CESNET CA Basic Level Certificate Policy
and
Certification Practice Statement

Version 3.1

Table of Contents

1 Introduction

This Certificate Policy and Certification Practice Statement (CP/CPS) defines the Basic Level certificate policy and practices for use by the CESNET CA when issuing public key certificates.

This document is formatted according to RFC 3647 [RFC3647]. There are some sections that are maintained for compatibility although they do not apply exactly to the services required by this Certificate Policy. These sections contain the text “No stipulation”.

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 [RFC2119].

1.1 Overview

This CP/CPS describes the requirements which MUST be met by CESNET CA in issuing digital public key certificates.

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

1.2 Document name and identification

This document is *CESNET CA Basic Level Certificate Policy and Certification Practice Statement* version 3.1. This policy is uniquely identified by the following identifier: 1.3.6.1.4.1.8057.1.2.2.3.1.

ISO assigned	1
ISO Identified organization	3
US Department of Defense	6
Internet	1
Internet Private	4
IANA registered private enterprises	1
CESNET	8057
PKI	1
Certificate Policies	2
CESNET CA Basic Level Certificate Policy	2
Major Version	3
Minor Version	1

1.3 PKI participants

1.3.1 Certification authorities

The CESNET CA is part of CESNET PKI services. It is operated by CESNET, a. l. e. to issue public key certificates to persons, hosts and applications for use within the Czech academic community.

The CESNET CA is an on-line CA, subordinate to the CESNET CA Root CA.

Requirements described in this CP/CPS are binding for the CESNET CA when issuing Basic Level public key certificates.

1.3.2 Registration authorities

This CP/CPS is binding for Registration Authorities (RA) operated by the CESNET CA or on behalf of the CESNET CA.

1.3.3 Subscribers

The CESNET CA SHALL issue certificates to employees and students of Czech universities, Czech Academy of Sciences, and any organization cooperating with these entities in the practice of research, educational and administrative functions as well as to computers and application services operated by these organizations.

1.3.4 Relying parties

This CP/CPS does not limit the community of relying parties.

1.3.5 Other participants

No stipulation.

1.4 Certificate usage

1.4.1 Appropriate certificate uses

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

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

1.4.2 Prohibited certificate uses

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

1.5 Policy administration

1.5.1 Organization administering the document

CESNET PKI
CESNET, a. l. e.
Zikova 4
106 00 Praha 6
Czech Republic

Email: ca@cesnet.cz

1.5.2 Contact person

Policy Administrator is appointed by CESNET, a. l. e. Contact details are published at the CESNET PKI repository (see Section 2.1).

1.5.3 Person determining CPS suitability for the policy

CPS suitability for the CP is determined by the Policy Administrator (see Section 1.5.2).

1.5.4 CPS approval procedures

Proposed changes to this CP/CPS MUST be delivered to the Policy Administrator. The Policy Administrator informs the requester about the review results within one month.

1.6 Definitions and acronyms

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.

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

Certificate policy (CP)
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.

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

Certificate revocation list (CRL)
A time stamped list identifying revoked certificates which is signed by a CA.

Issuing certification authority
In the context of a particular certificate, the issuing CA is the CA that issued the certificate.

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 (RA)
An entity that is responsible for identification and authentication of certificate subjects and for accepting revocation requests, 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.

2 Publication and repository responsibilities

2.1 Repositories

The CESNET CA SHALL operate a publicly accessible repository to publish its certificates, Certificate Revocation Lists (CRLs), and relevant public documentation. The repository SHALL be accessible at

http://www.cesnet.cz/pki.

2.2 Publication of certification information

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

1. The CESNET CA certificate,
2. the current version of this CP/CPS,
3. all previous versions of the CESNET CA CP, CPS, and CP/CPS that were in effect for issuing certificates,
4. the current version of the CESNET CA CRL.

In addition, the CESNET PKI SHALL make publicly available in it repositories:

1. The CESNET Root CA certificate,
2. the current version of the CESNET Root CA CP/CPS,
3. all previous versions of the CESNET Root CA CP, CPS and CP/CPS that were in effect for issuing certificates,
4. the current version of the CESNET Root CA CRL.

