SWITCHgrid Root CA

Certificate Policy and Certification Practice Statement

Status: Released

Version: 1.0

Table of Contents

Document history

V0.9 (Nov 4, 2006)	First draft version to be submitted to EuGridPMA
V1.0 (Jan 24, 2007)	Editorial changes after EuGridPMA meeting in Abingdon
V1.0 (Feb 8, 2007)	Changed status to Released and updated the date

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 tele-computing 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.

This document is the Certificate Policy and Certification Practice Statement (CP/CPS) of the SWITCHgrid Root CA, further referred to as “Root CA” or “this CA” or “this CA and its subsidiary CAs". It describes the set of procedures followed by this CA and is structured according to RFC 3647. No other documentations form part of this document and only the information provided in this document may be relied on.

The purpose of the SWITCHgrid Root CA is to issue certificates, targeted for use in grid and e-Science environment, to CAs for the Swiss higher education and research sector. The Root CA is an offline CA, which is used exclusively to sign subordinate CAs. Currently the only subordinate CA is the SWITCHslcs CA, but more subordinate CAs may be added in the future.

This service and its subordinate CAs are independent of the SWITCHpki service as described by in the document “SWITCH Certificate Policy and Certification Practice Statement”, OID 2.16.756.1.2.6.1.*.

1.2 Document name and identification

This document is named SWITCHgrid Root CA Certificate Policy and Certification Practice Statement. It heavily draws on the certificate policy and certification practices statement of the UK e-Science CA run by CCLRC (Council for the Central Laboratory of the Research Councils), whose permission to reuse parts from the original document is herewith gratefully acknowledged.

The version is 1.0, dated February 8, 2007.

The following ASN.1 Object Identifier (OID) has been assigned to this document (where the OID components starting at position 8 reflect the version number):
2.16.756.1.2.6.3.1.0

1.3 PKI participants

1.3.1 Certification authorities

The SWITCHgrid Root CA only issues CA certificates. Subject CAs under the Root CA may themselves issue to further Subordinate CAs.

1.3.2 Registration authorities

There are no RAs external to the issuing authority. The issuing authority alone is responsible for all approvals and revocations.

1.3.3 Subscribers

Only Subject CAs receives certificates from the Root CA.

1.3.4 Relying parties

No stipulation.

1.3.5 Other participants

No stipulation.

1.4 Certificate usage

Nothing should be inferred about the assurance of Subordinate CAs: they may have different assurance levels and purposes, and the Root CA does not guarantee a minimum. Relying parties should consult the policy of Subordinate CAs before reliance. The Root CA does not assert that all Subordinate CAs serve the same community, and they all issue in distinct namespaces – see section 3.1.

1.4.1. Appropriate certificate uses

The Root certificate may be used for the following purposes:

- To validate the signature of a Subject CA and, more generally, as a part of validation of any certificate chain ending with the Root, provided all certificates in the chain are being used for their permitted purposes;
- To validate the signature of a CRL issued by the Root CA.

1.4.2. Prohibited certificate uses

Every use other than 1.4.1 of the Root CA is prohibited.

1.5 Policy administration

1.5.1 Organization administering the document

SWITCH – Teleinformatikdienste für Lehre und Forschung
SWITCHpki Policy Management Authority (PMA)
P. O. Box
CH-8021 Zürich
Switzerland
Tel: +41 44 268 15 15
www.switch.ch

1.5.2 Contact person

Kaspar Brand
pki@switch.ch
Tel: +41 44 268 15 15

1.5.3 Person determining CPS suitability for the policy

The PMA of SWITCH is responsible for reviewing and approving this CP/CPS.

1.5.4 CPS approval procedures

The PMA of SWITCH is responsible for reviewing and approving this CP/CPS such that it adheres to RFC 3647.

