

SWITCH Certification Authority

Certificate Policy and Certification Practice Statement

DRAFT VERSION 0.3

Document OID: 2.16.756.1.2.6.1.0.3

29 April 2003

Contents

Contents	2
1. INTRODUCTION	7
1.1 Overview	7
1.2 Identification	8
1.3 Community and Applicability	8
1.3.1 Certification authorities	8
1.3.2 Registration authorities	8
1.3.3 End entities	8
1.3.4 Applicability	8
1.4 Contact Details	8
1.4.1 Specification administration organization	8
1.4.2 Contact person	8
1.4.3 Person determining CPS suitability for the policy	9
2. GENERAL PROVISIONS	9
2.1 Obligations	9
2.1.1 CA obligations	9
2.1.2 RA obligations	9
2.1.3 Subject CAs obligations	9
2.1.4 Relying party obligations	9
2.1.5 Repository obligations	10
2.2 Liability	10
2.2.1 CA liability	10
2.2.2 RA liability	10
2.3 Financial responsibility	10
2.3.1 Indemnification by relying parties	10
2.3.2 Fiduciary relationships	10
2.3.3 Administrative processes	10
2.4 Interpretation and Enforcement	10
2.4.1 Governing law	11
2.4.2 Severability, survival, merger, notice	11
2.4.3 Dispute resolution procedures	11
2.5 Fees	11
2.5.1 Certificate issuance or renewal fees	11
2.5.2 Certificate access fees	11
2.5.3 Revocation or status information access fees	11
2.5.4 Fees for other services such as policy information	11
2.5.5 Refund policy	11
2.6 Publication and Repository	11
2.6.1 Publication of CA information	12
2.6.2 Frequency of publication	12
2.6.3 Access controls	12
2.6.4 Repositories	12
2.7 Compliance audit	12
2.7.1 Frequency of entity compliance audit	12
2.7.2 Identity/qualifications of auditor	12

2.7.3 Auditor's relationship to audited party	12
2.7.4 Topics covered by audit	12
2.7.5 Actions taken as a result of deficiency	12
2.7.6 Communication of results	13
2.8 Confidentiality	13
2.8.1 Types of information to be kept confidential	13
2.8.2 Types of information not considered confidential	13
2.8.3 Disclosure of certificate revocation/suspension information	13
2.8.4 Release to law enforcement officials	13
2.8.5 Release as part of civil discovery	13
2.8.6 Disclosure upon owner's request	13
2.8.7 Other information release circumstances	13
2.9 Intellectual Property Rights	13
3. IDENTIFICATION AND AUTHENTICATION	14
3.1 Initial Registration	14
3.1.1 Types of names	14
3.1.2 Need for names to be meaningful	14
3.1.3 Rules for interpreting various name forms	14
3.1.4 Uniqueness of names	14
3.1.5 Name claim dispute resolution procedure	14
3.1.6 Recognition, authentication and role of trademarks	14
3.1.7 Method to prove possession of private key	15
3.1.8 Authentication of organization identity	15
3.1.9 Authentication of individual identity	15
3.2 Routine Rekey	15
3.3 Rekey after Revocation	15
3.4 Revocation Request	15
4. OPERATIONAL REQUIREMENTS	16
4.1 Certificate Application	16
4.1.1 User certificate	16
4.1.2 Host certificate	16
4.2 Certificate Issuance	16
4.2.1 Request approval by a RA	16
4.2.2 Certificate issuance by SWITCH Root CA	16
4.3 Certificate Acceptance	16
4.4 Certificate Suspension and Revocation	16
4.4.1 Circumstances for revocation	16
4.4.2 Who can request revocation	17
4.4.3 Procedure for revocation request	17
4.4.4 Revocation request grace period	17
4.4.5 Circumstances for suspension	17
4.4.6 Who can request suspension	17
4.4.7 Procedure for suspension request	17
4.4.8 Limits on suspension period	17
4.4.9 CRL issuance frequency (if applicable)	17
4.4.10 CRL checking requirements	17
4.4.11 On-line revocation/status checking availability	18