2.3 Time or frequency of publication

This CP/CPS is published before issuing the first certificate under this CP/CPS.

New versions of this CP/CPS are published at least seven days before issuing the first certificate under the new version of the CP.

2.4 Access controls on repositories

Information listed in Section 2.2 SHALL be publicly available.

The information published in the repository SHALL be protected against any unauthorized modification.

3 Identification and authentication

3.1 Naming

3.1.1 Types of names

The CESNET CA assigns each entity a non-empty X.501 Distinguished Name (DN) 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.

All end-entity subject DNs SHALL start with an invariable part identifying the issuing CA (`dc=cesnet-ca, dc=cz`). The subsequent variable part MAY consist of the following attributes:

Organization

Attribute name	O
OID	2.5.4.10
Necessity	required
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 the CESNET CA requires an evidence of the affiliation.

Organizational Unit

Attribute name	OU
OID	2.5.4.5
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 the CESNET CA requires an evidence of the affiliation.

Common Name

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

Subscribers MAY request including other types of names in their certificates, such as email addresses, DNS host names, IP addresses, or URIs. These names MAY be included in the subjectAltName certificate extension in accordance with RFC 5280 [RFC5280] if allowed by the requested certificate profile (see Section 7.1).

3.1.2 Need for names to be meaningful

The 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 subscriber.

3.1.3 Anonymity or pseudonymity of subscribers

The CESNET CA MUST be able to trace every name it certifies to the respective subscriber.

3.1.4 Rules for interpreting various name forms

Names in certificates SHALL be interpreted according to RFC 5280 [RFC5280].

3.1.5 Uniqueness of names

Every Subject DN SHALL be associated with exactly one entity.

3.1.6 Recognition, authentication, and role of trademarks

No stipulation.

3.2 Initial identity validation

3.2.1 Method to prove possession of private key

The requester MUST prove possession of the private key which corresponds to the public key in the certificate request. The possession SHAL be proved by submitting a digitally signed PKCS#10 request or by providing another cryptographically equivalent demonstration.

3.2.2 Authentication of organization identity

Organizations are authenticated using officially recognized documents. The CESNET CA MAY use third party services to confirm the identity of an organization.

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

3.2.3 Authentication of individual identity

Individuals MUST be authenticated using officially recognized identity documents containing a photograph of the individual. The registering RA MUST meet the requester 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 acceptable for authentication.

3.2.4 Non-verified subscriber information

All names in the certificate SHALL be verified by the CESNET CA.

3.2.5 Validation of authority

When a subscriber requests the inclusion of the name of a certain organization in a certificate, he/she MUST provide an evidence that the organization has approved the request (see Section 3.2.2).

The requester asking for a certificate for a server or a software component MUST prove that he/she has the necessary authorization by providing a signed statement made by the representatives of the organization operating the server/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 or a Certification Authority recognized by the CESNET CA for authenticating persons. The list of recognized CAs is maintained in Appendix A .

3.2.5.1 Validation of authority for eduroam® RADIUS/TLS certificates

The requester asking for for a certificate for an eduroam® RADIUS/TLS certificate MUST provide a proof of his/her email address as registered with the corresponding eduroam® National Roaming Operator. A personal certificate asserting the email address issued by the CESNET CA or a CA recognized for authenticating persons is accepted as the proof. The eduroam® National Roaming Operator MUST approve issuing the requested certificate to the requester identified by the provided email address.

3.2.6 Criteria for interoperation

No stipulation.

3.3 Identification and authentication for re-key requests

3.3.1 Identification and authentication for routine re-key

After a certificate expiration, the CESNET CA MUST NOT issue a new certificate for the same key. The CA MAY issue a new certificate for a new key.

The re-key authentication MAY be accomplished with the same procedure as for initial registration or using a request digitally signed with the private key

corresponding to the old certificate. The old certificate MUST be valid at the time of the request delivery to the CA.

3.3.2 Identification and authentication for re-key after revocation

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

A new certificate may be issued only after authenticating the request with the same procedure as for initial registration.

