CESNET CA GRID Certificate Policy

Version 1.1

Draft 2
# Table of Contents

1. INTRODUCTION .................................................................................................................. 8  
   1.1. Overview .......................................................................................................................... 8  
   1.2. Identification .................................................................................................................... 8  
      1.2.1. Certificate Policy Name .............................................................................................. 8  
      1.2.2. Object Identifiers ....................................................................................................... 8  
   1.3. Community and Applicability ........................................................................................... 9  
      1.3.1. Certification authorities ............................................................................................. 9  
      1.3.2. Registration authorities .............................................................................................. 9  
      1.3.3. End entities .................................................................................................................. 9  
      1.3.4. Applicability ............................................................................................................... 9  
   1.4. Contact Details ................................................................................................................ 10  
      1.4.1. Specification administration organization ................................................................. 10  
      1.4.2. Contact person .......................................................................................................... 10  
      1.4.3. Person determining CPS suitability for the policy ..................................................... 10  

2. GENERAL PROVISIONS ........................................................................................................ 11  
   2.1. Obligations ...................................................................................................................... 11  
      2.1.1. CA obligations ........................................................................................................... 11  
      2.1.2. RA obligations .......................................................................................................... 11  
      2.1.3. Subscriber obligations .............................................................................................. 12  
      2.1.4. Relying party obligations .......................................................................................... 12  
      2.1.5. Repository obligations .............................................................................................. 12  
   2.2. Liability .......................................................................................................................... 13  
      2.2.1. CA liability ................................................................................................................. 13  
      2.2.2. RA liability ................................................................................................................. 13  
   2.3. Financial responsibility ................................................................................................... 13  
      2.3.1. Indemnification by relying parties .............................................................................. 13  
      2.3.2. Fiduciary relationships .............................................................................................. 13  
      2.3.3. Administrative processes .......................................................................................... 13  
   2.4. Interpretation and Enforcement ....................................................................................... 13  
      2.4.1. Governing law ............................................................................................................ 14  
      2.4.2. Severability, survival, merger, notice ...................................................................... 14  
      2.4.3. Dispute resolution procedures ................................................................................... 14  
   2.5. Fees .................................................................................................................................. 14  
      2.5.1. Certificate issuance or renewal fees .......................................................................... 14  
      2.5.2. Certificate access fees ............................................................................................... 14  
      2.5.3. Revocation or status information access fees ............................................................ 14  
      2.5.4. Fees for other services such as policy information .................................................... 14  
      2.5.5. Refund policy ............................................................................................................ 14
2.6. Publication and Repository ............................................................................ 15
  2.6.1. Publication of CA information ................................................................. 15
  2.6.2. Frequency of publication ........................................................................ 15
  2.6.3. Access controls ........................................................................................ 15
  2.6.4. Repositories ............................................................................................. 15
2.7. Compliance audit ........................................................................................... 15
  2.7.1. Frequency of entity compliance audit ....................................................... 15
  2.7.2. Identity/qualifications of auditor .............................................................. 15
  2.7.3. Auditor’s relationship to audited party ..................................................... 15
  2.7.4. Topics covered by audit .......................................................................... 16
  2.7.5. Actions taken as a result of deficiency ..................................................... 16
  2.7.6. Communication of results ....................................................................... 16
2.8. Confidentiality ............................................................................................... 16
  2.8.1. Types of information to be kept confidential ........................................... 16
  2.8.2. Types of information not considered confidential ................................. 16
  2.8.3. Disclosure of certificate revocation/suspension information .................... 16
  2.8.4. Release to law enforcement officials ....................................................... 16
  2.8.5. Release as part of civil discovery .............................................................. 16
  2.8.6. Disclosure upon owner’s request ............................................................. 17
  2.8.7. Other information release circumstances .............................................. 17
2.9. Intellectual Property Rights ......................................................................... 17

3. IDENTIFICATION AND AUTHENTICATION .................................................. 18
  3.1. Initial Registration ....................................................................................... 18
    3.1.1. Types of names .................................................................................... 18
    3.1.2. Need for names to be meaningful ....................................................... 18
    3.1.3. Rules for interpreting various name forms .......................................... 18
    3.1.4. Uniqueness of names ......................................................................... 19
    3.1.5. Name claim dispute resolution procedure ....................................... 19
    3.1.6. Recognition, authentication and role of trademarks ............................. 19
    3.1.7. Method to prove possession of private key ......................................... 19
    3.1.8. Authentication of organization identity .............................................. 19
    3.1.9. Authentication of individual identity .................................................. 19
  3.2. Routine Rekey ............................................................................................. 19
  3.3. Rekey after Revocation ............................................................................. 19
  3.4. Revocation Request ................................................................................... 20