1.6 Definitions and acronyms

CA Manager	Persons managing a given CA. This includes access to the CA, maintenance and operation of CA software as well as maintenance of the CP/CPS associated with this CA.
CA Operator	Persons who maintain and operate the CA software. CA Managers are also CA operators for the SWITCHgrid CA.
End Entity (EE)	Party receiving a certificate from a CA upon submission of a certificate signing request.
PMA	The Policy Management Authority, established by SWITCH, consists of a minimum of three (3) persons responsible for defining the functioning of the SWITCH PKI by means of this CP/CPS
Profile	Content of the signed envelope within a certificate, but excluding the public key itself and the lifetime.
Root CA	Top-level CA, which is signed by itself. Its sole purpose is to be the starting point for a CA chain.
Relying Party (RP)	Party to which an EE presents its certificate as authentication method
Rollover	To rollover a certificate means that a new certificate is issued while the old is still valid and usable. This is used to issue a new CA certificate while keeping the old valid and all the certificates that were issued with it.
Subject CA	CA whose certificate was issued by the Root whose policy and practises are described in this document.
Subordinate CA	Subject CA or any CA underneath it.

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES

This CA will make its Certificate(s), CP, CPS, CRL and related documents for this CA publicly available through the SWITCH web site. In addition it will maintain an online accessible repository of certificate revocation information.

2.1 Repositories

A CA related website is maintained by SWITCH. It contains all the information published by this CA. The website can be reached at the following address:
http://www.switch.ch/pki/grid

2.2 Publication of certification information

SWITCH operates a secure online repository that contains:

- All publicly accessible certificates of this CA
- An overview of the hierarchy of which it forms the root

- All past and current versions of the CP/CPS for this CA
- Its CRL

2.3 Time or frequency of publication

New versions of CP/CPS are published as soon as they have been approved.

2.4 Access controls on repositories

The CP/CPS of this CA is available to the public as read-only information from the SWITCH web site.

Modification of CP, CPS and EUA is only permissible to SWITCH employees with proper authorization by the Policy Management Authority (PMA).

3. IDENTIFICATION AND AUTHENTICATION

3.1 Naming

- Each of the Subject CAs shall have a unique name
- The Subject name of each Subject CA shall be formed so that the written form starts with /C=CH/O=Switch - Teleinformatikdienste fuer Lehre und Forschung.
- No subject name of a Subject CA shall be reused anywhere in the hierarchy
- In general national characters are represented by their ASCII equivalent. E.g. é, è, à, ç are represented by e, e, a, c.
- The German “Umlaut” characters may receive special treatment: ä, ö, ü are represented by either ae, oe, ue or a, o, u.

3.2 Initial identity validation

A certificate shall be issued to a Subject CA only when

- The Subject CA has defined CP and CPS consistent with the policy and practises described in this document
- The Subject CA has implemented and described policy and practises sufficient to meet the restrictions that this document imposes on Subject CAs and all Subordinate CAs issued under the Subject CA
- The Subject CA has submitted a certificate request and is able to prove to the Root CA possession of the corresponding private key

Furthermore, the Root CA requires, as a condition for certificate issuance, that

- All Subject CAs make available to the Root CA results of CA audits and plans to remedy deficiencies
- The Subject CA’s certificate request (and hence certificate) contains no personal information

3.3 Identification and authentication for re-key requests

The CA Manager of the Subject CA shall prove possession of the private key corresponding to the certificate being renewed, and prove possession of the private key

corresponding to the request being submitted.

3.4 Identification and authentication for revocation request

The certificate of a Subject CA will be revoked in the following cases:

- A revocation request is received which is signed with the private key of the Subject CAs
- An authenticated revocation request from the CA Manager of the Subject CA is received
- The Root CA has otherwise determined the need for revocation, e.g. if the Subject CA does not comply with the requirements on it by the Root CA.

4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

For both the Root CA and Subject CAs, keys shall be generated by the CA Manager using high entropy input. The private key shall be protected according to the practises of the CA.

The Subject CA certificate shall have a lifetime not exceeding five years. The Root CA shall have a lifetime of twenty years.

4.1 Certificate Application

For an initial request, the Manager of the Subject CA shall agree on the namespace of the Subject CA with the Manager of the Root CA, and shall then submit the CP/CPS under which the Subject CA will operate. It is the responsibility of the Manager of the Subject CA to ensure that the Subject CA and all its Subordinate CAs (if any) operate within the constraints imposed by the Policy of the Root.