3.4 Identification and authentication for revocation request

A revocation request made by a requester who can prove his/her possession of the private key corresponding to the certificate MUST be considered authenticated and accepted.

Requesters not in possession of the private key corresponding to the certificate MUST be authenticated using the same procedure as for initial registration or by validating the digital signature using a valid personal certificate issued by the CESNET CA or a CA recognized for personal authentication (see Appendix A).

4 Certificate life-cycle operational requirements

4.1 Certificate Application

4.1.1 Who can submit a certificate application

A certificate application may be issued by an eligible entity.

An entity submitting a certificate application MUST be registered with the CA system in compliance with Section 3.2.

4.1.2 Enrollment process and responsibilities

The enrollment process usually follows the following steps:

1. The requester submits a certificate application.
   - The application MUST contain the public key request to be certified.
   - The application MUST contain all the names requested to be certified.
   - The application MUST identify the requested type of certificate.
   - The application MUST be delivered using a secure and authenticated method, i. e. using the secured CA web interface or a signed email.
2. The Registration Authority verifies the application. If the application is accepted, the RA issues a one-time authentication token to the requester. The token MUST be passed during a face-to-face meeting with the requester or using a message encrypted using the requester's valid personal certificate.
3. The requester requests the certificate from the CA's enrollment application using the one-time authentication token for authentication.
4. The CA's enrollment application issues the certificate and delivers it to the requester.

4.2 Certificate application processing

4.2.1 Performing identification and authentication functions

Registration Authority MUST verify the identity and authorization of a requester using either

- an official personal photo ID during a face-to-face meeting or
- a personal certificate of the requester to verify the signature on the electronically signed certificate application.

4.2.2 Approval or rejection of certificate applications

Registration Authority SHALL approve a certificate application only if

- the identity of an requester has been properly verified,
- all names requested to be included in the certificate have been properly verified,
- all names requested to be included in the certificate have been authorized by their respective owners.

Otherwise, the application SHALL be rejected.

4.2.3 Time to Process Certificate Applications

A Registration Authority SHOULD act on a certificate application within two business days.

4.3 Certificate issuance

4.3.1 CA actions during certificate issuance

The CESNET CA SHALL verify requester's identity using the one-time authentication token issued by to the requester the RA (see Section 4.1.2).

The CESNET CA SHOULD verify the quality of the public key supplied by the requester according to the actual status of knowledge about weak and compromised keys.

After successful verification of requester's identity and the quality of the supplied key, the CESNET CA SHALL assemble the certificate from the data obtained during the registration process and issue it.

4.3.2 Notification to subscriber by the CA of issuance of certificate

The issued certificate is delivered to the requester during his/her session with the enrollment application. No other notification SHALL be provided.

4.4 Certificate acceptance

4.4.1 Conduct constituting certificate acceptance

A certificate SHALL be deemed to be accepted by a requester at the time of the certificate's delivery to the requester.

4.4.2 Publication of the certificate by the CA

The CESNET CA SHALL NOT publish the issued certificates.

4.4.3 Notification of certificate issuance by the CA to other entities

The CESNET CA SHALL NOT notify other entities of certificate issuance.

4.5 Key pair and certificate usage

4.5.1 Subscriber private key and certificate usage

A private key corresponding to a certificate issued by the CESNET CA may be used only in compliance of this CP/CPS and the intended key usage as specified in the certificate.

4.5.2 Relying party public key and certificate usage

Relying party MUST before relying on a certificate:

- use the certificate in compliance with this CP/CPS,
- verify that the certificate has not been revoked,
- verify that the signature to rely on was created within the validity period of the certificate, and
- use the certificate in accordance with the specific purpose for which it has been issued.

4.6 Certificate renewal

The CESNET CA SHALL NOT support certificate renewal.

4.6.1 Circumstance for certificate renewal

Not applicable.

4.6.2 Who may request renewal

Not applicable.

4.6.3 Processing certificate renewal requests

Not applicable.

4.6.4 Notification of new certificate issuance to subscriber

Not applicable.

4.6.5 Conduct constituting acceptance of a renewal certificate

Not applicable.

4.6.6 Publication of the renewal certificate by the CA

Not applicable.