4.4.12 On-line revocation checking requirements.....	18
4.4.13 Other forms of revocation advertisements available	18
4.4.14 Checking requirements for other forms of revocation advertisements.....	18
4.4.15 Special requirements re key compromise.....	18
4.5 Security Audit Procedures	18
4.5.1 Types of event audited	18
4.5.2 Frequency of processing log.....	18
4.5.3 Retention period for audit log.....	18
4.5.4 Protection of audit log.....	18
4.5.5 Audit log backup procedures.....	18
4.5.6 Audit collection system (internal vs external).....	18
4.5.7 Notification to event-causing subject.....	19
4.5.8 Vulnerability assessments	19
4.6 Records Archival.....	19
4.6.1 Types of event recorded.....	19
4.6.2 Retention period for archive.....	19
4.6.3 Protection of archive	19
4.6.4 Archive backup procedures.....	19
4.6.5 Requirements for time-stamping of records.....	19
4.6.6 Archive collection system (internal or external)	19
4.6.7 Procedures to obtain and verify archive information.....	19
4.7 Key changeover.....	20
4.8 Compromise and Disaster Recovery	20
4.8.1 Computing resources, software, and/or data are corrupted.....	20
4.8.2 Entity public key is revoked.....	20
4.8.3 Entity key is compromised.....	20
4.8.4 Secure facility after a natural or other type of disaster	20
4.9 CA Termination.....	20
5. PHYSICAL, PROCEDURAL, AND PERSONNEL SECURITY CONTROLS.....	21
5.1 Physical Controls.....	21
5.1.1 Site location and construction	21
5.1.2 Physical access	21
5.1.3 Power and air conditioning.....	21
5.1.4 Water exposures.....	21
5.1.5 Fire prevention and protection.....	21
5.1.6 Media storage	21
5.1.7 Waste disposal.....	21
5.1.8 Off-site backup	21
5.2 Procedural Controls	21
5.2.1 Trusted roles	21
5.2.2 Number of persons required per task.....	22
5.2.3 Identification and authentication for each role.....	22
5.3 Personnel Controls.....	22
5.3.1 Background, qualifications, experience, and clearance requirements	22
5.3.2 Background check procedures.....	22
5.3.3 Training requirements	22
5.3.4 Retraining frequency and requirements	22

5.3.5 Job rotation frequency and sequence	22
5.3.6 Sanctions for unauthorized actions	22
5.3.7 Contracting personnel requirements	22
5.3.8 Documentation supplied to personnel	22
6. TECHNICAL SECURITY CONTROLS	23
6.1 Key Pair Generation and Installation	23
6.1.1 Key pair generation	23
6.1.2 Private key delivery to entity	23
6.1.3 Public key delivery to certificate issuer	23
6.1.4 CA public key delivery to users	23
6.1.5 Key sizes	23
6.1.6 Public key parameters generation	23
6.1.7 Parameter quality checking	23
6.1.8 Hardware/software key generation	23
6.1.9 Key usage purposes (as per X.509 v3 key usage field)	24
6.2 Private Key Protection	24
6.2.1 Standards for cryptographic module	24
6.2.2 Private key (n out of m) multi-person control	24
6.2.3 Private key escrow	24
6.2.4 Private key backup	24
6.2.5 Private key archival	24
6.2.6 Private key entry into cryptographic module	24
6.2.7 Method of activating private key	24
6.2.8 Method of deactivating private key	24
6.2.9 Method of destroying private key	24
6.3 Other Aspects of Key Pair Management	25
6.3.1 Public key archival	25
6.3.2 Usage periods for the public and private keys	25
6.4 Activation Data	25
6.4.1 Activation data generation and installation	25
6.4.2 Activation data protection	25
6.4.3 Other aspects of activation data	25
6.5 Computer Security Controls	25
6.5.1 Specific computer security technical requirements	25
6.5.2 Computer security rating	25
6.6 Life Cycle Technical Controls	25
6.6.1 System development controls	25
6.6.2 Security management controls	26
6.6.3 Life cycle security ratings	26
6.7 Network Security Controls	26
6.8 Cryptographic Module Engineering Controls	26
7. CERTIFICATE AND CRL PROFILES	26
7.1 Certificate Profile	26
7.1.1 Version number(s)	26
7.1.2 Certificate extensions	26
7.1.3 Algorithm object identifiers	26
7.1.4 Name forms	26

