities for organization certificates (to be used in conjunction with Sedex)

Step	Description	Responsible
Apply for regular 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 Admin-Directory.	Registration application
Issue certificate	3. Issue certificate on basis of request, generate soft-token and download to FCA application.	Registration application / CA (processes run automatically)

Table 4.4 – Registration Process and Responsibilities for e-Dec certificates

Step	**Description**	**Responsible**
Apply for regular certificate	1. Registration agent – the intended certificate owner with code signing certificates - generates and submits request through registration application.	Registration agent formally authorized by the head of the administrative body asking for the certificate and listed accordingly with Swiss Government's PKI
Register and approve application	2. Identify Registration Agent face-to-face on the basis of a passport/identity card. 3. Verify Registration Agent's authority. 4. Approve request.	PKI Security Officer
Issue certificate	5. Issue certificate for requester	Registration application / CA

		(processes run automatically)
	6. Generate soft-token and hand personally to requester.	PKI Security Officer

Table 4.5 – Registration Process and Responsibilities for code signing certificates

4.2 Certificate application processing

4.2.1 Performing identification and authentication functions

Swiss Government's PKI identifies Registration Agents authorized by the management of the administrative units having a need for certificates just initially and authorizes them to access its provisioning platform (or the application run by FCA) for requesting and downloading certificates[4]. The platform (or the FCA application) then authenticate the agents with each certificate request they issue.

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

4.2.2 Approval or rejection of certificate applications

Certificate type requested	Condition for approval	Responsible
Machine certificate general	1. Request formally correct and complete 2. Request submitted by authorized Registration Agent (a server administrator) 3. Domain names are within the range assigned to the requesting Registration Agent (see 3.2.3)	PKI Security Officer
Machine certificates for wildcards and/or SAN	1. Request formally correct and complete 2. Request submitted by authorized Registration Agent 3. Domain owner identified face-to-face on basis of passport/identity card	PKI Security Officer
Certificate for shared mailbox	Request formally correct and complete	Registration agent
Organization certificate	Request formally correct and complete	Registration agent

[4] Server administrators acting as registration agents for machine certificates must be identified face-to-face on the basis of a formal identity document.

e-Dec certificate	1. Request formally correct and complete 2. Subject DN (i.e. of company to be certified) is listed in Admin-Directory	Registration agent
Code signing certificate	1. Request formally correct and complete 2. Request submitted personally by authorized agent of requesting administrative unit	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 Swiss Government's PKI.

4.2.3 Time to process certificate applications

Certificate applications are processed instantaneously once the requests have been formally approved. Consequently, certificates are issued within minutes after the approval of a request.

4.3 Certificate issuance

4.3.1 CA actions during certificate issuance

Swiss Government Regular CA 01 issues certificates on-line, i.e. once a valid request has been approved the CA automatically issues the certificate asked for. The CA delivers the certificate tokens to the requesting parties either by mail (e.g. machine certificate tokens) or by download to the requesting application, except code signing certificates: these 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

Swiss Government Regular CA 01 notifies 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

Swiss Government's 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 CA.

4.4.2 Publication of the certificate by the CA

Of the certificates issued by Swiss Government Regular CA 01, e-Dec- and code signing certificates are published in Admin-Directory, accessible to employees of the federal administration.

Organization certificates to be used for Sedex are published in the Sedex user directory (OSCITV, not generally accessible within the administration).

Machine certificates are not published.

e-Dec certificates are published in Admin-Directory.

4.4.3 Notification of certificate issuance by the CA to other entities

Other entities are not actively notified of certificate issuance by Swiss Government Regular CA 01. 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 indicated 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.

4.6 Certificate renewal

Certificate renewal is not supported by Swiss Government Regular CA 01. 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

Regular certificates 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

Swiss Government Regular CA 01 doesn't' 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

Re-keyed regular Organization certificates used in Sedex, e-Dec and code signing certificates are published in the same way as 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 frame contract and concluded the agreement with Swiss Government's PKI have access to Swiss Govern-

ment's PKI's reporting. From there they can retrieve data on re-keyed certificates.

4.8 Certificate modification

Swiss Government Regular CA 01 doesn't 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

Regular certificates must be revoked under the following circumstances:

- A compromise of private key or password of a soft-token is suspected or has actually happened.
- A certificate token has been erased.
- Parts of the data in a certificate are obsolete.
- 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.
- Swiss Government Regular CA 01 ceases its operation.

4.9.2 Who can request revocation

Requests for revoking certificates can be requested by:

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

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

4.9.3 Procedure for revocation request

The procedure for revoking regular certificates 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 Swiss Government Regular CA 01.