4.6.7 Notification of certificate issuance by the CA to other entities

Not applicable.

4.7 Certificate re-key

4.7.1 Circumstance for certificate re-key

The CESNET CA SHALL NOT issue a new certificate for a public key that has already been submitted to it in a certificate application. Every non-first certificate for a subscriber MUST be obtained via a re-keying or certificate modification procedure.

A subscriber MAY request for a certificate re-key at his/her own discretion.

Information within the certificate MUST be valid and complete at the time of delivery of the re-key request.

The CESNET CA SHALL NOT support certificate re-keying for eduroam® RADIUS/TLS certificates. All applications for eduroam® RADIUS/TLS certificates SHALL be treated as initial Certificate Applications.

4.7.2 Who may request certification of a new public key

Only the subscriber may request a certificate re-keying.

4.7.3 Processing certificate re-keying requests

Registration Authority receiving the re-keying request MUST approve the request only if:

- the identity of the requester can has been verified in accordance with Section 3.3,
- the information within the current certificate is valid and complete,
- the requester is eligible for the certificate.

Otherwise, the request MUST be rejected.

Approved re-keying requests are processed in accordance with statements in Sections 4.2 and 4.3.

4.7.4 Notification of new certificate issuance to subscriber

See Section 4.3.2.

4.7.5 Conduct constituting acceptance of a re-keyed certificate

See Section 4.4.1.

4.7.6 Publication of the re-keyed certificate by the CA

See Section 4.4.2.

4.7.7 Notification of certificate issuance by the CA to other entities

See Section 4.4.3.

4.8 Certificate modification

4.8.1 Circumstance for certificate modification

A certificate MUST be modified when information in the certificate other than the public key changes and becomes invalid or incomplete.

The CESNET CA SHALL NOT support certificate modification procedures for eduroam® RADIUS/TLS certificates. All applications for eduroam® RADIUS/TLS certificates SHALL be treated as initial Certificate Applications.

4.8.2 Who may request certificate modification

Only the subscriber may request a change of the `Common Name` in the certificate subject name.

Only the subscriber or the organization whose name should be included in the modified certificate may request a change of the `Organization` attribute in the certificate subject name.

A change in other names in the certificate may be requested by the subscriber or the organization managing the respective names.

4.8.3 Processing certificate modification requests

Registration Authority receiving the modification request MUST approve the request only if:

- the identity of the requester has been verified in accordance with procedures described in Section 4.2.1,
- the requested content of the modified certificate is valid and complete,

- the subscriber is eligible for the certificate.

A request for a change of a common name in the certificate subject MUST be verified in accordance to Section 3.2.3.

A request for a change of an organizational name in the certificate subject MUST be verified in accordance to Section 3.2.2.

Approved modification requests are processed in accordance with statements in Sections 4.2 and 4.3.

4.8.4 Notification of new certificate issuance to subscriber

See Section 4.3.2.

4.8.5 Conduct constituting acceptance of modified certificate

See Section 4.4.1.

4.8.6 Publication of the modified certificate by the CA

See Section 4.4.2.

4.8.7 Notification of certificate issuance by the CA to other entities

See Section 4.4.3.

4.9 Certificate revocation and suspension

4.9.1 Circumstances for revocation

A certificate SHALL be revoked when any of the following circumstances occurs:

- the private key corresponding to the certificate is compromised or suspected to be compromised or lost;
- the subscriber's data has changed;
- the subscriber has violated his/her obligations;
- the certificate has not been issued in accordance with this CP/CPS;
- the end-entity is no longer eligible for the certificate;
- the CESNET CA terminates operation (see Section 5.8.2).

4.9.2 Who can request revocation

The CESNET CA SHALL accept a revocation request made by the entity in possession of the corresponding private key.

Other entities MAY request revocation, presenting proof of a reason for revocation.

4.9.3 Procedure for revocation request

The party requesting a certificate revocation SHALL submit the revocation request to a CESNET CA Registration Authority or to the CESNET CA.

The entity receiving a revocation request SHALL immediately revoke the certificate if

- the requester has been properly authenticated in accordance with Section 3.4 and
- the conditions for revocation have been fulfilled in accordance with Section 4.9.1.