The Manager of the Subject CA is responsible for the generation of keys for the Subject CA. The Root CA shall not have access to the private key of the Subject CA. The CA Manager of the Subject CA shall submit the request physically (e.g., memory stick, floppy disk) to the Root CA.

4.2 Certificate application processing

The Manager of the Root CA will issue and publish the certificate of the Subject CA as soon as

- the CA Manager of the Root CA has approved the CP/CPS of the Subject CA
- the Subject CA complies with the CP/CPS of the Root CA and Subject CA

4.3 Certificate issuance

The Manager of the Root CA makes the Subject CA certificate available on its web site, and notifies the Manager of the Subject CA by phone or mail or otherwise that the certificate has been issued.

4.4 Certificate acceptance

The CA Manager of the Subject CA shall verify the content of the Subject CA certificate against the CP/CPS of the Subject CA. If the CA Manager of the Subject CA has not made objections to the content of the certificate within five working days, it shall be considered accepted.
In case of non-acceptance, the CA Manager of the Subject CA shall inform the CA

Manager of the Root CA, describing required amendments. The certificate shall be revoked by the Root CA, and reissued with the amendments, provided the amended certificate is still compatible with the CP/CPSs of both the Root and Subject CAs. Re-issuance may be based on the original request.

4.5 Key pair and certificate usage

The certificates of all Subordinate CAs and those of the EE issued by Subordinate CAs are targeted to be used for purposes of e-Science and Grid work. Other purposes are not forbidden but neither supported.
The certificates issued to Subject CAs may only be used as CA certificates, i.e., for validating certificates issued by them, and for validating CRLs. A Subordinate CA may impose further constraints on the use of certificates on, and only on, CAs subordinate to itself and their EE. Conversely, no Subordinate CA shall relax constraints imposed on its policy or operations by the CP/CPS of a CA of which it is itself Subordinate.
It is the responsibility of the EE to use certificates for permitted purposes only. It is the responsibility of RPs to validate the certificate to their satisfaction at the time of reliance.

4.6 Certificate renewal

No Subject CA certificate shall be renewed except for the re-issuance associated with the non-acceptance of an issued certificate.

4.7 Certificate re-key

It is the responsibility of the CA Manager of each Subject CA to ensure that a timely re-keying of the Subject CA certificate is requested. The Manager shall further take into account time required for the Root CA Manager to perform any necessary validations of the Subject CA, operational requirements (Root operator availability and schedule), and the time permitted to the Manager to validate acceptance of the certificate, and certificate redistribution to repositories and RPs.
It is the Manager's responsibility to ensure that this process is complete within a time interval not less than the maximal lifetime of certificates directly issued by the Subject CA before the date of expiry of the Subject CA certificate.
The lifetime of the re-keyed Subject CA certificate shall not exceed that of the Root. It is the responsibility of the CA Manager of the Root CA to ensure that a timely rollover of the Root certificate is in place. To this end, the Root shall require that no Subject CA has a lifetime longer than five years.
The process for acceptance of a re-keyed Subject CA certificate is the same as for the acceptance of an initial request – see section 4.4.

4.8 Certificate modification

The CA Manager of a Subject CA may request certificate modification. Provided it is consistent with the policy and practises of the Root CA, the Manager of the Root CA shall:

- Reissue the certificate with the requested modifications, provided a timely request is made due to non-acceptance of an issued certificate
- Issue and re-publish the certificate with the requested modifications based on a new certificate, as for re-key.

Only in exceptional circumstances will the Manager of the Root CA reissue the certificate with the same keys. The CA Manager of the Subject CA shall describe:

- The need for the modification of the existing certificate
- Justify the urgency requiring a modified certificate containing the same keys
- The means by which the modified certificate shall be published and redistributed

- Compatibility: that the modifications will not impair the usability of the certificate with existing middleware and infrastructure, except to the extent that such impairment is the intention of the modification.

The exceptional circumstances include, but are not limited to:

- Vulnerabilities of cryptographic algorithms used in the certificate are discovered, and a compatible security update is available
- Exceptional circumstances (force majeure) beyond the control of the CA Manager of the Subject CA has prevented a timely re-keying request, thus requiring a temporary, limited extension of the lifetime of the certificate.