7.1.5 Name constraints27

7.1.6 Certificate policy Object Identifier27

7.1.7 Usage of Policy Constraints extension.....27

7.1.8 Policy qualifiers syntax and semantics27

7.1.9 Processing semantics for the critical certificate policy extension27

7.2 CRL Profile27

 7.2.1 Version number(s)27

 7.2.2 CRL and CRL entry extensions.....27

8. SPECIFICATION ADMINISTRATION27

 8.1 Specification change procedures27

 8.2 Publication and notification policies27

 8.3 CPS approval procedures28

Bibliography28

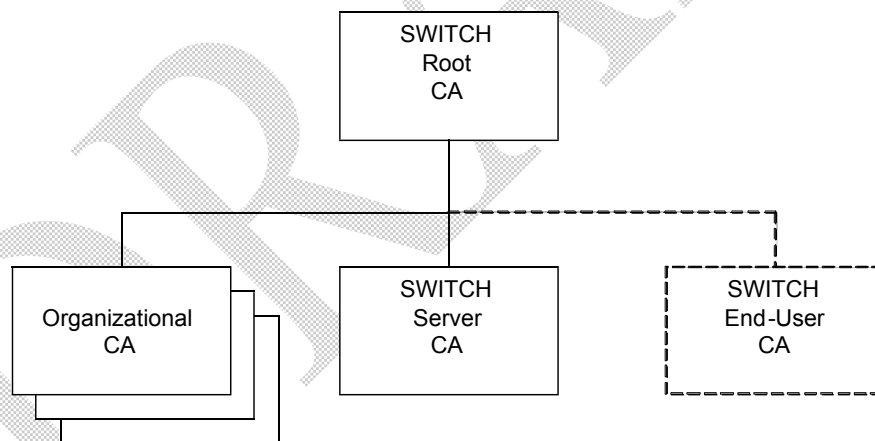
DRAFT

1. INTRODUCTION

1.1 Overview

"SWITCH - The Swiss Education & Research Network" was established as a foundation by the Swiss Confederation and the university cantons. The Berne-based foundation has as its objective "to create, promote and offer the necessary basis for the effective use of modern methods of telecomputing in teaching and research in Switzerland, to be involved in and to support such methods". It is a non-profit foundation that does not pursue commercial aims.

SWITCH offers a broad variety of different services from domain name registration to different network services. One of their latest services is the Authentication and Authorization Infrastructure (AAI) with the goal to simplify inter-organizational access to networked services. In order to provide this and for other services it is necessary for SWITCH to maintain a Root Certificate Authority that accepts subject CAs of three different kinds: Server CAs, Organizational CAs and End-User CAs. The following picture shows the possible CA hierarchy. In a first phase the End-User CA will not be supported by the SWITCH Root CA.



This document is the combined Certificate Policy and Certification Practice Statement (CP/CPS) of the SWITCH Root Certification Authority (SWITCH Root CA). It describes the set of procedures followed by the SWITCH Root CA and is structured according to RFC 2527 [2]. The latter does not form part of this document and only the information provided in this document may be relied on.

1.2 Identification

This document is named *SWITCH Certification Authority Certificate Policy and Certification Practice Statement*. The version is 0.3, dated 29. April 2003. The following ASN.1 Object Identifier (OID) has been assigned to this document: 2.16.756.1.2.6.1.0.3.

(Thomas defines the number and the last two digits represent the version number)

1.3 Community and Applicability

1.3.1 Certification authorities

SWITCH Root CA does issue only certificates to subordinate Certification Authorities. Subject CAs can be any of the following three types:

- Server CA: Certificate Authority that issues only server certificates. Depending on their policies RAs can be supported.
- Organizational CAs can only be members of the Swiss higher education community. These CAs can issue either server certificates and/or end-user certificates according to their policies.
- End-User CA: currently not supported

1.3.2 Registration authorities

Not applicable

1.3.3 End entities

Not applicable

1.3.4 Applicability

The authorised uses of certificates issued by SWITCH Root CA are only for subject CAs. Signing of subject CAs certificates has to be done in accordance with these policies.