- The CA processes the revocation request automatically and instantaneously. It then informs the Registration Agent on the completed revocation.
- ~~Finally, the AP investigates the reasons leading to the need for revocation, e.g. why a key has been compromised, what rules the certificate holder has violated and why, etc. The AP feeds its findings to a database run by Swiss Government's PKI for the purpose.~~

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

Swiss Government Regular CA 01 revokes 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-Directory 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 CRL issued by Swiss Government Regular CA 01 at the moment they verify a signature on the basis of a Swiss Government's PKI certificate.

4.9.7 CRL issuance frequency

Swiss Government Regular CA 01 issues and publishes updated CRLs every four hours during office hours (see 2.3).

Swiss Government 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 Root CA 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 Admin-Directory and via http://www.pki.admin.ch within maximally 24h.

4.9.9 On-line revocation/status checking availability

Swiss Government's PKI doesn't offer any on-line revocation/status checking services for regular certificates, e.g. an on-line certificate status protocol (OCSP).

4.9.10 On-line revocation checking requirements

Relying parties are not requested to do on-line revocation checking when validating regular

certificates.

4.9.11 Other forms of revocation advertisements available

Beside the publication of CRLs in Admin-Directory 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.

4.9.13 Circumstances for suspension

Swiss Government's PKI doesn't support suspension with regular certificates.

4.9.14 Who can request suspension

Not applicable (see 4.9.13).

4.9.15 Procedure for suspension request

Not applicable (see 4.9.13).

4.9.16 Limits on suspension period

Not applicable (see 4.9.13).

4.10 Certificate status services

4.10.1 Operational characteristics

The service for verifying certificates' status is strictly confined to the issuance and publication of CRLs by Swiss Government Regular CA 01. The CRLs list the serial nos. of all revoked certificates issued by the CA which haven't expired yet. The CRLs are published in Admin-Directory and via http://www.pki.admin.ch (see 2.1).

4.10.2 Service availability

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

4.10.3 Optional features

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

4.11 End of subscription

The end of subscription is specified in the frame contract agreed between subscribers and Swiss Government's PKI.

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's PKI.. The encryption 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 Swiss Government's 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

Swiss Government's PKI doesn't support session key encapsulation and recovery with regular keys/certificates.

5 Management, Operational, and Physical Controls

5.1 Physical Controls

5.1.1 Site location and construction

Swiss Government's 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 Swiss Government's PKI's access control directive [ref. 7].

Only persons possessing a badge issued by FOITT security administration can enter the secured location with Swiss Government's PKI's IT hardware. Access to the location is prohibited for all other persons unless accompanied by an authorized Swiss Government's 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 specifically run for the secured location ensures constant temperature and humidity 7x24h.

5.1.4 Water exposures

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

5.1.5 Fire prevention and protection

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

5.1.6 Media storage

Not applicable, data related to the certification infrastructure is backed up in specific servers exclusively (see 5.1.8).

5.1.7 Waste disposal

Swiss Government's 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

Swiss Government's PKI disposes of a backup-site from where certification can be upheld in case of an emergency.

Swiss Government's 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, Swiss Government's 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 Swiss Government's PKI in the FOITT directorate and is the primary responsible for Swiss Government's 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 Swiss Government's PKI's services. His tasks include participating in the strategic planning, maintaining relations with clients and providers and managing Swiss Government's PKI personnel.

- **PKI Engineer**

  The PKI Engineer of Swiss Government's PKI is responsible for the technical support and the improvement of Swiss Government's 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 Swiss Government's PKI possesses the latest software versions and has these installed where appropriate. Finally, he sees also to the maintenance of the configuration management database CMDB and the standard on the usage of certificate tokens by subscribers (A006).

- **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 Swiss Government's PKI and its environment. He manages the physical access control to the certification platform. The security officer is the only one entitled to access and read archives

and analyze activity logs.

- **Operating Team**

  The Operating Team is responsible for the running all services delivered by Swiss Government's PKI. In particular, its tasks are maintaining support contracts with suppliers, ensure the availability of the certification infrastructure and co-ordinate Swiss Government's 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 Swiss Government's 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 Swiss Government's PKI's website http://www.pki.admin.ch and answers client's questions addressed to pki-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 Swiss Government's PKI with this certificate policy and practice statement and Swiss Government's 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 Swiss Government's PKI staff by their superiors to support certificate issuance for the department or the organization concerned. Registration agents get authorized by Swiss Government's 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

Swiss Government's 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 Swiss Government's 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

Swiss Government Root CA II and its subordinated CA 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 Swiss Government's PKI role, Swiss Government's PKI staff are subjected to a security review as per the ordinance on security checks for persons [ref. 8].

5.3.3 Training requirements

Swiss Government's 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 Swiss Government's 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 Swiss Government's 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 Swiss Government's 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 Swiss Government's PKI employees (see 5.3.1, 5.3.2, 5.3.3 and 5.3.4).