4. OPERATIONAL REQUIREMENTS .................................................................. 21
  4.1. Certificate Application .............................................................................. 21
  4.2. Certificate Issuance ................................................................................... 21
  4.3. Certificate Acceptance .............................................................................. 21
  4.4. Certificate Suspension and Revocation .................................................... 21
4.4.1. Circumstances for revocation ................................................................. 21
4.4.2. Who can request revocation ................................................................. 21
4.4.3. Procedure for revocation request ......................................................... 22
4.4.4. Revocation request grace period ......................................................... 22
4.4.5. Circumstances for suspension ............................................................. 22
4.4.6. Who can request suspension ............................................................... 22
4.4.7. Procedure for suspension request ....................................................... 22
4.4.8. Limits on suspension period ................................................................. 22
4.4.9. CRL issuance frequency (if applicable) .................................................. 23
4.4.10. CRL checking requirements ............................................................... 23
4.4.11. On-line revocation/status checking availability ..................................... 23
4.4.12. On-line revocation checking requirements ......................................... 23
4.4.13. Other forms of revocation advertisements available ............................ 23
4.4.14. Checking requirements for other forms of revocation advertisements ...... 23
4.4.15. Special requirements re key compromise ........................................... 23
4.5. Security Audit Procedures ....................................................................... 24
  4.5.1. Types of event recorded ....................................................................... 24
  4.5.2. Frequency of processing log ............................................................... 24
  4.5.3. Retention period for audit log ............................................................. 24
  4.5.4. Protection of audit log ........................................................................ 24
  4.5.5. Audit log backup procedures .............................................................. 24
  4.5.6. Audit collection system (internal vs external) ....................................... 24
  4.5.7. Notification to event-causing subject .................................................. 24
  4.5.8. Vulnerability assessments ................................................................. 24
4.6. Records Archival ..................................................................................... 24
  4.6.1. Types of event recorded ...................................................................... 25
  4.6.2. Retention period for archive .............................................................. 25
  4.6.3. Protection of archive .......................................................................... 25
  4.6.4. Archive backup procedures ............................................................... 25
  4.6.5. Requirements for time-stamping of records ....................................... 25
  4.6.6. Archive collection system (internal or external) .................................... 26
  4.6.7. Procedures to obtain and verify archive information ............................ 26
4.7. Key changeover .................................................................................... 26
4.8. Compromise and Disaster Recovery ....................................................... 26
  4.8.1. Computing resources, software, and/or data are corrupted .................. 26
  4.8.2. Entity public key is revoked ............................................................... 26
  4.8.3. Entity key is compromised ............................................................... 26
  4.8.4. Secure facility after a natural or other type of disaster ....................... 27
4.9. CA Termination ..................................................................................... 27

5. PHYSICAL, PROCEDURAL, AND PERSONNEL SECURITY CONTROLS .......... 28
6. TECHNICAL SECURITY CONTROLS

5.1. Physical Controls

5.1.1. Site location and construction

5.1.2. Physical access

5.1.3. Power and air conditioning

5.1.4. Water exposures

5.1.5. Fire prevention and protection

5.1.6. Media storage

5.1.7. Waste disposal

5.1.8. Off-site backup

5.2. Procedural Controls

5.2.1. Trusted roles

5.2.2. Number of persons required per task

5.2.3. Identification and authentication for each role

5.3. Personnel Controls

5.3.1. Background, qualifications, experience, and clearance requirements

5.3.2. Background check procedures

5.3.3. Training requirements

5.3.4. Retraining frequency and requirements

5.3.5. Job rotation frequency and sequence

5.3.6. Sanctions for unauthorized actions

5.3.7. Contracting personnel requirements

5.3.8. Documentation supplied to personnel

6. Key Pair Generation and Installation

6.1.1. Key pair generation

6.1.2. Private key delivery to entity

6.1.3. Public key delivery to certificate issuer

6.1.4. CA public key delivery to users

6.1.5. Key sizes

6.1.6. Public key parameters generation

6.1.7. Parameter quality checking

6.1.8. Hardware/software key generation

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

6.2. Private Key Protection

6.2.1. Standards for cryptographic module

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

6.2.3. Private key escrow

6.2.4. Private key backup

6.2.5. Private key archival

6.2.6. Private key entry into cryptographic module
1. INTRODUCTION

This document is consistent with RFC 2527. Therefore there are some sections that are maintained for compatibility, although they do not apply exactly to the services required by the GRID projects. Glossary provides a glossary of terms used in this document.

Within this document the words “MUST”, “MUST NOT”, “REQUIRED”, “SHALL”, “SHALL NOT”, “SHOULD”, “SHOULD NOT”, “RECOMMENDED”, “MAY”, “OPTIONAL” are to be interpreted as in RFC 2119. (See Appendix Appendix A).

In this document the expression “conforming CA” is used to indicate a CA whose behavior is conforming to the set of provisions specified in this document.

1.1. Overview

This CP describes the requirements which MUST be met by a conforming CA in issuing digital certificates for GRID users and services.

This CP MAY be used by a relying party to determine the level of trust associated with this policy. An X.509 Version 3 certificate issued by a conforming CA SHOULD contain a reference to this certificate policy.

More detailed information about the practices which a conforming CA employs in its operations in issuing certificates can be found in its Certification Practice Statements (CPS).