4.9 Certificate revocation and suspension

A certificate of a Subject CA shall be revoked if

- the Subject CA is seen to consistently and wilfully violate its own CP/CPS and the CA Manager of the Subject CA does not take steps to address such violations
- It is seen to violate the requirements imposed by the policy and practises of the Root
- It can be shown that the private key has been compromised

4.10 Certificate status services

The Root CA shall issue a CRL. Certificates and certificate status of Subject CAs are available on the Root CA's web site. See also section 7.2

4.11 End of subscription

No stipulation.

5. FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

5.1 Physical controls

The Root CA is kept offline on a removable storage device, which contains a complete operating system. At least two identical copies of this device as well as a paper copy of the private key are stored offline in a safe. Access is only performed to sign Subject CAs, whereby one of the removable storage devices is used to boot the entire operating system on a laptop, which is brought into the room, where the safe is located. The removable storage devices never leave the room, where the safe is located. Every access is done in groups of at least two Root CA operators.

5.2 Procedural controls

Only operators of the Root CA are system administrators of the signing machine. Any one operator may perform administrative tasks. For auditing of the signing system (logs), at least one member of the SWITCH PMA must be present.

5.3 Personnel controls

Training: the Root CA is OpenSSL based, and CA operators must have sufficient experience with OpenSSL to be able to issue certificates and CRLs. Operators must be permanent staff of the SWITCH security department.

5.4 Audit logging procedures

All operations on the signing machine are logged, both on paper, and basic system logs on the signing machine itself: bootup/shutdown, login, signatures.

5.5 Records archival

Records are kept throughout the lifetime of the CA, and for a period of no less than three years after the termination of the CA.

5.6 Key changeover

At re-keying, the new Root key shall be published on the Root CA's web site, as certificates signed by both the old and the new private key. The transitional certificate, signed with the old key, shall expire at the same time as the old Root certificate, but shall otherwise have the same content as the new Root certificate. It shall be clearly marked as a transitional certificate, and instructions shall be provided for users explaining how to verify the transition.

5.7 Compromise and disaster recovery

Following a compromise of the Root private key, the root CA shall make this widely known to all peer CAs, Subject CAs, and RPs. Subject CAs shall further communicate this to their communities.

5.8 CA or RA termination

Upon termination of the root CA, the CA Manager shall communicate this in advance to peer CAs, Subject CAs and RPs by sending an email to the EUGRIDPMA mailing list and posting an announcement on the SWITCHpki website. The advance notice should be no less than the longest lifetime of any currently valid Subject CA.

6. TECHNICAL SECURITY CONTROLS

6.1 Key pair generation and installation

The Root CA's key pair shall be generated with sufficient entropy: every bit of random input comes from a good random source. It shall be the responsibility of the CA Manager to generate the key pair. The Root key shall be RSA and have a length of at least 2048 bits.

For the Subject CAs, it is the responsibility of the CA Manager to ensure that the key pairs are generated according to best practices. Each Subject CA key pair shall have a length of at least 2048 bits.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

The private key of the Root CA shall be protected with the 2-out-of-3 activation date as

described in section 6.4. There shall be at any given time exactly three operators.

The private key is not escrowed.

At least three different digital copies of the encrypted private key shall be kept. The digital backups shall have the following properties:

- They shall be kept on different media (e.g. disk, memory stick) from different vendors
- They shall be kept so only operators have normal authorised access to them
- Non-removable media shall be administrated and have access control equivalent to the site's protection of personnel records or their backups
- Removable media shall be kept locked in a safe. No person other than the operator(s) and site operations personnel shall have keys
- Each copy shall be checked for integrity at least once every year.

The private key must be unencrypted only in volatile memory. The passphrase is typed in as needed, and is also never written to non-volatile storage except paper. The machine used for signing is powered down after the signing.

It is the responsibility of the Operator to safeguard their own copies of the encrypted private key, to take no unauthorised copies thereof, and to surrender all copies to the CA Manager when they cease to be Operators.