5.3.8 Documentation supplied to personnel

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

- Certificate Policy and Certification Practice Statement of the Swiss Government Root CA II (this document).
- Swiss Government's PKI security policy [ref. 10].
- Swiss Government's 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 Swiss Government's 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 Swiss Government's 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 Swiss Government's PKI's routine backup of its host system.

5.4.6 Audit collection system

A dedicated server within Swiss Government's 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 Swiss Government's 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

Swiss Government's 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

Swiss Government's 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 Swiss Government's PKI staff member (four eyes rule).

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 (SAN).

5.6 Key Changeover

Swiss Government Regular CA 01doesn't 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 Swiss Government's PKI staff accordingly.

5.7.2 Computer resources, software and/or data are corrupted

All active keys and certificates used by Swiss Government Root CA II and its subordinated Swiss Government Regular 01 are backed up off-site in at least two security modules at all times. All data related to the issuance and maintenance of end-user certificates is backed up daily as well. Consequently, in case any of Swiss Government's 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 Swiss Government Regular CA 01's key should have been compromised or is suspected to be compromised, Swiss Government's PKI Manager activates the predefined action plan. In particular, this comprises the following steps:

- Informing all subscribers concerned.
- Revoking the CA's certificate (by Swiss Government Root CA II) and publishing an updated ARL.
- Revoking all subscribers' certificates signed by the compromised key.
- 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 Swiss Government's PKI CA certificates as trust anchors and providing them with the necessary updates.

If the key of Swiss Government Root CA II should have been compromised the above measures are carried out for the subordinated Swiss Government CA 01 and all its 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 Swiss Government's PKI's Swiss Government 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's PKI

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

All valid certificates, including Root CA and subordinated CA certificates, will be revoked and a final CRL and ARL published on FOITTs 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] The federal authorities don't plan to hand over their certification services to any other provider in such a situation.

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 – Swiss Government's 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.

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, EAL 4+.

6.1.2 Private key delivery to subscriber

As a standard, private keys to be certified by Swiss Government Regular CA 01 are generated on subscribers' premises and not submitted to the CA at all, private key delivery is thus not necessary.

With some types of certificates issued (e.g. e-Dec certificates) Swiss Government CA 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 personally.

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

Swiss Government's PKI publishes the certificates of Swiss Government Root CA II and its subordinated Swiss Government Regular CA 01

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

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

6.1.5 Key sizes

Swiss Government Root CA II and its subordinated Swiss Government Regular CA 01 use keys of 4096 bits.

Subscribers to Swiss Government Regular CA 01 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, EAL 4+.

6.1.7 Key usage purposes

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

Swiss Government's 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 Swiss Government's 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

Swiss Government's PKI CAs use modules (HSMs) conformant to FIPS 140-2 level 3, EAL 4+ (see also 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 Swiss Government's 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 Swiss Government's PKI which encrypts the key pairs for storage. The server is operated in a secure location and accessible to specifically authorized Swiss Government's PKI staff only.

6.2.4 Private key backup

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

6.2.5 Private key archival

There aren't any private keys archived.

6.2.6 Private key transfer into or from a cryptographic module

Root CA and subordinate CA private keys are transferred between HSMs for backup purposes. The transfers require two Swiss Government's 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 Swiss Government's 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 Swiss Government's PKI staff members authorized for the task beside the PKI Security Officer.

Subscribers' private keys are deactivated when their workstations are closed down.

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 Swiss Government's PKI staff members authorized for the task.

Subscribers' private keys are deleted together with the respective certificate tokens.

6.2.11 Cryptographic module rating

For ratings see section 6.2.1.

6.3 Other aspects of key pair management

6.3.1 Public key archival

All public keys – Root CA's, 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

Swiss Government's PKI certificate validity periods are:

- 24 years with Swiss Government Root CA II.
- 14 years with the subordinated CA.
- 2 years with end-user certificates.

The usage periods for the private signature keys are:

- 10 years with Swiss Government 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 Swiss Government's 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

Swiss Government's 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 Swiss Government's 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

Swiss Government's 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 Swiss Government's PKI staff members for a process to execute.

There is a penetration test performed weekly on Swiss Government's 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

With each development of a new software component, Swiss Government's PKI performs an analysis of the risks this brings about.

Swiss Government's PKI operates a configuration management tool ensuring only approved and tested hard- and software is deployed. With priority Swiss Government's 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

Swiss Government's 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 Swiss Government's PKI's operations.

6.8 Time-stamping

Swiss Government's PKI offers a time-stamping service supporting electronic signing. Swiss Government's PKI operational rules apply likewise for the time-stamping service, for details see the time stamping authority's policy [ref. 13].

