CESNET CA Certificate Practice Statement

Version 2.0

CESNET CA Certificate Practice Statement: Version 2.0

Published 2005

Table of Contents

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 offered by CESNET CA. 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 A).

1.1. Overview

This CPS describes the practices employed by the CESNET CA in issuing the digital certificates.

This CPS MAY be used by a relying party to determine the level of trust associated with a given policy.

1.2. Identification

1.2.1. Certificate Practice Statement Name

CESNETCACertificatePracticeStatementv2:0

1.2.2. Object Identifiers

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

1.3.6.1.4.1.8057.1.1.2.0

ISO assigned	1
Organization acknowledged by ISO	3
US Department of Defense	6
Internet	1
IANA registered private enterprises	1
CESNET	8057
PKI	1
Certificate Practice Statement	1
Major version	2
Minor version	0

1.3. Community and Applicability

CESNET CA provides PKI services for the Czech academic community.

The specific applicability of the certificates issued by the CESNET CA MAY be stated in the relevant CP.

1.3.1. Certification authorities

The CESNET CA digital certificates MUST be issued only by persons formally assigned by the CESNET a. l. e. director.

1.3.2. Registration authorities

The CESNET CA manages the functions of its Registration Authority.

Other RAs MAY be operated by sites within the Czech academic community, e. g. by universities or faculties. In that case the RAs MUST sign an agreement with the CESNET CA stating the obligation to adhere to this CPS and the relevant CPs.

1.3.3. End entities

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

In accordance with the corresponding CP, subscribers that are the subject of the issued certificates may be:

1. Any natural person which can be uniquely identified.

2. Any legal person or entity which can be uniquely identified (e. g. university of faculty).

3. Any other object (e. g. server or hardware/software component) that can be uniquely identified.

1.3.4. Applicability

Certificates issued by the CESNET CA MUST NOT be used for financial transactions.

Certificates issued by the CESNET CA can facilitate:

- Authentication
- Authorization
- Confidentiality
- Integrity
- Non-repudiation

Applicable key usage is indicated in the “Key Usage” extension of the certificate. Any usage other than the one(s) indicated in this extension is at the risk of the relying party.

The specific applicability requirements MAY be stated in the relevant CP.

1.4. Contact Details

1.4.1. Specification administration organization

This CPS 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

Not applicable.

2. GENERAL PROVISIONS

2.1. Obligations

2.1.1. CA obligations

2.1.1.1. Compliance

The CESNET CA MUST publish a CPS describing the practices employed in issuing the digital certificates. The CA MUST operate in accordance with its CPS, and the law of the Czech Republic.

2.1.1.2. Assurance of cross certification compliance

The CESNET CA MUST verify that any CA with which it cross-certifies complies with the mutually recognized CPs.

2.1.1.3. Certificate requests

The CA is obliged to handle certificate requests and issue new certificates:

- accept certification requests from entities requesting a certificate according to the agreed procedures contained in this CPS and in the relevant CP
- authenticate entities requesting a certificate, possibly by the help of separately designated RAs
- issue certificates based on requests from authenticated entities
- send notification of issued certificate to requesters
- make issued certificates publicly available

2.1.1.4. Certificate revocation

The CA is obliged to handle certificate revocation requests and certificate revocation:

- accept revocation requests from entities requesting a certificate to be revoked according to the agreed procedures contained in this CPS and the relevant CP
- authenticate entities requesting a certificate to be revoked
- issue a CRL
- make CRLs publicly available

2.1.1.5. Data privacy

The CA is authorized to collect the information related to personal data that is necessary to perform its services. These personal data can only be used in the context of the certification services provision. The subscriber has the right to access and request correction of these data.

2.1.1.6. Protection of issuing CA's private key

The CA is obliged to protect its private key in accordance with this CPS.

2.1.1.7. Restriction on issuing CA's private key use

The CA's private key used for issuing certificates in accordance with this CPS may be used only for signing certificates and CRLs, and other adequate information consistent with the certificate issuance.

2.1.2. RA obligations

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

2.1.2.1. Compliance

The RA MUST operate in accordance with its CPS and the law of the Czech Republic.

2.1.2.2. Authentication of the subject's identity

The RA is obliged to authenticate the identity of the subject to be certified using procedures specified in Section 3.1.

2.1.2.3. Validation of the connection between a public key and the requester identity

The RA is obliged to verify that the requester is in possession of the private key corresponding to the public key contained in the certificate request using procedures specified in Section 3.1.7.

2.1.2.4. Maintain certificate application information

The RA is obliged to keep supporting evidence for any certificate request made to a CA (e. g., certificate request forms) in accordance with this CPS.

2.1.2.5. Protection of RA's private key

The RA is obliged to protect its private key in accordance with this CPS.

2.1.2.6. Restriction on RA private key use

The private key used by a RA for signing certificate signing requests (CSRs), certificate suspensions, and certificate revocations as part of its RA function must not be used for any other purpose. Separate certificates will be issued to facilitate routine secure communication by the RA.