The certificates issued by SWITCH Root CA must not be used for financial transactions. Additional exclusions necessary??

1.4 Contact Details

1.4.1 Specification administration organization

The Policy Management Authority (PMA) of SWITCH Root CA is the SWITCH Head office.

1.4.2 Contact person

t.b.d.

1.4.3 Person determining CPS suitability for the policy

The PMA of SWITCH Root CA is responsible for reviewing and approving CPSs.

2. GENERAL PROVISIONS

2.1 Obligations

2.1.1 CA obligations

SWITCH Root CA is solely responsible for the issuance and management of certificates referencing this policy. SWITCH Root CA shall:

- handle certificate requests and issue new certificates :
 - accept and confirm certification requests from entities requesting a certificate according to the procedures described in this document
 - send notification of issued certificates to requesting entities
 - make issued certificates publicly available
- handle certificate revocation requests and certificate revocation :
 - accept and confirm revocation requests from entities requesting that a certificate be revoked according to the procedures described in this document
 - authenticate entities requesting that a certificate be revoked
 - make certificate revocation information publicly available

2.1.2 RA obligations

Not applicable for SWITCH Root CA.

2.1.3 Subject CAs obligations

In requesting a certificate, subject CAs agree to:

- read and adhere to the procedures described in this document
- use the certificate exclusively for authorized and legal purposes, consistent with this policy and their own policy
- by using the authentication procedures described in this document subject CAs accept the restrictions to liability described in section 2.2.
- generate a key pair using a trustworthy method
- take reasonable precautions to prevent any loss, disclosure or unauthorized use of the private key associated with the certificate
- notify SWITCH Root CA immediately in case a private key is lost or compromised

2.1.4 Relying party obligations

In using a certificate issued by the SWITCH Root CA in any system relying parties agree to:

- accept this CP/CPS
- verify the certificate revocation information before validating a certificate
- use the certificates only for the permitted purposes as defined in this document

2.1.5 Repository obligations

SWITCH Root CA maintains an online accessible repository of certificate revocation information. The repository is operated at a best-effort basis, where the intended availability is continuous.

2.2 Liability

2.2.1 CA liability

SWITCH Root CA shall control the identity of the subjects requesting a certificate in accordance with the procedures described in this document. Although it aims to achieve a reasonable level of security, SWITCH Root CA provides its certification services on a best effort basis only and provides no warranties, express or implied, including in respect of security and confidentiality, and of fitness for a particular purpose. SWITCH accepts no liability for or in connection with the certification services and the parties using or relying on them shall hold SWITCH free and harmless from liability resulting from such use or reliance.

2.2.2 RA liability

Not applicable.

2.3 Financial responsibility

See section 2.2.1

2.3.1 Indemnification by relying parties

No stipulation.

2.3.2 Fiduciary relationships

No stipulation.

2.3.3 Administrative processes

No stipulation.

2.4 Interpretation and Enforcement

2.4.1 Governing law

Insofar as any of the conditions stipulated in this document are ambiguous or unclear, exclusive reference shall be had to Swiss law, subject to SWITCH's status as a foundation.

2.4.2 Severability, survival, merger, notice

SWITCH shall be entitled to terminate the certification services at any time. SWITCH Root CA will make all reasonable efforts to notify all its subject CAs, all cross-certifying CAs, and any relying parties known to SWITCH Root CA to be currently and actively relying on certificates issued by SWITCH Root CA on such termination. All certificates issued by SWITCH Root CA that reference this policy will be revoked no later than the time of termination.

2.4.3 Dispute resolution procedures

The PMA shall resolve any disputes associated with the use of the certificates issued by SWITCH Root CA.

2.5 Fees

Fees are charged for any service provided by SWITCH Root CA based on the fee-list for SWITCH Root CA.

2.5.1 Certificate issuance or renewal fees

See section 2.5.

2.5.2 Certificate access fees

See section 2.5.

2.5.3 Revocation or status information access fees

See section 2.5.

2.5.4 Fees for other services such as policy information

See section 2.5.

2.5.5 Refund policy

No stipulation.