Additionally, a printout on paper of the encrypted key shall be kept in tamper evident envelope in SWITCH's safe for classified information.

6.3 Other aspects of key pair management

All Root CA certificates shall be kept and published throughout the lifetime of the CA, and a period of no less than three years after the termination of the CA.

Subject CA's key pairs shall have a lifetime not exceeding 1826 days (five years).

6.4 Activation data

The activation data shall be chosen such that according to current cryptographic practise, estimates and recommendations, recovering the key from its encrypted form is at least as hard as recovering it from the public key.

The activation data shall then be encoded into ASCII characters as a passphrase. The passphrase shall then be split into three parts, as close to equal length as possible. These parts are written on paper, and are further referred to in this section as parts A, B, and C.

Each Operator shall be given two parts: Operator 1 gets parts A and B, Operator 2 gets A and C, and Operator 3 gets B and C. Thus, no single Operator, and any two Operators together, has parts A, B, and C. Operators are responsible for the safe keeping of the parts, and, in particular, shall not share them with each other. They are further responsible for not taking copies of them, and for surrendering them to the CA Manager when they cease to be Operators. An Operator may keep the two parts together, but must not keep them in the same location as any copy of the encrypted private key.
Additionally, a full paper copy of the activation data shall be kept in tamper evident envelope in SWITCH's safe for classified information.

The circumstances for updating the activation data include:

- Cryptographic advances have made the encrypted private key vulnerable to attack in the sense that recovering the private key from the encrypted form is significantly easier than recovering it from the public key;

- An Operator is suspected to have copied activation data or shared it with anyone else, or made unauthorized copies of the private key;
- An Operator has lost copies of the private key, or of the parts of the passphrase.

The procedure for generating or updating the activation data is as follows:

- (Update only) Operators shall surrender to the CA Manager all copies of the encrypted private key and activation data with the old encryption
- Together, Operators shall generate new activation data of a sufficient quality as described above, and split it as described above. A brief exposure to other parts of it is not considered a compromise, as each part will be too complex to memorize.
- All copies of the previous encrypted private key shall be deleted and replaced with the new version, except the ones in the safe for classified information, which may be kept for archival, and recovery purposes.

6.5 Computer security controls

The operating system of the CA including the private key is kept on a removable storage device in a safe. There is no other part of the CA other than its website, whose security controls need not be described in this document.

6.6 Life cycle technical controls

Not applicable – see section 6.5.

6.7 Network security controls

Not applicable – see section 6.5.

6.8 Time-stamping

The signing machine's clock shall be checked and set every time it is booted up. It is considered sufficient that it is accurate to within one minute.

7. CERTIFICATE, CRL, AND OCSP PROFILES

7.1 Certificate profile

The Root CA certificate has the following properties:

- the certificate is version 3 (i.e., version number is set to 2)
- issuer name and subject name are /C=CH/O=Switch - Teleinformatikdienste fuer Lehre und Forschung/CN=SWITCHgrid Root CA
- the signature algorithm is sha1WithRSAEncryption (1.2.840.113549.1.1.5)
- the validity is 7305 days (20 years)
- the following extensions are included:
    - basicConstraints: critical; CA=true
    - keyUsage: critical; keyCertSign and cRLSign bits are set
    - subjectKeyIdentifier: not critical; value is set to the SHA-1 hash of the BIT

STRING subjectPublicKey of the Root CA certificate

Subject CA certificates have the following properties:

- The certificate is version 3 (i.e., version number is set to 2)
- The issuer name is /C=CH/O=Switch - Teleinformatikdienste fuer Lehre und Forschung/CN=SWITCHgrid Root CA
- The signature algorithm is sha1WithRSAEncryption (1.2.840.113549.1.1.5)
- The following extensions are included:
  - basicConstraints: critical; CA=true. It may contain a pathlen constraint.
  - keyUsage: critical; keyCertSign bit is set. The cRLSign may be set, any other bits are unset.
  - authorityKeyIdentifier: not critical; value is set to the SHA-1 hash of the BIT STRING subjectPublicKey of the Root CA certificate
  - subjectKeyIdentifier: not critical; value is set to the SHA-1 hash of the BIT STRING subjectPublicKey of the Subject CA certificate

Subject CA certificates may contain other extensions, such as CRL distribution points or authority information access.