2.1.3. Subscriber obligations

2.1.3.1. Accuracy of representations in certificate applications

Subscribers MUST accurately represent the information required of them in a certificate request process.

2.1.3.2. Key pair generation

Subscribers MUST generate their public key pair using a trustworthy method.

2.1.3.3. Protection of entity's private key

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 CPS and the relevant CP. 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.

2.1.3.4. Notification of CA upon private key compromise

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

2.1.3.5. Notification of CA upon any change in their certificate content

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

2.1.3.6. Restrictions on private key and certificate use

Subscribers MUST use the keys and certificates only for the purposes authorized by the CA.

2.1.3.7. Personal data

By submitting a certificate request, the subscriber authorizes the CESNET CA to treat and conservate their personal data in compliance with this CPS.

2.1.4. Relying party obligations

2.1.4.1. CPS

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

2.1.4.2. Purposes for which certificate is used

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

2.1.4.3. Digital signature verification responsibilities

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.

2.1.4.4. Revocation and suspension checking responsibilities

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

2.1.5. Repository obligations

The CESNET 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

The CESNET CA warrants that all certificates issued were issued in accordance with this CPS and the relevant CP.

2.2.2. RA liability

RA warrants that subscriber's identity has been verified and that the identities in the certificate were valid at the time of issuance.

2.3. Financial responsibility

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

2.3.1. Indemnification by relying parties

The CESNET CA assumes no financial responsibility for improperly used certificates.

2.3.2. Fiduciary relationships

Issuance of certificates in accordance with this CPS and the corresponding CP does not make the CESNET CA, or any RA within the CESNET CA infrastructure an agent, fiduciary, trustee, or other representative of subscribers or relying parties.

2.3.3. Administrative processes

Not applicable.

2.4. Interpretation and Enforcement

2.4.1. Governing law

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

2.4.2. Severability, survival, merger, notice

Should it be determined that one section of this CPS is incorrect or invalid, the other sections shall remain in effect until the CPS is updated as indicated in Chapter 8

2.4.3. Dispute resolution procedures

In case of a dispute based on the contents of this CPS, the Director of CESNET a. l. e. will be the sole person responsible for resolution of the problem. The complainer cannot take legal action against CESNET a. l. e. or any of the CESNET a. l. e. partners.

If arbitration proves impossible, the parties can take legal actions.

2.5. Fees

2.5.1. Certificate issuance or renewal fees

No fees are charged for issuing certificates.

2.5.2. Certificate access fees

Access to certificates on the CESNET CA Certificate Registry is free of charge.

2.5.3. Revocation or status information access fees

Access to Certificate Revocation Lists on the CESNET CA Certificate Registry is free of charge.

2.5.4. Fees for other services such as policy information

No fees are charged for allowing policy and CPS information access.

2.5.5. Refund policy

Not applicable.

2.6. Publication and Repository

2.6.1. Publication of CA information

The CESNET CA MUST make publicly available, in its repositories:

1. The CESNET CA Certificate Practice Statement in http://www.cesnet.cz/pki/CPS.html
2. The applicable Certificate Policies in http://www.cesnet.cz/pki/CP/.
3. All issued certificates including CA-certificates in ldap://ldap.cesnet-ca.cz/.
4. Signed Certificate Revocation Lists in http://www.cesnet.cz/pki/crl/.

2.6.2. Frequency of publication

CRL publication must be in accordance with Section 4.4.9 of this CPS.

CPS publication must be in accordance with Chapter 8 of this CPS.

2.6.3. Access controls

There is no access control on reading the CP or the CPS.

There is no access control on reading the certificates.

The certificates, CRLs, CPs and CPS in the electronic repository are protected against any unauthorized modification.

2.6.4. Repositories

Chosen electronic repository must comply to this CPS. See Section 2.1.5.

2.7. Compliance audit

The CESNET CA declares that their practices fully comply with this 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

The CA collects personal information about the subscribers (e. g. full name, organization, and e-mail address). These data MUST be processed in a way that ensures privacy protection according to the law of the Czech Republic.

2.8.1. Types of information to be kept confidential

All subscribers' information that is not present in the certificate and CRL issued by the CESNET 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 the CESNET CA are not considered confidential.

2.8.3. Disclosure of certificate revocation/suspension information

When a certificate is revoked, a reason code MAY be included in the CRL entry for the action. This 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

The CESNET 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

The CESNET CA MUST NOT disclose confidential information to any third party, except when required by law enforcement officials that exhibit regular warrant.

2.8.6. Disclosure upon owner's request

The CA will release information if authorized by the subscriber.

2.8.7. Other information release circumstances

Not applicable

2.9. Intellectual Property Rights

The CESNET CA claims no intellectual property rights on issued certificates.

3. IDENTIFICATION AND AUTHENTICATION

3.1. Initial Registration

3.1.1. Types of names

The CESNET 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`.