1.2. Identification

1.2.1. Certificate Policy Name

CESNETCAGRIDCertificatePolicyv1:1

1.2.2. Object Identifiers

This certificate policy is identified by the following unique registered Object Identifier (OID):

1.3.6.1.4.1.8057.1.2.1.1.1

<table>
<thead>
<tr>
<th>ISO assigned</th>
<th>1</th>
</tr>
</thead>
<tbody>
<tr>
<td>US Department of Defense</td>
<td>6</td>
</tr>
<tr>
<td>Internet</td>
<td>1</td>
</tr>
</tbody>
</table>
1.3. Community and Applicability

Conforming CAs provide PKI services for the Czech academic community. Certificates issued under this CP are issued to users and services affiliated to organizations participating in GRID project.

1.3.1. Certification authorities

Conforming CAs SHOULD be operated by organizations participating in the GRID projects.

1.3.2. Registration authorities

Registration Authorities (RA) are needed for physical identification/authentication of entities. These authorities MUST not be permitted to issue certificates. The RA MUST sign an agreement with the certifying CA, stating the obligation to adhere to the agreed procedures as identified in the CA’s CPS. The conforming CA MAY manage the functions of its Registration Authority.

1.3.3. End entities

The targeted end entities are employees and students of Czech universities, employees of Czech Academy of Sciences, and any organizations cooperating with these entities in the GRID project as well as computers and application services operated by these organizations.

1.3.4. Applicability

Certificates issued by a conforming CA MUST NOT be used for financial transactions.
1.4. Contact Details

1.4.1. Specification administration organization
This CP is maintained by CESNET a.l.e. (http://www.cesnet.cz/).

1.4.2. Contact person
All questions and comments concerning this CPS must be addressed to:

CESNET CA
CESNET a.l.e.
Zikova 4
Prague
160 00
Czech Republic

Email: ca@cesnet.cz
URI: http://www.cesnet.cz/pki/

1.4.3. Person determining CPS suitability for the policy
See Section 1.4.2
2. GENERAL PROVISIONS

This chapter describes obligations for relevant parties and makes statements on liability and financial/economical issues. Moreover there is a section about confidentiality that classifies information into confidential information and publicly available and distributable information. Auditing statements are also located here.

2.1. Obligations

2.1.1. CA obligations

A conforming CA SHALL operate a certificate authority service. The conforming CA is responsible for all aspects of the issuance and management of a certificate referencing this policy, including:

- Development of a detailed statement of practices and procedures (the CPS) by which the CA implements the requirements of this policy.
- Publication of CA contact information.
- Certificate application/enrollment process.
- Verification of the identity of the applicant.
- Certificate creation process.
- Posting of the certificate in a public repository.
- Suspension and revocation of the certificate.
- Certificate renewals.
- Ensuring that all aspects of the CA services and CA operations and CA infrastructure related to certificates issued under this policy are performed in accordance with the requirements, representations, and warranties of this policy.
- Define and publish a dispute resolution procedure.

By issuing a certificate that references this policy, the CA certifies to the subscriber, and to all relying parties who reasonably and in good faith rely on the information contained in the certificate during its operational period, that:

- The CA has issued, and will manage, the certificate in accordance with this policy.
- There are no misrepresentations of fact in the certificate known to the CA, and the CA has taken reasonable steps to verify additional information in the certificate unless otherwise noted in its CPS.
- The certificate meets all material requirements of this policy and the CA's CPS.
2.1.2. RA obligations

An RA is obliged to operate RA service. This includes:

- Authenticating the identity of the subject
- Validating the connection between a public key and the requester identity including a suitable proof of possession method of the corresponding private key
- Confirming such validation versus the CA
- Adhere to the agreement made with the CA

2.1.3. Subscriber obligations

Subscribers MUST accurately represent the information required of them in a certificate request.
Subscribers MUST properly protect their private key at all times, against loss, disclosure to any other party, modification and unauthorized use, in accordance with this CP and the CPS. From the creation of their private and public key pair, subscribers are personally and solely responsible of the confidentiality and integrity of their private keys. Every usage of their private key is assumed to be the act of its owner.

Upon suspicion that their private keys are compromised subscribers MUST notify the CA that issued their certificates by sending a certificate revocation request.

Upon any change of information in their certificates subscribers MUST notify the CA that issued their certificates by sending a certificate revocation request.

Subscribers MUST use the keys and certificates only for the purposes authorized by the CA.
Subscribers MUST authorize the treatment and conservation of their personal data.

2.1.4. Relying party obligations

A relying party MUST be familiar with the CPS and this CP before drawing any conclusion on how much trust he can put in the use of a certificate issued from the CA.

The relying party MUST only use the certificate for the proscribed applications and MUST NOT use the certificates for forbidden applications.

Relying parties MUST verify the digital signature of a received digitally signed message and to verify the digital signature of the CA who issued the certificate used for the verification purpose.

When validating a certificate a relying party MUST check it for its validity, revocation, or suspension.
2.1.5. Repository obligations

A conforming CA SHALL use a publicly accessible repository to store certificates and Certificate Revocation Lists (CRLs). The repository SHALL be available as much as practically possible.