2.6 Publication and Repository

2.6.1 Publication of CA information

SWITCH Root CA operates a secure online repository that contains:

- SWITCH Root CA's certificate for its signing key
- a Certificate Revocation List (CRL) signed by SWITCH Root CA
- all past and current versions of this CP/CPSs

2.6.2 Frequency of publication

Certificates are published as soon as issued. The frequency of CRL publication is specified in subsection 4.4.9. New versions of CP/CPSs are published as soon as they have been approved.

2.6.3 Access controls

SWITCH Root CA does not impose any access control on its CP/CPSs and CRLs.

2.6.4 Repositories

A website is maintained by SWITCH Root CA. It contains all the information published by SWITCH Root CA specified in section 2.6.1. The website can be reached at the following address: <http://www.switch.ch/ca>.

2.7 Compliance audit

No external audit will be required, only a self-assessment by SWITCH Root CA that its operation is according to this CP/CPS.

2.7.1 Frequency of entity compliance audit

No stipulation.

2.7.2 Identity/qualifications of auditor

No stipulation.

2.7.3 Auditor's relationship to audited party

No stipulation.

2.7.4 Topics covered by audit

No stipulation.

2.7.5 Actions taken as a result of deficiency

No stipulation.

2.7.6 Communication of results

No stipulation.

2.8 Confidentiality

SWITCH Root CA collects only service specific information provided by the subject CAs beyond their policies.

2.8.1 Types of information to be kept confidential

Under no circumstances does SWITCH Root CA have access to the private keys of any subject CA to whom it issues a certificate.

2.8.2 Types of information not considered confidential

Data contained in the subject CA's certificate, the subject CA's CP/CPS and data contained in CRLs shall not be considered confidential.

2.8.3 Disclosure of certificate revocation/suspension information

No information about the reason for a revocation is published.

2.8.4 Release to law enforcement officials

See section 2.8.2.

2.8.5 Release as part of civil discovery

See section 2.8.2.

2.8.6 Disclosure upon owner's request

SWITCH Root CA does provide only information in accordance with the Swiss Data Protection Law.

2.8.7 Other information release circumstances

See section 2.8.2.

2.9 Intellectual Property Rights

The structure of this CP is according to RFC 2527 [2] with content based on the CERN Certification Authority CP/CPS. This text may be used by others without prior approval. Acknowledgements are welcomed but not required. No copyrights are asserted on issued certificates or certificate revocation lists.

3. IDENTIFICATION AND AUTHENTICATION

3.1 Initial Registration

3.1.1 Types of names

The subject name is a X.500 distinguished name. Apart from this specification no other restrictions apply to any of the following fields: C, O, OU, CN, etc. The subject CAs can use their names or the ones provided by the SWITCH Root CA which are as follows:

- C=CH
- O=SWITCH
- CN=SWITCH Root CA

Organizations using a name under C=CH must have their name registered with OFCOM (<http://www.e-ofcom.ch/>) under RDN (Relative Distinguished Name).

3.1.2 Need for names to be meaningful

For a host/server certificate, the CN must be the fully qualified domain name registered in DNS. In this case it can be an alias (CNAME).

3.1.3 Rules for interpreting various name forms

No stipulation.

3.1.4 Uniqueness of names

The name must be unique for each certificate issued by SWITCH Root CA. If the name presented by the subject CA is not unique, additional numbers or letters are appended to the name to ensure uniqueness.

3.1.5 Name claim dispute resolution procedure

The PMA resolves this kind of dispute. See also section 2.4.3

3.1.6 Recognition, authentication and role of trademarks

No stipulation.

3.1.7 Method to prove possession of private key

Subject CAs must have at least a legal accepted and valid agreement with SWITCH. Apart from this the following procedure has to be executed to prove possession of the private key. It is assumed that members of the organization that wish to have their subject CA certified are known to SWITCH Root CA members and therefore no additional authentication beyond the points mentioned under 3.1.8 are necessary.

- The request sent to the SWITCH Root CA has to be self signed with the subject CA's private key with the public key included (usually the case).
- The hash value (RIPEMD-160) of the request has to be presented personally (face-to-face) by a known member of the demanding party to a PMA member of the SWITCH Root CA.
- Verification of the formal request and the existing agreement with SWITCH by the PMA member.
-
- Further request or ideas?