All end entity DNs in certificates issued under this CPS SHALL start with invariable part identifying the CA (`dc=cesnet,dc=cz`). The following variable part can consists of the optional RDN indicating the organization which the subscriber is affiliated to (`O=`*name of the organization*, see Organization), followed by an optional RDN indicating the organizational unit which the subscriber is affiliated to (`OU=`*name of the organization unit*), followed by the end entity's common name (`CN=`*end entity's name*, see Common name). The structure of the variable part of the DN MAY be defined or restricted by the relevant CP.

The naming attributes of the subscriber to be requested to identify and authenticate the requester depend on the type of certificate that the subscriber requires. The choice of the types and format of names used in the fields of the certificate conforms to RFC 3280.

Following naming attributes MAY be used in end entities' Distinguished Names. In the case where the applicable CP states the rules for constructing the DN, the rules required by the CP take precedence over this CPS.

Country.

Attribute name	`C`
OID	`2.5.4.6`
Necessity	Optional.
Comments	For personal certificates, this is the country of residence of the subscriber. For server certificates, it is the country where the server is located. CESNET CA requires a proper evidence of the relation.

Location.

Attribute name	`L`
OID	`2.5.4.7`
Necessity	Optional.
Comments	For personal certificates, this is the locality of residence of the subscriber. For server certificates, it is the locality where the server is located. CESNET CA requires a proper evidence of the relation.

Common name.

Attribute name	`CN`
OID	`2.5.4.3`
Necessity	Mandatory.
Comments	For personal certificates, this attribute SHOULD contain subscriber's first name followed optionally by initials followed by surname. CESNET CA MUST verify the personal names comparing them with an official id document.

For server certificates, it SHOULD contain the fully qualified domain name of the server.

Organization.

Attribute name	`O`
OID	`2.5.4.10`
Necessity	Optional.
Comments	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. In both cases CESNET CA requires an evidence of the affiliation.

Organizational Unit.

Attribute name	`OU`
OID	`2.5.6.5`
Necessity	Optional.
Comments	For personal certificates, this is the official name of the organizational unit or department the subscriber is affiliated with. For server certificates, it is the official name of the organizational unit or department operating the server. In both cases CESNET CA requires an evidence of the affiliation.

3.1.1.1. Alternate names

In addition to names used to construct the `Subject` field of the certificate, other names, as specified in Section 4.2.1.7 of RFC 3280, are recognized by CESNET CA and MAY be included in the certificate upon subscriber's request. These include:

Internet email address.

Included as	`subjectAltName` extension
type	`rfc822Name`
Necessity	Optional.
Comments	Email address(es) in the `addr-spec` format, as defined in RFC 822 provided by the subscriber. The functionality of all email addresses MUST be checked by sending a unique email challenge message to which the subscriber must respond.

Domain name system label.

Included as	`subjectAltName` extension
type	`dNSName`
Necessity	Optional.
Comments	DNS name(s) in the “preferred name syntax”, as defined by RFC 1034 provided by the subscriber. The CESNET CA MUST be presented a signed statement of the DNS name(s) holder claiming its rights to use the name(s) and delegating the right to use the name in a certificate to the subscriber.

IP address.

Included as	`subjectAltName` extension
type	`iPAddress`
Necessity	Optional.

Comments	IP address as in “network byte order”, as specified in RFC 791 (IPv4) or RFC 1883 (IPv6) provided by the subscriber. The CESNET CA MUST be presented a signed statement of the IP address holder claiming its rights to use the address and delegating the right to use the address in a certificate to the subscriber.

Other names defined in in Section 4.2.1.7 of RFC 3280 MAY be used in full conformance with the standard.

3.1.2. Need for names to be meaningful

The Subject and Issuer names contained in a certificate MUST be meaningful in the sense that the issuing CA has proper evidence of the existent association between these names and the entities to which they belong.

For personal certificates, the CN DN attribute SHOULD contain the legal name as presented in a government issued photo-identification.

For server certificates, the CN DN attribute SHOULD contain the fully qualified domain name of the server.

3.1.3. Rules for interpreting various name forms

See Section 3.1.1 and Section 3.1.2.

3.1.4. Uniqueness of names

The CESNET CA guarantees the uniqueness of the subject names. In case of name collision when more than one person use the same name, a random string is appended to the CN to make the name unique.

3.1.5. Name claim dispute resolution procedure

Name disputes are managed according to the law of the Czech Republic.

3.1.6. Recognition, authentication and role of trademarks

The CESNET CA does not guarantee that the names issued will contain the requested trademarks.

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.

When obtaining a personal or individual certificate is initiated by a key generation tag or control which the individual's web browser reads on the CA's user registration web page. Key generation and certificate signing request generation and submission are tied together in a single session, and there is a reasonable presumption of possession of private key in requests originating in web browser functions.

For signature keys not generated in a single certificate certificate issuing HTTPS session, this is done by the requester using its private key to sign a value and providing that value to the RA. The RA SHALL then validate the signature using the public key from the subscriber's certificate request.