2.2. Liability

2.2.1. CA liability

A conforming CA MAY accept liability. The complete list of accepted liabilities MUST be specified in the CPS.

2.2.2. RA liability

See Section 2.2.1.

2.3. Financial responsibility

No financial responsibility is accepted for certificates issued under this CP.

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

This CP is governed by the law of the Czech Republic.

2.4.2. Severability, survival, merger, notice

No stipulation.

2.4.3. Dispute resolution procedures

No stipulation

2.5. Fees

2.5.1. Certificate issuance or renewal fees

No fees SHOULD be charged for issuing certificates.

2.5.2. Certificate access fees

Access to certificates SHOULD be free of charge.

2.5.3. Revocation or status information access fees

Access to Certificate Revocation Lists SHOULD be free of charge.

2.5.4. Fees for other services such as policy information

No fees SHOULD be charged for allowing policy and CPS information access.

2.5.5. Refund policy

No stipulation.
2.6. Publication and Repository

2.6.1. Publication of CA information

A conforming CA MUST make publicly available, in its repositories:

1. The Certificate Practice Statement it operates according to.
2. This Certificate Policy.
3. All issued certificates including CA-certificates.

2.6.2. Frequency of publication

The certificates issued SHALL be published as soon as they are issued.
The CRLs SHALL be published in accordance with Section 4.4.9.
CP and CPS SHALL be published as soon as they are updated.

2.6.3. Access controls

The CP, CPS, CRLs, and the certificates issued SHOULD be publicly available with no access control.

2.6.4. Repositories

No stipulation.

2.7. Compliance audit

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

2.8.1. Types of information to be kept confidential
All subscribers’ information that is not present in the certificate and CRLs issued by a conforming CA is considered confidential and SHALL not be released outside without explicit subscriber's authorization.

2.8.2. Types of information not considered confidential
Information included in public certificates and CRLs issued by a conforming CA are not considered confidential.

2.8.3. Disclosure of certificate revocation/suspension information
When a certificate is revoked/suspended, a reason code is not considered confidential and MAY be shared with all other users and relying parties. However, no other details concerning the revocation are normally disclosed.

2.8.4. Release to law enforcement officials
A conforming CA MUST NOT disclose confidential information to any third party, except when required by law enforcement officials that exhibit regular warrant.

2.8.5. Release as part of civil discovery
No stipulation.

2.8.6. Disclosure upon owner’s request
The CA SHALL release information if authorized by the subscriber.

2.8.7. Other information release circumstances
No stipulation.

2.9. Intellectual Property Rights
A conforming CA MUST NOT claim any intellectual property rights on issued certificates.
3. IDENTIFICATION AND AUTHENTICATION

3.1. Initial Registration

3.1.1. Types of names

A conforming CA assigns each entity a X.501 Distinguished Name (DN, see X.501) which serves as a unique identifier of the entity. The DN is inserted in the subject field of the certificate(s) issued to the entity to bind the entity to the certificate(s). The DN MUST be a non-empty printableString.

The certificate DN SHOULD be constructed using following naming attributes:

3.1.1.1. organizationName (O)

Necessity. Mandatory.

For personal certificates, this is the official name of the institution the subscriber is affiliated with. For server certificates, it is the official name of the institution operating the server.

3.1.1.2. commonName (CN)

Necessity. Mandatory.

For personal certificates, this is the full name of the person as stated in the proof-of identity documents, with any diacritical marks removed.

For server certificates, it is the fully qualified domain name of the server prefixed by the string “host/”. E.g. CN for server server.cesnet.cz will be host/server.cesnet.cz.

3.1.2. Need for names to be meaningful

A conforming SHALL be able to identify the entities associated with subject and issuer names contained in the certificates.

3.1.3. Rules for interpreting various name forms

All end entity certificates issued under this CP SHALL start with invariable part identifying the CA (e.g. RDN O=CESNET). The variable part following consists of the RDN indicating the organization which is the subscriber affiliated to (O=name of the organization, see Section 3.1.1.1) followed by the subscriber’s common name (CN=subscriber’s name, see Section 3.1.1.2).
3.1.4. Uniqueness of names
Every name assigned by a conforming CA SHALL be associated with exactly one entity.

3.1.5. Name claim dispute resolution procedure
No stipulation.

3.1.6. Recognition, authentication and role of trademarks
No stipulation.

3.1.7. Method to prove possession of private key
The requester is required to prove possession of the private key which corresponds to the public key in the certificate request before signing.
The method used to prove possession of private key MUST be detailed in the CPS.

3.1.8. Authentication of organization identity
All certificates issued under this CP include the name of a certain organization. The subscriber MUST provide a written statement of affiliation signed by the representatives of the organization.

3.1.9. Authentication of individual identity
The RA MUST personally authenticate any requester asking a personal certificate, using officially recognized identity card containing a photograph.
If the entity to be certified is a software or hardware component the requester MUST prove that he has the necessary authorization.