SWITCH Root CA does not generate the key pair for subject CAs and does not accept or retain private keys generated by subject CAs.

3.1.8 Authentication of organization identity

The same rules apply as for any agreement that is signed for every service provided by SWITCH. The rules for such an agreement can be found in the "Allgemeine Geschäftsbedingungen von SWITCH".

3.1.9 Authentication of individual identity

Not applicable.

3.2 Routine Rekey

Rekeying of certificates follows the same procedures as an initial registration.

3.3 Rekey after Revocation

A public key whose certificate has been revoked shall not be re-certified.

3.4 Revocation Request

Revocation of certificates follows the same procedures as an initial registration.

4. OPERATIONAL REQUIREMENTS

4.1 Certificate Application

4.1.1 User certificate

Not applicable.

4.1.2 Host certificate

Not applicable.

4.2 Certificate Issuance

There are two steps in the issuance process.

4.2.1 Request approval by a RA

Not applicable. No RAs supported.

4.2.2 Certificate issuance by SWITCH Root CA

t.b.d.

4.3 Certificate Acceptance

No stipulation.

4.4 Certificate Suspension and Revocation

4.4.1 Circumstances for revocation

A certificate is revoked when the information it contains is suspected to be incorrect or compromised. This includes situations where:

- the subject CA's private key is lost or suspected to be compromised
- the information in the subject CA's certificate is suspected to be inaccurate
- the subject CA no longer needs the certificate or requests the certificate to be revoked
- the subject CA has violated his/her obligations

4.4.2 Who can request revocation

A certificate revocation can be requested by the holder of the certificate to be revoked or by any other entity presenting evidence of circumstances implying a revocation, as described in section 4.4.1.

4.4.3 Procedure for revocation request

The entity requesting the revocation must authenticate itself in one of the following ways:

- sending a self signed revoke-request, signed by a valid SWITCH Root CA certificate belonging to SWITCH Root CA. It must specify the reason for the revocation request and provide evidence of circumstances implying a revocation, as described in section 4.4.1.
- revocation is only possible for self-owned certificates and follows the same procedure as an initial registration.

4.4.4 Revocation request grace period

SWITCH Root CA handles revocation requests with priority as soon as the request is recognized as such.

4.4.5 Circumstances for suspension

There is no provision for certificate suspension.

4.4.6 Who can request suspension

No stipulation.

4.4.7 Procedure for suspension request

No stipulation.

4.4.8 Limits on suspension period

No stipulation.

4.4.9 CRL issuance frequency (if applicable)

CRLs are issued after every certificate revocation and at least every 35 days.

4.4.10 CRL checking requirements

A relying party must verify a certificate against the most recent CRL issued, in order to validate the use of the certificate.

4.4.11 On-line revocation/status checking availability

SWITCH Root CA does not offer on-line status checking.

4.4.12 On-line revocation checking requirements

No stipulation.

4.4.13 Other forms of revocation advertisements available

No stipulation.

4.4.14 Checking requirements for other forms of revocation advertisements

No stipulation.

4.4.15 Special requirements re key compromise

No stipulation.

4.5 Security Audit Procedures

4.5.1 Types of event audited

No events are audited.

4.5.2 Frequency of processing log

See section 4.5.1.

4.5.3 Retention period for audit log

See section 4.5.1.

4.5.4 Protection of audit log

See section 4.5.1.

4.5.5 Audit log backup procedures

See section 4.5.1.

4.5.6 Audit collection system (internal vs external)

See section 4.5.1.

4.5.7 Notification to event-causing subject

See section 4.5.1.

4.5.8 Vulnerability assessments

No stipulation.

4.6 Records Archival

4.6.1 Types of event recorded

The following events are recorded and archived:

- certificate requests
- approved certificate requests
- issued certificates
- revocation of certificates

4.6.2 Retention period for archive

The minimum retention period is ten (10) years.

4.6.3 Protection of archive

Archives are stored in a room with restricted access.

4.6.4 Archive backup procedures

Archives are not backed up.

4.6.5 Requirements for time-stamping of records

No stipulation.

4.6.6 Archive collection system (internal or external)

The record archival is physically separated from the offline CA. There is also an archive directory on the offline CA which contains all events recorded.