For encryption keys not generated in a single certificate certificate issuing HTTPS session , the requester is asked to decrypt a random challenge encrypted with the public key contained in the certificate request.

In case that the validation fails, the certificate MUST NOT be issued.

3.1.8. Authentication of organization identity

Every time a subscriber requires the inclusion of the name of a certain organization in a certificate, issuing CA MUST have evidence that the organization has completely knowledge about this fact.

When the initial identification is performed by an RA representing the organization the name of which is requested to be included in the certificate, the RA MUST validate the request according to the rules defined by the organization and described in its CPS.

When the RA performing the initial identification is not itself affiliated with organization the name of which is requested to be included in the certificate, it MUST require written legally binding documents as evidence. In all cases suitable legal documents that prove the data to be certified MUST be presented by means of out-of-band methods.

3.1.9. Authentication of individual identity

The procedures of initial authentication of individual identity MUST comply with the CP applicable to the certificates.

In case where the CP requires personal photo-id authentication, the RA MUST meet the holder in person to compare the photograph and register the number of the identification document. Any identity card issued by government or by the organization operating the RA is accepted for authentication. The relevant CP MAY specify other acceptable identity documents.

The requester asking for a certificate for a server or a software component MUST prove that he has the necessary authorization by providing a signed statement made by the representatives of the organization operating the software. The statement MAY be in electronic form in which case it MUST be digitally signed by a valid certificate issued by the CESNET CA.

3.2. Routine Rekey

The identification and authentication for routine rekey may be accomplished either with the same procedure as for Section 3.1 or using digitally signed requests sent to the CA before certificate expiration.

In case where the certificate to be reissued contains the name of a certain organization, the new affiliation verification procedure as described in Section 3.1.8 MUST be performed before rekeying.

3.3. Rekey after Revocation

A rekey after a revocation without a key compromise is handled as a routine rekey (see Section 3.2).

A public key whose certificate has been revoked for private key compromise MUST NOT be re-certified.

3.4. Revocation Request

Revocation requests are authenticated either by procedures described in Section 3.1.9 or by verifying the digital signature of the revocation request made by a valid certificate under the corresponding CP.

4. OPERATIONAL REQUIREMENTS

4.1. Certificate Application

In order to apply for a certificate, the following steps need to be undertaken:

1. A requester registers his request record with the CESNET CA request registering database. The record MUST contain all user selectable fields requested to be included in the certificate, i. e. all the names and required extensions.

4.2. Certificate Issuance

In order to issue a certificate, the following steps need to be undertaken:

2. RA verifies all identity information such as email addresses, DNS names and IP addresses from the request record using procedures from Section 3.1.
3. RA verifies whether the requester qualifies for the certificate.
4. RA verifies the identity of the requester as indicated in Section 3.1 and accepts the request.
5. RA releases activation codes fro the certificate request to the subscriber. The activation codes may be delivered either personally or using a secured email message encrypted with subscribers valid and non-revoked certificate issued by CESNET CA.
6. The subscriber initiates a HTTPS session with the CESNET CA certificate issuing system providing activation codes for request authentication.
7. The CESNET CA certificate issuing system issues the requested certificate.

4.3. Certificate Acceptance

The certificate is assumed to be accepted unless its requester explicitly rejects it in an authenticated communication with the CA.

4.4. Certificate Suspension and Revocation

4.4.1. Circumstances for revocation

A certificate will be revoked when the information in the certificate is known to be suspected or compromised or at the request of the authorized entity. It includes following situations:

1. The associated private key is known to be compromised or misused.
2. The associated private key is suspected to be compromised or misused.
3. The subscriber's information in the certificate has changed.
4. The subscriber is known to have violated his obligations.
5. An authorized requester requested the certificate revocation.

4.4.2. Who can request revocation

The following entities can request the revocation of a certificate:

1. The entity who originally made the certificate request.

2. The entity which can prove its current responsibility for a certified machine or service.
3. Any entity which demonstrates the compromise of the private key or misuse of the certificate.
4. Any entity which demonstrates the change of subscriber's data.
5. The issuing CA or the associated RA.

4.4.3. Procedure for revocation request

In case where the CA can independently confirm that the certificate has been compromised or misused, the CA SHALL revoke the certificate, even if the request to do so comes from an unauthenticated source and/or the holder of the certificate is unreachable.

In all other cases the CA SHALL authenticate the revocation request and try to contact the subscriber before revoking the certificate.

If the revoked certificate is a CA certificate the CA SHALL in addition inform the subscribers and cross-certifying CAs and it SHALL terminate the certificate and CRLs distribution service for certificates/CRLs issued using the compromised private key.

4.4.4. Revocation request grace period

The CESNET CA MUST respond within two days (excluding weekends and public holidays) to revocation requests. It SHALL however handle revocation requests with priority as soon as the request is recognized as such.

4.4.5. Circumstances for suspension

The CESNET CA does not offer the suspension service.