The RA SHALL inform the requester about the outcome of the revocation procedure.

4.9.4 Revocation request grace period

Any party that becomes aware of circumstances for revocation SHALL request a revocation as soon as possible but not later than within one business day.

4.9.5 Time within which CA must process the revocation request

The Registration Authority SHALL act on a revocation request within one business day.

4.9.6 Revocation checking requirement for relying parties

Relying parties MUST check the revocation status of a certificate on which they are relying including the revocation status of all certificates in its certification path.

4.9.7 CRL issuance frequency (if applicable)

The CESNET CA SHALL issue a CRL at leas every 24 hours or immediately after a certificate revocation. The `nextUpdate` field of a CRL SHALL be set to the time 5 days after its issuance.

4.9.8 Maximum latency for CRLs (if applicable)

The CESNET CA SHALL publish a new CRL immediately after its issuance.

4.9.9 On-line revocation/status checking availability

The CESNET CA SHALL operate an OCSP service.

4.9.10 On-line revocation checking requirements

Relying parties MAY use OCSP for checking a revocation status of certificates.

4.9.11 Other forms of revocation advertisements available

No stipulation.

4.9.12 Special requirements re key compromise

No stipulation.

4.9.13 Circumstances for suspension

The CESNET CA SHALL NOT support certificate suspension.

4.9.14 Who can request suspension

Not applicable.

4.9.15 Procedure for suspension request

Not applicable.

4.9.16 Limits on suspension period

Not applicable.

4.10 Certificate status services

4.10.1 Operational characteristics

The CESNET CA SHALL issue direct, full and complete CRLs, i. e. every CRL contains serial numbers of all non-expired revoked certificates issued by the CA.

The OCSP service operated by the CESNET CA SHALL provide revocation status of all non-expired certificates.

4.10.2 Service availability

The current CRL SHALL be available for download continuously.

The OCSP service SHALL be available continuously.

4.10.3 Optional features

No stipulation.

4.11 End of subscription

A subscriber may request end of his/her subscription at his/her own discretion.

On receiving a subscription end request, the Registration Authority SHALL revoke all valid certificates issued to the subscriber and the Conforming CA SHALL cease providing services to the subscriber.

4.12 Key escrow and recovery

The CESNET CA SHALL NOT provide key escrow service.

4.12.1 Key escrow and recovery policy and practices

Not applicable.

4.12.2 Session key encapsulation and recovery policy and practices

Not applicable.

5 Facility, management, and operational controls

5.1 Physical Controls

5.1.1 Site location and construction

Systems of the CESNET CA SHALL be located at a dedicated closed, secure and safe location.

5.1.2 Physical access

Physical access to systems of the CESNET CA SHALL be monitored and restricted to authorized personnel only.

5.1.3 Power and air conditioning

Systems of the CESNET CA SHALL be connected to an uninterruptible power supply unit.

5.1.4 Water exposures

Systems of the CESNET CA SHALL be located at a location outside of a flood zone.

5.1.5 Fire prevention and protection

Fire prevention and protection of the CESNET CA site is covered by the CESNET, a. l. e. fire prevention policy.

5.1.6 Media storage

Physical access to removable media of the CESNET CA SHALL be restricted to authorized personnel only.

All the media SHALL be backed up and stored in fireproof safes in the CESNET, a. l. e. office area.

Critical backup media SHALL also stored off-site (see Section 5.1.8).

5.1.7 Waste disposal

The CESNET CA SHALL dispose its waste using procedures preventing using the waste to access any operational information, namely:

- all paper waste SHALL be shredded,
- all magnetic media SHALL be physically/mechanically destroyed before disposal.

5.1.8 Off-site backup

Backups of CESNET CA private keys SHALL be stored off-site.