3.2. Routine Rekey
After certificate expiration, the CA MUST NOT issue a new certificate for the same key. The CA MAY issue a new certificate for a new key. The rekey authentication MAY be accomplished with the same procedure indicated in Section 3.1 for initial registration or using requests digitally signed with the old certificate. These requests MUST be sent to the CA before the old certificate expiration.
3.3. Rekey after Revocation

A public key whose certificate has been revoked for private key compromise MUST NOT be re-certified. The public key MAY be re-certified if the revocation is only due to certificate suspension. In the latter case the rekey authentication MAY be accomplished with the same procedure indicated in Section 3.1 for initial registration or using digitally signed requests. These requests MUST be sent to the CA before certificate expiration.

3.4. Revocation Request

A proper authentication method is required in order to accept revocation request. The CA MUST accept as a revocation request a message digitally signed with a not expired and not previously revoked certificate issued under this policy. The same procedures adopted for the authentication during initial registration are also considered suitable. Alternative procedures MAY be supported such as secure communication of a revocation passphrases.

The exact procedures supported MUST be detailed in the CPS.
4. OPERATIONAL REQUIREMENTS

4.1. Certificate Application
An entity generates its own key pair and submit public key and other required data to the CA. After that the request MUST carefully follow the procedures detailed in this policy and in the CPS for identification and authentication.

4.2. Certificate Issuance
The CA and RA MUST carefully check the compliance and validity of documents presented by the subscribers. After the authentication accomplished by methods specified in Section 3.1, the CA SHOULD issue the certificate. In the case of issuance the CA MUST notify the requester. If for any reasons the CA decides not to issue the certificate (even if the checks and the authentication were correct) it SHOULD notify the reason for this choice to the requester.

4.3. Certificate Acceptance
No stipulation.

4.4. Certificate Suspension and Revocation

4.4.1. Circumstances for revocation
A certificate SHALL be revoked when information in the certificate is known to be suspected or compromised. This include situations where:

• the subscriber’s data changed
• the subscriber’s private key is compromised or is suspected to have been compromised or lost
• the subscriber’s information in the certificate is suspected to be inaccurate
• the subscriber is known to have violated his obligations

4.4.2. Who can request revocation
The CA MUST accept a revocation request made by the holder of the certificate to be revoked. Moreover the revocation request MAY come from the CA that issued the certificate or from associated RA.
Other entities MAY require revocation, presenting evident proof of knowledge of the private key compromise or the change of subscriber’s data.

### 4.4.3. Procedure for revocation request

The entity requesting the revocation SHALL be properly authenticated. The authentication method SHOULD be as strong as the one used in the issuing procedure. Conforming CA MUST accept as a revocation request a message digitally signed with a not expired and not previously revoked certificate issued under this policy. An alternative procedure MAY require the entity to visit RA or CA and to present a viable identity document.

If the entity is a CA, the CA SHALL in addition:

- Inform subscribers and cross-certifying CAs
- Terminate the certificate and CRLs distribution service for certificates/CRLs issued using the compromised private key.

### 4.4.4. Revocation request grace period

The conforming CA decides what is the amount of time necessary to accept the request.

### 4.4.5. Circumstances for suspension

A CA MAY temporarily suspend a subscriber’s certificate if the subscriber requests that service. Unlike revocation, suspension of a user allows for re-enabling at a later time. In every case conforming CA are not required to offer the suspension service. Information on public keys of disabled users MAY be available from CA repository.

### 4.4.6. Who can request suspension

In the case that a CA offers the suspension service, CA MUST accept a suspension request made by the holder of the certificate to be suspended.

### 4.4.7. Procedure for suspension request

The entity requesting the suspension SHALL be properly authenticated. A conforming CA MUST accept as a suspension request a message digitally signed with a not expired and not previously revoked certificate issued under this policy. An alternative procedure MAY require the entity to visit RA or CA and to present a viable identity document.
4.4.8. Limits on suspension period

No stipulation.

4.4.9. CRL issuance frequency (if applicable)

CRL lifetime MUST be at least 7 days and MUST NOT be longer than 30 days. CRLs MUST be reissued at least 7 days before expiration, even if no additional revocations have occurred.

4.4.10. CRL checking requirements

Relying party MUST verify a certificate against the most recent CRL issued from conforming CA in order to validate the use of the certificate.

4.4.11. On-line revocation/status checking availability

A conforming CA MAY support on-line revocation/status checking. Bearing in mind that this policy requires conforming CA to issue CRL, it is not mandatory to implement on-line revocation/status checking procedures. However this policy suggests taking into consideration OCSP RFC 2560 as such a mechanism.

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

This policy recognizes the importance of security audit procedures suggesting that a conforming CA specifies all this kind of provisions in the CPS.

4.5.1. Types of event recorded

No stipulation.

4.5.2. Frequency of processing log

No stipulation.

4.5.3. Retention period for audit log

No stipulation.

4.5.4. Protection of audit log

No stipulation.

4.5.5. Audit log backup procedures

No stipulation.

4.5.6. Audit collection system (internal vs external)

No stipulation.