4.4.6. Who can request suspension

Not applicable

4.4.7. Procedure for suspension request

Not applicable

4.4.8. Limits on suspension period

Not applicable

4.4.9. CRL issuance frequency

CRLs issued by CESNET CA are renewed whenever any certificate is revoked or when any CRLs is more than 1 day old.

4.4.10. CRL checking requirements

The CRLs are checked at the certificate relying party responsibility. Relying parties SHALL update their local copies of CRLs at least once per day.

4.4.11. On-line revocation/status checking availability

The on-line revocation/status checking service is not currently available.

4.4.12. On-line revocation checking requirements

Not currently applicable.

4.4.13. Other forms of revocation advertisements available

The subscriber is notified of the revocation of his certificate by email.

4.4.14. Checking requirements for other forms of revocation advertisements

Not applicable

4.4.15. Special requirements re key compromise

No stipulation

4.5. Security Audit Procedures

4.5.1. Types of event recorded

4.5.1.1. RA

The following types of events are recorded by RAs:

1. Boots of the equipment.
2. Login and logouts to the RA system.
3. Account management.
4. Use of the RA software.
5. Unauthorized attempts to access the RA system.
6. Requests for certificates.
7. Identity verification procedures.

4.5.1.2. CA

The following types of events are recorded by CAs:

1. Boots of the equipment.
2. Login and logouts to the issuing machine.
3. Account management.
4. Use of the CA software.
5. Unauthorized attempts to access the CA system.
6. Requests for certificates.
7. Certificate issuing.
8. Requests for revocation.
9. CRL issuing.

4.5.2. Frequency of processing log

The log files are analyzed at least once every month.

4.5.3. Retention period for audit log

Audit logs MUST be retained as archive records. The audit logs MUST be kept on CA equipment until moved to the archive.

4.5.4. Protection of audit log

Only authorized CESNET CA personnel is allowed to to view and process audit log files.

Audit log files stored on the CA equipment will not be open for modification by any human, or by any automated process other that those that perform audit and archival.

4.5.5. Audit log backup procedures

A backup of the audit logs on physical removable media SHALL be performed weekly. The backup media are saved in safe storage.

4.5.6. Audit collection system (internal vs external)

The audit collection system SHALL be running separately form the CA software.

The audit collection system is internal to the CESNET CA.

4.5.7. Notification to event-causing subject

The subjects causing an audit event are not notified of the audit action.

4.5.8. Vulnerability assessments

The CESNET CA personnel MUST pay attention to any sign of an attempt to violate the integrity of the PKI system. Any deficiency MUST be followed by a vulnerability assessment revision.

4.6. Records Archival

4.6.1. Types of event recorded

The following type of events are archived:

1. Certificate requests and related messages exchanged between the subscriber and the RA and CA.
2. Issued certificates.
3. Revocation requests and related messages exchanged with the requester and/or the subscriber.
4. Issued CRLs.
5. Records on CA rekeying.
6. Records on cross certification.
7. All implemented CPs and CPSs.
8. CA system configuration files.

9. Audit data as described in Section 4.5.1.

4.6.2. Retention period for archive

The minimum retention period is three years.

4.6.3. Protection of archive

Digitally stored archive records are stored encrypted in two copies placed in different locations. The encryption passwords SHALL be known only to the CESNET CA personnel.

4.6.4. Archive backup procedures

Archive records are weekly moved from the CA/RA equipment to the encrypted removable media. The copies are stored in different locations. See Section 4.6.3.

4.6.5. Requirements for time-stamping of records

All archive records are time stamped.

4.6.6. Archive collection system (internal or external)

The archive collection system is internal to the CESNET CA.

4.6.7. Procedures to obtain and verify archive information

Archived audit logs are available only to the CESNET CA personnel.

4.7. Key changeover

The CESNET CA's keys SHOULD be changed while sufficient validity time remains on the existing keys to allow uninterrupted validity of all subordinate keys. The following steps SHOULD be undertaken when changing the CESNET CA's keys:

1. A new CESNET CA key is generated and self signed certificate issued.

2. The old key is signed by the new one.

3. The new key is signed by the old one.

4. All the newly issued certificates are published.

4.8. Compromise and Disaster Recovery

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

In the case where the CESNET CA computing resource, software and/or data have been corrupted, the responsible personnel SHOULD immediately start the recovery procedures:

1. Backup public repository and services systems are started when needed.

2. Users are notified.

3. The cause of the corruption are diagnosed.

4. When the extent of the corruption cannot be exactly specified, the entire system MUST be rebuilt.

5. The corrupted parts of the system are repaired or replaced.
6. The corrupted data are replaced from backups if possible.
7. The certificates issued after disaster are re-issued.
8. The system is restarted and the users are notified.

4.8.2. Entity public key is revoked

4.8.2.1. Subscriber's public key

See Section 3.2, Section 3.3 and Section 3.4.

4.8.2.2. CA public key

1. The key is revoked.
2. The CRL is updated and published.
3. The CA system is brought down.
4. New CA keys pair is generated as indicated in Section 6.1.
5. Users are notified.