7 Certificate, CRL and OCSP Profiles

All certificates and CRLs issued by Swiss Government Root CA II and the subordinated Swiss Government Regular CA 01 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

Unless it is explicitly indicated, certificates issued for Swiss Government Root CA II the subordinated Swiss Government Regular CA 01 and end-users adhere to the identical profile

7.1.1 Version number(s)

Certificates issued by Swiss Government Regular CA 01 are of version 2 in accordance with recommendation X.509 v3.

7.1.2 Certificate extensions

Certificate extensions used with Swiss Government Root CA II's and the subordinated Swiss Government Regular CA 01certificates:

Extension	Objective	Criticality
Authority Key Identifier	Identifies key used by issuer of certificate.	not critical
Subject Key Identifier	Identifies key used by subject of certificate.	not critical
Key Usage	Lists intended usages of private key.	critical
Certificate Policies	Identifies policy governing the operation of the Root CA (the current CP/CPS).	not critical
Basic Constraints	1. Indicates type of certificate subject: CA or end-user (here: CA). 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

Table 7.1 – Root CA and CA certificate extensions

Certificate extensions used with end-user certificates:

Extension	Objective	Criticality
Authority Key Identifier	Identifies key used by issuer of certificate.	not critical
Subject Key Identifier	Identifies key used by subject of certificate (the end-user).	not critical
Key Usage	Lists intended usages of private key.	critical

Extension	Objective	Criticality
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 Swiss Government's 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 Swiss Government's PKI's subscribers.

7.1.4 Name forms

Swiss Government 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)	Admin
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 machine certificate subjects in the following way:

DN Field	Value
Country (c)	CH

Organization (o)	Admin
Organizational Unit (ou)	Weisse Seiten
Common Name (cn)	<name>.[<SLD>].<TLD>

Table 7.5 – Subscriber name forms for machines

7.1.5 Name constraints

Name constraints are not used by Swiss Government's PKI with the issuance of regular certificates.

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

Policy constraints are not used by Swiss Government's PKI with the issuance of regular certificates.

7.1.8 Policy qualifiers syntax and semantics

Policy qualifiers are not used by Swiss Government's PKI with the issuance of regular certificates.

7.1.9 Processing semantics for the critical certificate policies extension

With the issuance of regular certificates the certificate policies extension is set to 'not critical', Swiss Government's PKI doesn't expect relying parties to process policy information electronically.

7.2 CRL profile

7.2.1 Version number(s)

CRLs generated by Swiss Government Regular CA 01 are of version 2 in accordance with recommendation X.509 v3.

7.2.2 CRL and CRL entry extensions

CRL and CRL entry extensions used with Swiss Government 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		

CRL Extension	Objective	Criticality
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

Swiss Government's PKI doesn't offer any OCSP services in conjunction with the regular certificates its CA issues.

8 Compliance Audit and other Assessments

8.1 Frequency or circumstances of assessment

Swiss Government's PKI Root CA II and the subordinated Swiss Government Regular CA 01are 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 Root CA II and Regular CA 01are operated in the identical environment and subject to the identical security requirements as 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 Root CA II and Regular CA 01 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 Swiss Government's 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. Swiss Government's PKI staff, FOITT legal services, etc.

9 Other Business and Legal Matters

9.1 Fees

Swiss Government's PKI's costs for running the certification services basing on Swiss Government Root CA II and the subordinated Swiss Government Regular CA 01are 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 Swiss Government's 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 Swiss Government's 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 Swiss Government's 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).
- Swiss Government's PKI documents intended for subscribers, relying parties and third parties, e.g. this CP/CPS.

9.3.3 Responsibility to protect confidential information

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

All Swiss Government's 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

Swiss Government's PKI is owner of the intellectual property rights of the following documents:

- Certificate Policy and Certification Practice Statement of Swiss Government Root CA II (this document).
- Directives for registration for regular certificates.
- Contracts and other agreements concluded between Swiss Government's PKI and its clients (federal, cantonal and communal administrative units).
- 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 Swiss Government's 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 Swiss Government's PKI, they just obtain the right to used these.

9.6 Representations and warranties

9.6.1 CA representations and warranties

Swiss Government's PKI is committed to provide its services for issuing regular 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 Swiss Government's 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's PKI limitation of liability

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

In particular the Swiss Government PKI is not liable for:

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

9.8.2 Registration Agent's limitation of liability

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

9.8.3 Subscriber limitation of liability

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

9.9 Indemnities

Swiss Government's 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 Swiss Government's 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
- Swiss Government's 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, Swiss Government's 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 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 Swiss Government's 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 Swiss Government 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 Admin-Directory' 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 Swiss Government's PKI

[6] Subscriber agreement with Swiss Government's PKI

[7] Swiss Government's 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] Swiss Government's PKI security policy

[11] Swiss Government's PKI manual on operation and organization

[12] Swiss Government's 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