4.5.7. Notification to event-causing subject

No stipulation.

4.5.8. Vulnerability assessments

No stipulation.
4.6. Records Archival

This section specifies the type of events that are recorded for archival purposes from CA and RA and how this collected data are maintained. For further details not explicitly stipulated here the reference is the CPS.

4.6.1. Types of event recorded

A conforming CA SHOULD archive:

- certification requests corresponding to actually issued certificates
- issued certificates
- issued CRLs
- all signed agreements with other parties (e.g. RA)
- documents collected from the subscriber during the enrollment procedure
- all relevant messages exchanged with RA

The RAs SHOULD archive:

- all validation information collected from the subscriber
- all relevant messages exchanged with CA

4.6.2. Retention period for archive

The minimum retention period is 2 years.

4.6.3. Protection of archive

No stipulation.

4.6.4. Archive backup procedures

No stipulation.

4.6.5. Requirements for time-stamping of records

No stipulation.
4.6.6. Archive collection system (internal or external)
No stipulation.

4.6.7. Procedures to obtain and verify archive information
No stipulation.

4.7. Key changeover
No stipulation.

4.8. Compromise and Disaster Recovery
If a CA’s private key is compromised or suspected to be compromised, the CA SHALL at least:

• inform subscribers, cross-certifying CAs and relying parties
• terminate the certificates and CRLs distribution service for certificates/CRLs issued using the compromised private key
• request the revocation of the CA’s certificate

If a RA’s private key is compromised or suspected to be compromised, the RA SHALL at least inform the CA and request the revocation of the RA’s certificate

If an entity’s private key is compromised or suspected to be compromised, the entity SHALL at least inform the relying parties and request the revocation of the entity’s certificate.

4.8.1. Computing resources, software, and/or data are corrupted
No stipulation.

4.8.2. Entity public key is revoked
No stipulation.

4.8.3. Entity key is compromised
No stipulation.
4.8.4. Secure facility after a natural or other type of disaster

No stipulation.

4.9. CA Termination

Termination of a CA is regarded as the situation where all service associated with a logical CA is terminated permanently.

Before the CA terminates its services the following procedures MUST be completed as a minimum:

- inform all subscribers, cross certifying CAs, higher level CAs, and relying parties with which the CA has agreements or other form of established relations
- make publicly available information of its termination
- stop distributing certificates and CRLs.

A subordinate CA MAY terminate or continue operation as a self-standing CA.
5. PHYSICAL, PROCEDURAL, AND PERSONNEL SECURITY CONTROLS

Security requirements imposed on the conforming CA are indicated in the CPS. In every case this policy states that CA MUST be run on a dedicated workstation. The workstation MUST be physically secured.

5.1. Physical Controls

5.1.1. Site location and construction
No stipulation.

5.1.2. Physical access
The physical access to the site in which the CA operates MUST be restricted only to explicitly authorized people.

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
All the issues related to procedural control like the definition of trusted roles MUST be specified in the CPS.

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
The personnel operating the CA MUST be technically and professionally competent. Every conforming CA SHOULD specify in the CPS further details concerning this particular topic and the related issues.

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
Conforming CA's cryptographic keys are generated by the package chosen for certificate handling. End entities cryptographic keys are locally generated by their application during the requesting process.

6.1.2. Private key delivery to entity
The entity MUST generate his own key pair.

6.1.3. Public key delivery to certificate issuer
For individual certification, the entity SHALL submit a certification request containing the public key, locally generated, to the CA/RA. Every conforming CA MUST specify in its CPS the exact procedures for delivering public key. For CA's certification, the subject CA generates the key pair.

6.1.4. CA public key delivery to users
Conforming CA MUST provide mechanisms to deliver CA public key to the users in a trustworthy manner. Further details MUST be specified in the CPS. In every case CA's public keys MUST be publicly available in a repository accessible via standard protocol such as HTTP or LDAP.

6.1.5. Key sizes
The minimum length of the private key of an end entity to be certified MUST be decided by the CA issuer and MUST NOT be less than the value of 1024 bits. A CA key pair MUST have a minimum length of 2048 bits.

6.1.6. Public key parameters generation
No stipulation.

6.1.7. Parameter quality checking
6.1.8. Hardware/software key generation

The keys can be generated in software or in hardware (e.g. on a cryptodevice) depending on the various tools available to the entities.

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

The purposes for which a key can be used MAY be restricted by a CA through the keyUsage extension in the certificate.

This is a field that indicates the purpose for which the certified public key is used. Certificates issued under this policy MUST have the keyUsage extension flagged as critical. This means that the certificate SHALL be used only for a purpose for which the corresponding key usage bit is set to one.

6.1.9.1. CA certificates

In CA’s certificates the keyUsage extension SHOULD contain the following bits set to one:

- digitalSignature
- nonRepudiation
- keyCertSign
- cRLSign

It MAY contain also other bits set to one.