4.8.3. Entity key is compromised

4.8.3.1. Subscriber's key

Whenever the subscriber's key is compromised, the subscriber is obliged to notify CESNET CA as soon as possible. The revocation procedure will follow according to Section 3.3, Section 3.4.

4.8.3.2. CA key

In case that the CA private key is compromised, the following actions will be undertaken:

1. The key is revoked.
2. The CRL is updated and published.
3. The CA system is brought down.
4. The cause of the compromising is analyzed to minimize the risk in future.
5. New CA keys pair is generated as indicated in Section 6.1.
6. Users are notified.

4.8.4. Secure facility after a natural or other type of disaster

In the case of a natural or other type of disaster the CESNET CA MUST start the recovery as soon as possible using off-site stored backups.

4.9. CA Termination

4.9.1. Transfer of CA services

The CESNET CA can decide to transfer the PKI services to another organization. In that case it MUST inform all subscribers, cross certifying CAs, higher level CAs, and relying parties with which the CA has agreements or other form of established relations about the transfer at least 3 months before the transfer date. The new organization MUST comply with this CPS.

4.9.2. Cessation of CA services

The CESNET CA can decide to cease its services. In that case the following steps MUST be undertaken:

1. The CA MUST inform all subscribers, cross certifying CA s, higher level CAs, and relying parties with which the CA has agreements or other form of established relations about the decision at least one year before the termination date.

2. Any certificates issued after the announcement of the termination MUST have the expiration date not exceeding the termination date.

3. At the termination date all the certificates issued by the CA MUST be revoked.

4. The CA stops distributing certificates and CRLs.

5. PHYSICAL, PROCEDURAL, AND PERSONNEL SECURITY CONTROLS

5.1. Physical Controls

5.1.1. Site location and construction

The CESNET CA equipment SHALL be located within a dedicated closed room in the CESNET a. l. e. office area.

5.1.2. Physical access

The physical access to the CESNET CA operating room SHALL be allowed only to the CESNET CA authorized personnel. The keys to the operating room MUST not be taken out of the CESNET a. l. e. office area.

Unauthorized personnel and visitors who require access to secure areas must be escorted by authorized personnel at all times.

5.1.3. Power and air conditioning

The critical CESNET CA equipment is connected to uninterrupted power supply units.

5.1.4. Water exposures

The CESNET CA secure operating room is located on the fourth flour of the building in a building which is not in a flood zone.

5.1.5. Fire prevention and protection

The CESNET CA secure operating room MAY be provided with smoke detectors and/or a fire suppression system. The operating room is located in CESNET a. l. e. premises under continual control.

5.1.6. Media storage

All the media MUST be backed up and stored in fireproof safes in the CESNET a. l. e. office area. Critical backup media MUST also stored off-site (see Section 5.1.8).

5.1.7. Waste disposal

All CESNET CA paper waste MUST be shredded. Magnetic media MUST be physically/mechanically destroyed before disposal.

5.1.8. Off-site backup

Backups of CESNET CA computer operating system and CA software and CESNET CA private keys MUST be stored off site in a bank safe deposit box.

5.2. Procedural Controls

5.2.1. Trusted roles

Responsibilities at the CESNET CA are divided among different trusted roles:

1. *System Administrator* is responsible for:
   a. The CESNET CA equipment maintenance and management.
   b. The security of the CESNET CA equipment.
   c. The regular backups.

2. *Security Officer* is responsible for:
   a. CESNET CA signing key activation.
   b. Trusted roles assignment.
   c. Compliance with the CPS.

3. *Security Auditor* is responsible for:
   a. Audit logs monitoring.

4. *Registration Authority Officer* is responsible for:
   a. Authentication of identities.

5. *Security Trustee*
   a. CESNET CA private key activation assistance.

Different roles can be occupied by one person.

5.2.2. Number of persons required per task

CESNET CA requires at least one Security Officer and one Security Trustee to activate its private signing key.

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 background checks or clearance procedures for trusted roles are required.

5.3.2. Background check procedures

No background checks or clearance procedures are required.

5.3.3. Training requirements

The CESNET CA personnel MUST be trained in:

1. Basic PKI Concepts.

2. The use and operation of the PKI software.

3. The relevant CPs and CPSs.

4. Computer security.

5.3.4. Retraining frequency and requirements

Training MUST be provided to the personnel at least annually.

Training in the use and operation of the PKI software MUST be provided whenever the software is updated.

Any changes in CPs and/or CPS MUST be communicated to the CESNET CA personnel as soon as possible.

5.3.5. Job rotation frequency and sequence

No job rotation has been defined.

5.3.6. Sanctions for unauthorized actions

Unauthorized actions will be dealt with by the director of CESNET a. l. e..