5.2 Procedural controls

5.2.1 Trusted roles

Responsibilities at the CESNET CA SHALL be divided among different trusted roles:

- *System Administrator*
  - manages PKI hardware and software
- *Security Officer*
  - manages and activates CA signing keys
- *Security Trustee*
  - assists during CA signing key activation
- *CA Operator*
  - manages CA system configuration
- *RA Officer*
  - manages subscribers registration and records, revocation request and other communication with subscribers
- *Auditor*
  - performs system audits

5.2.2 Number of persons required per task

Activation of the CESNET CA signing key SHALL require cooperation of two persons, one of them in the role of *Security Officer*, the other one in the role of *Security Trustee*.

5.2.3 Identification and authentication for each role

System Administrator SHALL be authenticated with a user name and password.

Security Officer SHALL be authenticated with a personal certificate. The private key to the certificate SHALL be stored within a hardware cryptographic module complying with FIPS 140-2 level 2 or higher.

Security Trustee SHALL be authenticated with a personal RFID chip.

CA Operator SHALL be authenticated with a personal certificate. The private key to the certificate SHALL be stored within a hardware cryptographic module complying with FIPS 140-2 level 2 or higher.

RA Officer SHALL be authenticated with a personal certificate. The private key to the certificate SHALL be stored within a hardware cryptographic module complying with FIPS 140-2 level 2 or higher.

Auditor SHALL be authenticated with a personal certificate.

5.2.4 Roles requiring separation of duties

Roles of *Security Officer* and *Security Trustee* SHALL NOT be shared by one individual.

5.3 Personnel controls

5.3.1 Qualifications, experience, and clearance requirements

The personnel of the CESNET CA SHALL be technically and professionally competent.

5.3.2 Background check procedures

No stipulation.

5.3.3 Training requirements

The CESNET CA personnel SHALL be trained in:

- basic PKI concepts,
- the use and operation of the PKI software,
- the relevant documentation including the CP/CPS,
- computer security.

5.3.4 Retraining frequency and requirements

Training SHALL be provided to the personnel at least annually.

Training in the use and operation of the PKI software SHALL be provided whenever the software is updated or changed.

Any change in CP/CPS SHALL 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 Independent contractor requirements

No stipulation.

5.3.8 Documentation supplied to personnel

The CESNET CA personnel SHAL be supplied with documentation required for their operation including but not limited to:

- the relevant CP, CPS, or CP/CPS
- documentation of the PKI software.

5.4 Audit Logging Procedures

5.4.1 Types of events recorded

The CESNET CA SHALL record the following events:

- registration of a subscriber,
- certificate applications,
- certificate issuance,
- certificate revocation requests,
- certificate revocation,
- CRL issuance,
- initiation of the CA systems,
- activation and deactivation of the CA's signing key,
- access to CA systems.

5.4.2 Frequency of processing log

Logs SHALL be processed monthly or immediately after discovering a security incident.

5.4.3 Retention period for audit log

Logs SHALL be retained for at least five years.

5.4.4 Protection of audit log

Access to logs SHALL be restricted to authorized personnel only namely the CA personnel and the auditors.

Logs SHALL be protected against lost and modification.

5.4.5 Audit log backup procedures

Audit logs are SHALL be backed up with other CA data.

5.4.6 Audit collection system (internal vs. external)

The audit collection system is internal to the CESNET CA.

5.4.7 Notification to event-causing subject

The subjects causing an audit event are generally not notified.

5.4.8 Vulnerability assessments

Audit logs SHALL be regularly monitored to find potential security incidents and non-standard events.

5.5 Records archival

5.5.1 Types of records archived

The CESNET CA SHALL archive:

- software,
- the CA certificate,
- issued certificates,
- issued CRLs,
- audit logs,
- all implemented CPs and CPSs,
- operational documentation.

5.5.2 Retention period for archive

The CESNET CA SHALL archive items listed in Section 5.5.1 for at least five years.

5.5.3 Protection of archive

Archived information SHALL be accessible to authorized personnel only namely the CA personnel and the auditors.

5.5.4 Archive backup procedures

Archive records SHALL be regularly moved to an archive media. The media SHALL be stored in a secure place.

5.5.5 Requirements for time-stamping of records

No stipulation.

5.5.6 Archive collection system (internal or external)

The archive collection system is internal to the CESNET CA.

5.5.7 Procedures to obtain and verify archive information

Access to archive SHALL be recorded.