6.1.9.2. User certificates

In personal (user) certificates the keyUsage extension SHOULD contain the following bits set to one:

- digitalSignature
- keyEncipherment
- nonReputiation
- dataEncipherment

6.1.9.3. Server certificates
In server (application, service) certificates the keyUsage extension SHOULD contain the following bits set to one:

- digitalSignature
- nonReputiation

### 6.2. Private Key Protection

#### 6.2.1. Standards for cryptographic module

This policy does not mandate the adoption of cryptographic module compliant with pre-determined standards. Every conforming CA MAY give in the CPS more details about the adoption of standard compliant module.

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

The private key of individual MUST NOT be under (n out of m) multi-person control. Only private keys belonging to a CA, a hardware component or a software component MAY be under such a control: in this case the type of control MUST be specified in the CPS.

#### 6.2.3. Private key escrow

This policy discourages the implementation of private key escrow policy both for end entities and CA. Implementation of such policies MAY be permitted if and only if the governing law of the country in which the CA is established explicitly requires them.

#### 6.2.4. Private key backup

This policy suggests that all the parties SHOULD maintain a backup copy of the private key in order to reconstitute it in case of destruction of the key. This backup MUST be carefully protected especially in the case of backup of private key CA.

#### 6.2.5. Private key archival
This policy suggests the implementation of a procedure for private key archival only for private key used for encryption/decryption. Indeed it MAY be necessary to maintain a copy of a private key in order to correctly decrypt messages even if the corresponding public-key certificate is expired.

6.2.6. Private key entry into cryptographic module

The private key of all entities SHOULD be stored in an encrypted form. This provision is particularly important if the entity is a CA.

6.2.7. Method of activating private key

Specific details about how to activate private key SHOULD be found in the CPS. As a general suggestion this policy recommends that for the activation of a private key some specific activation data MUST be entered in the cryptographic module. At least the activation data MUST consist in a PIN or passphrase, but for the most valuable private key (e.g. the ones belonging to CA) the use of hardware tokens or biometrics data is suggested.

6.2.8. Method of deactivating private key

No stipulation.

6.2.9. Method of destroying private key

No stipulation.

6.3. Other Aspects of Key Pair Management

6.3.1. Public key archival

A conforming CA MUST archive all issued certificates. Mechanisms to provide integrity controls other than digital signatures MAY be implemented.
6.3.2. Usage periods for the public and private keys

6.3.2.1. CA key pair
The validity period of a conforming CA’s key pair MUST NOT extend 5 years.

6.3.2.2. End entity key pair
The validity period of an end entity key pair MUST NOT extend one year.

6.4. Activation Data

6.4.1. Activation data generation and installation
Pass phrases or PINs SHALL be selected according to “best practice”. This means that it is necessary to suggest a suitable minimal length for the pass phrases and to enforce mechanisms to check that pass phrases show enough entropy.

6.4.2. Activation data protection
Pass phrases protecting private keys SHALL be accessible only to the legitimate users (e.g. certificate holder for personal certificates, CA operators for CA signing keys, etc). An exception for this indication is the implementation of a secure archival/backup mechanism for activation data. Such a mechanism MUST be clearly defined in the CPS.

6.4.3. Other aspects of activation data
No stipulation

6.5. Computer Security Controls

6.5.1. Specific computer security technical requirements
No stipulation.
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
This policy strongly suggests that the machine on which the cryptographic module used for CA operations SHOULD be kept off-line to prevent network attacks. In every case network access to the CA workstation MUST be limited in order to protect the CA's private key in an appropriate way from disclosure.

6.8. Cryptographic Module Engineering Controls
No stipulation.
7. CERTIFICATE AND CRL PROFILES

7.1. Certificate Profile

In order to promote interoperability this policy strongly encourages conforming CA to issue certificates profiling them accordingly to RFC 2459. In every case CPS MUST detail the specific profile adopted.

7.1.1. Version number(s)

The version field in the certificate SHALL state 2, indicating X.509v3 certificates.

7.1.2. Certificate extensions

In compliance with RFC 2459, the inclusion of the following certificate extensions is RECOMMENDED:

<table>
<thead>
<tr>
<th>Extension</th>
<th>Criticality</th>
</tr>
</thead>
<tbody>
<tr>
<td>subjectKeyIdentifier</td>
<td>NOT CRITICAL</td>
</tr>
<tr>
<td>authorityKeyIdentifier</td>
<td>NOT CRITICAL</td>
</tr>
<tr>
<td>basicConstraints</td>
<td>CRITICAL</td>
</tr>
<tr>
<td>keyUsage</td>
<td>CRITICAL</td>
</tr>
<tr>
<td>certificatePolicies</td>
<td>NOT CRITICAL</td>
</tr>
</tbody>
</table>

It is also RECOMMENDED the use of other two extensions: cRLDistributionPoint for providing information useful to retrieve the CRL, and subjectAltNames when there is the need to include an RFC822 e-mail address to a certificate. Both these two extensions SHOULD be marked as NOT CRITICAL.

7.1.3. Algorithm object identifiers

No stipulation.

7.1.4. Name forms

All related issues MUST be specified in the CPS.
7.1.5. Name constraints
All related issues MUST be specified in the CPS.