5.3.7. Contracting personnel requirements

Not applicable

5.3.8. Documentation supplied to personnel

The CESNET CA personnel SHOULD be supplied witch documentation including:

- this CPS
- all applicable CPs
- documentation to the CA/RA software

6. TECHNICAL SECURITY CONTROLS

6.1. Key Pair Generation and Installation

6.1.1. Key pair generation

Key pairs for the CESNET CA are generated exclusively by authorized CESNET CA personnel acting in the role of CA.

End entities' key pairs are always generated by their application during the requesting process. They are never generated or stored by the CESNET CA.

6.1.2. Private key delivery to entity

Private keys are never delivered. End entities are required to generate their own key pairs.

6.1.3. Public key delivery to certificate issuer

The CESNET CA SHALL accept certificate requests in any of the formats:

1. PKCS#10 request format.(See RFC 2314).

2. Netscape Signed Public Key And Challenge (SPKAC) format.

The preferred transport method for certification requests is s SSL protected HTTP.

6.1.4. CA public key delivery to users

CA public keys are published on the CESNET CA certificate repository and the CESNET CA WWW site. (See Section 2.6).

6.1.5. Key sizes

The CESNET CA uses RSA public key algorithm.

The CA private key MUST be of 2048 bit key size.

The RA private key MUST be of 2048 bit key size.

All other private keys MUST be of at least 1024 bit key size.

6.1.6. Public key parameters generation

Public key parameters are generated by the relevant applications.

6.1.7. Parameter quality checking

The CESNET CA does not require checking of the quality of the public keys parameters.

6.1.8. Hardware/software key generation

The CESNET CA keys are generated in hardware security module certified to be compliant with FIPS 140-1 level 3.

The subscribers keys MAY be generated in software or hardware.

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

The X.509 v3 `keyUsage` extension field is set according to the requirements stated in the relevant CP.

6.2. Private Key Protection

6.2.1. Standards for cryptographic module

The CESNET CA hardware security module used to generate its signing keys and signatures is compliant with FIPS 140-1 level 3.

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

The CESNET CA does not use multi-person control of keys.

6.2.3. Private key escrow

The CESNET CA private keys are not given in escrow. The CESNET CA is also not available for accepting escrow copies of keys of other parties.

6.2.4. Private key backup

The CESNET CA private keys are backup protected. The backup copies encrypted with 3DES or AES are securely stored off-site.

6.2.5. Private key archival

The CESNET CA private keys are archived on encrypted media.

6.2.6. Private key entry into cryptographic module

All private keys managed by the CESNET CA are generated by the hardware security module and cannot be exported.

6.2.7. Method of activating private key

The CESNET CA's private signing keys are activated by one representative of the Security Officer role and one representative of the Security Trustee role authenticated by a hardware token and a pass phrase..

6.2.8. Method of deactivating private key

Cryptographic modules which have been activated MUST NOT be left unattended. They MUST be deactivated after use, e. g. via logout procedure.

6.2.9. Method of destroying private key

The CESNET CA private keys are archived. After the retention period (see Section 4.6.2) the archive media SHALL be destroyed.

Private keys on magnetic disk can be removed by overwriting the key files.

6.3. Other Aspects of Key Pair Management

6.3.1. Public key archival

Public keys are archived as part of the certificate archival.

6.3.2. Usage periods for the public and private keys

The validity period for issued certificates is set according to the requirements stated in the relevant CP.

6.4. Activation Data

6.4.1. Activation data generation and installation

The pass phrases used by the CESNET CA are at least 15 characters long.

6.4.2. Activation data protection

The CESNET CA private key activation data stored in the physical activation keys protected with a password of minimum 15 characters. The pass phrases MUST be known to authorized CESNET CA personnel only. The pass phrases MUST be used only in secure physic environment.

6.4.3. Other aspects of activation data

No stipulation.

6.5. Computer Security Controls

6.5.1. Specific computer security technical requirements

The CESNET CA computer system MUST satisfy following requirements:

1. The CESNET CA is run on dedicated computer system.
2. Only the software needed to perform the CA tasks is installed on the system.
3. Access to the operating system and the CA software is allowed only to the authorized CESNET CA personnel.
4. Physical access to the system is allowed only to the authorized CESNET CA personnel.
5. All security related events are audited.

The desired functionality MAY be provided by the operating system, the CA software, physical protection or by a combination of those.

6.5.2. Computer security rating

No formal computer security rating is required.

6.6. Life Cycle Technical Controls

6.6.1. System development controls

The development of the CESNET CA software is carried in a controlled secure environment.

Production and development environment are totally separated.

6.6.2. Security management controls

The logs, the configuration files and the entire file system of the CESNET CA computer systems are regularly checked.

6.6.3. Life cycle security ratings

No formal life cycle security rating is required.

6.7. Network Security Controls

The CESNET CA computer system is operated in a controlled network environment protected by packet filtering firewalls.

6.8. Cryptographic Module Engineering Controls

No stipulation.

7. CERTIFICATE AND CRL PROFILES

7.1. Certificate Profile

The certificate profile described in this subcomponent can be overridden by the requirements stated in the relevant CP.