4.6.7 Procedures to obtain and verify archive information

No stipulation.

4.7 Key changeover

CA's private signing key is changed periodically. To avoid interruption of validity of all subordinate keys the new CA key is generated 13 (thirteen) month before the old one loses validity. From that point on new certificates are signed by the new CA key. The new CA key is posted in the repository.

4.8 Compromise and Disaster Recovery

4.8.1 Computing resources, software, and/or data are corrupted

If the CA equipment is damaged or rendered inoperative, but the CA private key is not destroyed, CA operation will be reestablished as quickly as possible. If the private key is destroyed the case will be treated as in section 4.8.3.

4.8.2 Entity public key is revoked

See section 4.8.3.

4.8.3 Entity key is compromised

If SWITCH Root CA's private key is - or suspected to be - compromised, SWITCH Root CA:

- informs subject CAs
- terminates the certificates and CRL distribution services for certificates and CRLs issued using the compromised key.
- generates a new CA authority certificate (with a new key pair) and make it immediately available in the public repository
- all subjects have to recertify following the initial identification procedures defined in section 3.1.

4.8.4 Secure facility after a natural or other type of disaster

In the case of a disaster whereby the CA installation is physically damaged and all copies of the CA signature key are destroyed as a result, the PMA will take whatever action it deems appropriate.

4.9 CA Termination

Before SWITCH Root CA terminates its services, it:

- informs subject CAs
- makes widely available information of its termination

- stops issuing certificates and CRLs
- destroys private keys and all copies

5. PHYSICAL, PROCEDURAL, AND PERSONNEL SECURITY CONTROLS

5.1 Physical Controls

5.1.1 Site location and construction

t.b.d. depending on whether SWITCH maintains the CA or it will be outsourced.

5.1.2 Physical access

Physical access to the CA hardware is restricted to authorized personnel.

5.1.3 Power and air conditioning

No stipulation.

5.1.4 Water exposures

No stipulation.

5.1.5 Fire prevention and protection

No stipulation.

5.1.6 Media storage

No stipulation.

5.1.7 Waste disposal

No stipulation.

5.1.8 Off-site backup

No stipulation.

5.2 Procedural Controls

5.2.1 Trusted roles

No stipulation.

5.2.2 Number of persons required per task

No stipulation.

5.2.3 Identification and authentication for each role

No stipulation.

5.3 Personnel Controls

5.3.1 Background, qualifications, experience, and clearance requirements

No stipulation.

5.3.2 Background check procedures

No stipulation.

5.3.3 Training requirements

No stipulation.

5.3.4 Retraining frequency and requirements

No stipulation.

5.3.5 Job rotation frequency and sequence

No stipulation.

5.3.6 Sanctions for unauthorized actions

No stipulation.

5.3.7 Contracting personnel requirements

No stipulation.

5.3.8 Documentation supplied to personnel

No stipulation.

6. TECHNICAL SECURITY CONTROLS

6.1 Key Pair Generation and Installation

6.1.1 Key pair generation

The issuing CA key pair gets generated off-line on the server used for the Root CA in presence of at least three SWITCH staff members including the legal counsel and remains off-line.

Subject CAs generate their key pair according to their CP/CPS.

6.1.2 Private key delivery to entity

Not applicable for Root CA since generated on the server itself.

6.1.3 Public key delivery to certificate issuer

The public key of a subject CA is part of the self-signed certification sent by e-mail to the Root CA or gets submitted via a web page.

6.1.4 CA public key delivery to users

SWITCH Root CA certificate is available from its public repository:
<http://www.switch.ch/ca/repository/>

6.1.5 Key sizes

The key size of the SWITCH Root CA is at least 4096 bits.
The key size of the subject CAs has to be at least 2048 bits.

6.1.6 Public key parameters generation

No stipulation.

6.1.7 Parameter quality checking

No stipulation.

6.1.8 Hardware/software key generation

The key pair of the SWITCH Root CA gets generated with OpenSSL software.

The CP/CPS of the subject CAs defines the method of key generation they are applying.

6.1.9 Key usage purposes (as per X.509 v3 key usage field)

For certificates issued by SWITCH Root CA under this policy, the keyUsage extension left blank (unused).