7.1.6. Certificate policy Object Identifier
Other certificate policy object identifiers are applicable if and only if the other policies identified are compliant with this policy. Conforming CA MUST contact the maintainers of the various policies to verify the level of mutual compliance. However in order to promote interoperability, following RFC 2459, this policy suggests to include only one certificate policy object identifier in a certificate.

7.1.7. Usage of Policy Constraints extension
All related issues MUST be specified in the CPS.

7.1.8. Policy qualifiers syntax and semantics
The Certificate Policies extension field has a provision for conveying, along with each certificate policy identifier, additional policy-dependent information in a qualifier field. The certificates issued under this CP SHOULD NOT use the policy qualifiers.

7.1.9. Processing semantics for the critical certificate policy extension
No stipulation

7.2. CRL Profile

7.2.1. Version number(s)
The version field in the certificate SHALL be omitted, indicating X.509v1 CRL.

7.2.2. CRL and CRL entry extensions
Not applicable.
8. SPECIFICATION ADMINISTRATION

8.1. Specification change procedures

Editorial changes can be made to the policy and CPS. In case of substantial changes of the policy all CAs and users SHALL be notified in advance. Moreover CAs SHALL update the policy in accordance with the policy changes.

Policy changes that imply minor technical adjustments SHALL be notified in advance.

8.2. Publication and notification policies

This policy is available at the URI: (http://www.cesnet.cz/pki/CP/...doplnit...).

8.3. CPS approval procedures

No stipulation
Glossary

Certification Authority (CA)

An authority trusted by one or more users to create and assign public key certificates. Optionally the CA may create the user’s keys. It is important to note that the CA is responsible for the public key certificates during their whole lifetime, not just for issuing them.

CA-certificate

A certificate for one CA’s public key issued by another CA.

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. For example, a particular certificate policy might indicate applicability of a type of certificate to the authentication of electronic data interchange transactions for the trading of goods within a given price range.

Certificate subject

The entity (person, organization, or server) whose public key is certified in the certificate.

Certification path

An ordered sequence of certificates which, together with the public key of the initial object in the path, can be processed to obtain that of the final object in the path.

Certification Practice Statement

A statement of the practices which a certification authority employs in issuing certificates.

Certificate revocation list

A CRL is a time stamped list identifying revoked certificates which is signed by a CA and made freely available in a public repository.

End entity

A person or resource that needs to have their public key certified.
Glossary

Entity
Any autonomous element within the Public Key Infrastructure. This may be a CA, an RA, or an End-Entity.

Issuing certification authority
In the context of a particular certificate, the issuing CA is the CA that issued the certificate (see also Subject certification authority).

Public Key Certificate
A data structure containing the public key of an end entity and some other information, which is digitally signed with the private key of the CA which issued it.

Registration authority
An entity that is responsible for identification and authentication of certificate subjects, but that does not sign or issue certificates (i.e., an RA is delegated certain tasks on behalf of a CA).

Relying party
A recipient of a certificate who acts in reliance on that certificate and/or digital signatures verified using that certificate. In this document, the terms "certificate user" and "relying party" are used interchangeably.

Subject certification authority
In the context of a particular CA-certificate, the subject CA is the CA whose public key is certified in the certificate.

Subscriber
In the case of certificates issued to resources (such as web servers), the person responsible for the certificate for that resource. For certificates issued to individuals, same as certificate subject.
Appendix A. Key words for use in RFCs to Indicate Requirement Levels

According to RFC 2119 Key words for use in RFCs to Indicate Requirement Levels, we specify how the main keywords used in RFCs should be interpreted. Authors who follow these guidelines should incorporate this phrase near the beginning of their document:

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT;", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119.

1. MUST. This word, or the terms "REQUIRED" or "SHALL", mean that the definition is an absolute requirement of the specification.

2. MUST NOT. This phrase, or the phrase "SHALL NOT", mean that the definition is an absolute prohibition of the specification.

3. SHOULD. This word, or the adjective "RECOMMENDED", mean that there may exist valid reasons in particular circumstances to ignore a particular item, but the full implications must be understood and carefully weighed before choosing a different course.

4. SHOULD NOT. This phrase, or the phrase "NOT RECOMMENDED" mean that there may exist valid reasons in particular circumstances when the particular behavior is acceptable or even useful, but the full implications should be understood and the case carefully weighed before implementing any behavior described with this label.

5. MAY. This word, or the adjective "OPTIONAL", mean that an item is truly optional. One vendor may choose to include the item because a particular marketplace requires it or because the vendor feels that it enhances the product while another vendor may omit the same item. An implementation which does not include a particular option MUST be prepared to interoperate with another implementation which does include the option, though perhaps with reduced functionality. In the same vein an implementation which does include a particular option MUST be prepared to interoperate with another implementation which does not include the option (except, of course, for the feature the option provides.)
Bibliography

http://www.europki.org/ca/root/

[RFC 2119]  RFC 2119 *Key words for use in RFCs to Indicate Requirement Levels* March 1997