7.2 CRL profile

The Root CA issues CRL version 2, using the sha1WithRSAEncryption signature algorithm (1.2.840.113549.1.1.5). The validity of the CRL (time delta between thisUpdate and nextUpdate) is 548 days (18 months); the CRL is issued at least once every year.

7.3 OCSP profile

Not applicable.

8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS

The PMA of SWITCH shall carry out a compliance audit of the operators once every year. The audit shall inspect the logs, and check the security of the activation data and the copies of the encrypted private key.

9. OTHER BUSINESS AND LEGAL MATTERS

9.1 Fees

The Root CA charges no fees for its services.

9.2 Financial responsibility

No financial responsibility is accepted.

9.3 Confidentiality of business information

No stipulation.

9.4 Privacy of personal information

The Root CA does not process any personal data, except for the following:

- The contact details of the Managers of the Root CA and Subject CA. These are published in the respective CP/CPS documents, and are thus not considered confidential, but the Root CA does not publish them. They must, however, be published by the Subject CAs themselves.
- The email address of the Subject CA Managers and operators. These are not published and are used only for announcements pertaining to the Root CA, or announcements affecting all Subject CAs.

9.5 Intellectual property rights

The Root CA does not claim any intellectual property rights on certificates which it has issued.

9.6 Representations and warranties

When issuing a certificate to a Subject CA, the Root CA will have evaluated the CP/CPS of the Subject CA, and has verified that the Subject CA, when operating according to its CP/CPS, complies with the requirements imposed on it by this document.

9.7 Disclaimers of warranties

SWITCH warrants that the information in the certificate issued by this CA and its subsidiaries is true to the best of the CA's knowledge based on the RA performing certain identity authentication procedures with due diligence.

9.8 Limitations of liability

SWITCH denies any liability for damages that occurred to relying parties or subscribers of its certificates.

9.9 Indemnities

This CA declines any payment of indemnities for damages occurring from the use of its certificates.

9.10 Term and termination

The Root CA shall announce its termination widely, to subject CAs and major RPs and PMAs. The announcement should be made five years, or the maximal lifetime of any valid Subject CA certificate, whichever is shorter, prior to actual termination. The Root CA shall issue no certificates whose lifetime will exceed the date of termination. The Root CA shall be under obligation to maintain the CRL until its termination.

9.11 Individual notices and communications with participants

SWITCH reserves the right to make arbitrary decisions regarding severability, survival, merger and notice.

Any participant has to communicate, in an appropriate way, to all those concerned, any changes in its status as participant of the SWITCH PKI, which may reasonably affect any or all those concerned.

9.12 Amendments

The Root CA shall communicate amendments to Subject CAs, and its relevant PMA.

9.13 Dispute resolution provisions

The laws of Zurich, Switzerland shall govern all aspects of this CA. Sole place of venue for any dispute in connection with this CP/CPS or arising in connection with the usage of a SWITCHgrid certificate shall be the commercial court of Zurich (Zürcher Handelsgericht).

9.14 Governing law

The laws of Zurich, Switzerland shall govern all aspects of this CA. Sole place of venue for any dispute in connection with this CP/CPS or arising in connection with the usage of a SWITCH certificate shall be the commercial court of Zurich (Zürcher Handelsgericht).

9.15 Compliance with applicable law

The laws of Switzerland shall govern all aspects of this CA.

9.16 Miscellaneous provisions

Not applicable

9.16.1 Entire agreement

Not applicable

9.16.2 Assignment

Not applicable

9.16.3 Severability

In the event that a court or other tribunal determines that a clause within this CP/CPS is, for some reason, invalid or unenforceable, the remainder of the document remains in force.

9.16.4 Enforcement (attorneys' fees and waiver of rights)

Not applicable

9.16.5 Force Majeure

Events, compromising the SWITCHgrid services, that are outside the reasonable control of SWITCH (i.e. "Force Majeure") will be dealt with immediately by the PMA.

9.17 Other provisions

Not applicable