The certificates issued in accordance with this CPS SHOULD follow the RFC 3280 and the PKIX profiles.

7.1.1. Version number(s)

Certificates issued under this CPS are X.509 version 3 certificates. The `version` field in certificates MUST be set to 0x2 to indicate this.

7.1.2. Certificate extensions

This CPS allows using the extensions defined in PKI RFCs and some major vendor extensions. The typical certificate SHOULD populate following extensions:

7.1.2.1. Basic Constraints

CRITICAL

Set to TRUE in CA certificates.

7.1.2.2. Key Usage

CRITICAL

For CA certificates the bits `keyCertSign` and `cRLSign` SHOULD be set to one.

For personal certificates the `keyUsage` extension is set according to the relevant CP.

For server certificates the `keyUsage` extension is set according to the relevant CP.

7.1.2.3. Subject Key Identifier

Unique identifier of the subject key according to RFC 3280.

The `subjectKeyIdentifier` extension is non-critical.

7.1.2.4. Authority Key Identifier

Unique identifier of the issuer key according to RFC 3280.

The `authorityKeyIdentifier` extension is non-critical.

7.1.2.5. Subject Alternative Name

The `subjectAltName` extension SHOULD contain names provided by the subscriber in the formats specified in RFC 3280.

The `subjectAltName` extension is non-critical.

7.1.2.6. CRL Distribution Points

URIs of the current CRL.

The `cRLDistributionPoint` extension is non-critical.

7.1.2.7. Certificate Policies

The OID of the relevant CP without any qualifiers.

The `certificatePolicies` extension is non-critical.

7.1.3. Algorithm object identifiers

The CESNET CA issues certificates using following algorithms:

7.1.3.1. Signature algorithms

`sha-1WithRSAEncryption`
{ iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 5 }

7.1.3.2. Subject public key algorithms

`rsaEncryption`
{ iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) 1 }

7.1.4. Name forms

See Section 3.1.1.

7.1.5. Name constraints

No stipulation.

7.1.6. Certificate policy Object Identifier

The certificates issued under this CPS SHOULD populate the the `certificatePolicies` extension with the OID of the relevant CP without any qualifiers.

7.1.7. Usage of Policy Constraints extension

No stipulation.

7.1.8. Policy qualifiers syntax and semantics

The certificates issued under this CPS 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)

CRLs issued by the CESNET CA are version X.509 version2 CRLs. This is indicated by setting the `version` field in the CRL to value of 1.

7.2.2. CRL and CRL entry extensions

Following CRL and CRL entry extensions are used:

7.2.2.1. Authority Key Identifier

Unique identifier of the issuer key according to RFC 3280.

The `authorityKeyIdentifier` extension is non-critical.

7.2.2.2. CRL Number

Monotonically increasing sequence number for each CRL issued by the CA according to RFC 3280.

The `cRLNumber` extension is non-critical.

7.2.2.3. CRL Reason Code

The revocation reason code as specified in RFC 3280.

The `reasonCode` CRL entry extension is non-critical.

8. SPECIFICATION ADMINISTRATION

8.1. Specification change procedures

Suggested changes to this CPS MUST be communicated to the contact person (see Section 1.4).

The significance of the change is evaluated by the CESNET CA. If the change is determined to influence the trust procedures of relying parties and/or cooperating CAs, the CESNET CA MUST assign a new OID to the modified CPS.

Minor editorial or typographical changes to this CPS MAY be made without approval.

All changes MUST be communicated to the interested parties. See Section 8.2.

8.2. Publication and notification policies

The CPS is published on http://www.cesnet.cz/pki/CPS.html.

8.3. CPS approval procedures

Not applicable.

Glossary

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

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.

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.

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).

Relevant CP
The CP under which the certificate is being issued.

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.

References

[EuroPKI] *EuroPKI Certificate Policy : VERSION 1.1 (DRAFT 4)*. October 2000. http://www.europki.org/ca/root/.

[RFC 791] *Internet Protocol*. J. Postel. RFC 791. September 1981.

[RFC 822] *Standard for the format of ARPA Internet text messages*. D. Crocker. RFC 822. August 1992.

[RFC 1034] *Domain Names - Concepts and Facilities*. P. Mockapetris. RFC 1034. November 1987.

[RFC 1883] *Internet Protocol, Version 6 (IPv6) Specification*. S. Deering and R. Hinden. RFC 1883. December 1995.

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

[RFC 2314] *PKCS #10 : Certification Request Syntax Version 1.5*. B. Kaliski. RFC 2314. February 1993.

[RFC 3280] *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*. R. Housley, W. Polk, W. Ford, and D. Solo. RFC 3280. April 2002.

[RFC 2527] *Internet X.509 Public Key Infrastructure : Certificate Policy and Certification Practices Framework*. S. Chokhani and W. Ford. RFC 2527. March 1999.

[X.501] *ITU-T Recommendation X.501 - Information technology - Open Systems Interconnection - The Directory: Models*.

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.)