6.2 Private Key Protection

6.2.1 Standards for cryptographic module

SWITCH Root CA does not use any cryptographic module.

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

No stipulation.

6.2.3 Private key escrow

SWITCH Root CA keys are not given in escrow. SWITCH Root CA is also not available for accepting escrow copies of keys of other parties.

6.2.4 Private key backup

t.b.d.

6.2.5 Private key archival

The SWITCH Root CA private key will be printed on paper and stored in a burglarproof, fire safe location.

6.2.6 Private key entry into cryptographic module

See section 6.2.1.

6.2.7 Method of activating private key

The activation of the CA private key is done by providing the passphrase.

6.2.8 Method of deactivating private key

No stipulation.

6.2.9 Method of destroying private key

t.b.d.

6.3 Other Aspects of Key Pair Management

6.3.1 Public key archival

The public key is archived as part of the certificate archival.

6.3.2 Usage periods for the public and private keys

SWITCH Root CA certificates have a validity of ten (10) year [Investigations have shown, that root certificates validity range from 5 to 45 years]. For other entity certificates, the maximum validity period for a certificate is one year.

6.4 Activation Data

6.4.1 Activation data generation and installation

The length of the passphrase is at least of sixteen (16) characters.

6.4.2 Activation data protection

All pass phrases are known to all current staff members of the SWITCH Root CA.

6.4.3 Other aspects of activation data

No stipulation.

6.5 Computer Security Controls

6.5.1 Specific computer security technical requirements

t.b.d.

The machine used for signing certificates is not connected to any network.

6.5.2 Computer security rating

No stipulation.

6.6 Life Cycle Technical Controls

6.6.1 System development controls

No stipulation.

6.6.2 Security management controls

No stipulation.

6.6.3 Life cycle security ratings

No stipulation.

6.7 Network Security Controls

Certificates are issued on a machine not connected to any kind of network. Further details have to be defined.

6.8 Cryptographic Module Engineering Controls

No stipulation.

7. CERTIFICATE AND CRL PROFILES

7.1 Certificate Profile

7.1.1 Version number(s)

X.509 v3 (0x2)

7.1.2 Certificate extensions

The following extensions are set in subject CA's certificates:

- t.b.d. if necessary

The following extensions are set in host/server certificates:

- t.b.d.

The following extensions are set in SWITCH Root CA self-signed certificate:

- *no extensions are defined*

7.1.3 Algorithm object identifiers

No stipulation.

7.1.4 Name forms

See section 3.1.1.

7.1.5 Name constraints

See section 3.1.2.

7.1.6 Certificate policy Object Identifier

See section 1.2.

7.1.7 Usage of Policy Constraints extension

No stipulation.

7.1.8 Policy qualifiers syntax and semantics

No stipulation.

7.1.9 Processing semantics for the critical certificate policy extension

No stipulation.

7.2 CRL Profile

Does SWITCH has to provide a CRL service or will this be done by the subject CAs?

7.2.1 Version number(s)

X.509 v1 (0x0)

7.2.2 CRL and CRL entry extensions

No stipulation.

8. SPECIFICATION ADMINISTRATION

8.1 Specification change procedures

Users will not be warned in advance of changes to SWITCH Root CA's CP and CPSs. Relevant changes are made as widely available as possible.

8.2 Publication and notification policies

This policy and any older versions are available from the on-line repository managed by the PMA (see section 1.4).

8.3 CPS approval procedures

No stipulation.

Bibliography

1. Centre Europeen de Recherche Nucleaire - <http://www.cern.ch>
2. S. Chokani and W. Ford, Internet X.509 Infrastructure Certificate Policy and Certification Practices Framework, RFC 2527, March 1999
3. CERN CA Security Group - <http://home.cern.ch/globus/> - Email: *cern-globus-ca@cern.ch*
4. INFN CA Certificate Policy and Certification Practice Statement - <http://security.fi.infn.it/CA/CPS>
5. EuroPKI Certificate Policy - http://www.europki.org/ca/root/cps/en_index.html
6. CP/CPS SwissSign: http://swisssign.com/trust/SwissSign_Private_CPS.pdf