5.6 Key changeover

The following steps SHOULD be taken when re-keying the signing key of the CESNET CA:

1. A new certificate with the new key for the CA SHALL be issued.
2. The new certificate SHALL be published in accordance with Section 2.2.
3. The new certificate is used for issuing certificates. Both the new and the old certificate may be active at the same time. The old key SHALL be used as long as all certificates signed by it have not expired.

5.7 Compromise and disaster recovery

5.7.1 Incident and compromise handling procedures

In case of an incident that might lead to compromising integrity of a CA system, the CA personnel SHALL initiate the incident analysis immediately. Further steps depend on the outcome of the analysis.

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

In case of hardware corruption, the system SHALL be recovered from backup to a new hardware and brought into operation.

In case of software or data corruption, the system SHALL be recovered from backup and brought into operation.

5.7.3 Entity private key compromise procedures

When the signing key of the CESNET CA is compromised, the CA SHALL:

1. immediately request revocation the corresponding CA certificate(s),
2. stop operations,
3. inform users about the incident,

4. eliminate the circumstances that lead to the compromise,
5. generate a new key pair,
6. request a new certificate for the CA,
7. restart the CA operations with the new certificate.

Whenever the subscriber's key is compromised, the subscriber is obliged to notify the CESNET CA as soon as possible. The revocation procedure will follow according to Section 4.9.

5.7.4 Business continuity capabilities after a disaster

After a disaster, the CESNET CA SHALL recover its systems from backup and restart operations. The outage SHOULD NOT take longer than 5 business days.

5.8 CA or RA Termination

5.8.1 RA Termination

The CESNET CA SHALL announce a Registration Authority termination to its customers.

The terminating RA SHALL hand over all its documentation to the CA.

The CESNET CA SHALL disable the terminated RA access to the CA systems.

5.8.2 CA Termination

The CESNET CA SHALL announce its intent to terminate its operation at least three months in advance.

Before terminating its operations CESNET CA SHALL:

- revoke all issued certificates,
- publish the CRL with the `nextUpdate` field set to a time after the expiration dates of all issued Certificates
- request its CA certificate revocation,
- destroy the private keys in possession of the CA,
- archive all relevant information in accordance with Section 5.5.

6 Technical security controls

6.1 Key pair generation and installation

6.1.1 Key pair generation

The CESNET CA SHALL generate and store its private keys in a hardware security module by authorized personnel.

Private keys for *CA Operators*, *RA Officers*, and *Security Officers* SHALL be generated as non-exportable objects in hardware security modules.

Subscribers SHALL be responsible for generating their private keys.

6.1.2 Private key delivery to subscriber

The CESNET CA SHALL NOT generate private keys for subscribers.

6.1.3 Public key delivery to certificate issuer

Subscribers SHALL deliver their public keys in a form of PKCS#10 or in other digitally signed format.

6.1.4 CA public key delivery to relying parties

The CESNET CA SHALL publish its certificates in its repository (see Section 2.2).

6.1.5 Key sizes

An RSA signing key of the CESNET CA SHALL be at least 2048 bits long.

RSA keys of *CA Operators*, *RA Officers*, and *Security Officers* SHALL be at least 2048 bits long.

RSA keys of eduroam® server certificates SHALL be at least 2048 bits long.

RSA keys of other end-entities SHALL be at least 1024 bits long.

6.1.6 Public key parameters generation and quality checking

The CESNET CA SHOULD refuse to certify public keys not matching its quality requirements.

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

Certificates and private keys MUST be used only in accordance with this policy and for the purpose specified in the Key Usage extension.

6.2 Private key protection and cryptographic module engineering controls

6.2.1 Cryptographic module standards and controls

Hardware security modules used to generate and store signing keys of the CESNET CA shall be certified to FIPS 140-2 Level 3 or higher.

Cryptographic modules used to generate and store private keys of *CA Operators*, *RA Officers* and *Security Officers* SHALL comply with requirements of FIPS 140-2 Level 2 or higher.

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

See Section 6.4.2.

6.2.3 Private key escrow

The CESNET CA SHALL NOT support private key escrow.

6.2.4 Private key backup

Private keys of a Conforming CA SHALL be backed up using procedures and tools provided by the HSM used.

Private keys of the *CA Operators*, *RA Officers* and *Security Officers* SHALL NOT be backed up.

Subscribers SHALL be responsible for back up of their private keys. Their private-key backups MUST always be encrypted using a key known only to the authorized personnel.

6.2.5 Private key archival

The CESNET CA SHALL NOT archive private keys.

6.2.6 Private key transfer into or from a cryptographic module

Private keys of the CESNET CA SHALL be generated in an HSM and SHALL be usable only in the HSM. The private key SHALL be transferred from the HSM only as part of an encrypted backup of the HSM.

Private keys of the *CA Operators*, *RA Officers* and *Security Officers* SHALL NOT be transferred into or from the cryptographic module.

6.2.7 Private key storage on cryptographic module

Private keys of CESNET CA SHALL be stored in an HSM in an encrypted form.

Private keys of *CA Operators*, *RA Officers* and *Security Officers* SHALL be stored in hardware cryptographic modules in an encrypted form.

6.2.8 Method of activating private key

Activation of a private key of the CESNET CA SHALL require cooperation of two persons: a *Security Trustee* to insert a smart cart in the HSM reader and a *Security Officer* to provide the PIN for the card. Every activation of a CESNET CA signing key is recorded.

Private keys of *CA Operators*, *RA Officers* and *Security Officers* SHALL be activated by providing a PIN for the cryptographic module.

Personal private keys SHALL never be stored unencrypted.

Server private keys MAY be stored unencrypted only in the key store used by the pertinent server. In that case, appropriate measures must be used to protect the key from unauthorized access.

6.2.9 Method of deactivating private key

Private keys of the CESNET CA SHALL be deactivated by terminating the CA application.

Private keys of *CA Operators*, *RA Officers* and *Security Officers* SHALL be deactivated by disconnecting the cryptographic module from the operating system.

6.2.10 Method of destroying private key

Private keys of the CESNET CA SHALL be destroyed using procedures and tools of the HSM.

6.2.11 Cryptographic module rating

See Section 6.2.1.

6.3 Other aspects of key pair management

6.3.1 Public key archival

The CESNET CA SHALL archive its public keys and all public keys submitted as part of a certificate application.

6.3.2 Certificate operational periods and key pair usage periods

The CA-Certificate of the CESNET CA SHALL be valid for 20 years.

Operational period of end-entity certificates SHALL be at most 13 months.

Key pair usage period is identical to the operational period of the corresponding certificate.

6.4 Activation data

6.4.1 Activation data generation and installation

Activation data for an HSM of the CESNET CA SHALL be generated during configuration of the HSM using procedures and tools of the HSM. The activation data SHALL be generated within a dedicated smart card protected by a PIN at least 12 characters long.

Activation data for cryptographic modules of *CA Operators*, *RA Officers* and *Security Officers* SHALL be generated by the holder of the cryptographic module during the module initialization.

Activation data for end-entities private keys SHALL be generated by subscribers. End-entities' private keys SHOULD be protected by activation data equivalent to a pass phrase of at least 12 characters.

6.4.2 Activation data protection

The smart card holding the activating data for the CESNET CA private key SHALL be physically accessible only to the personnel in the role of *Security Trustee*. The PIN needed to unlock the activation data SHALL be known only to the CA personnel in the role of *Security Officer*.

Holders of activation data SHALL be responsible for the protection of their activation data.

Activation data MUST NOT be kept in unencrypted form.

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 systems SHALL satisfy the following requirements:

- The issuing system is run on a dedicated computer system.
- No software not required for the CA operation is installed on the issuing system.
- Relevant security patches and updates are regularly applied.

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

Significant modification of CA systems SHALL be developed and tested on a separated development system.

6.6.2 Security management controls

No stipulation.

6.6.3 Life cycle security controls

No formal life cycle security rating is required.

6.7 Network security controls

All publicly accessible systems of a Conforming CA SHALL be connected only to a dedicated network isolated from the public Internet with a packet filtering firewall.

The network traffic accessing the CA systems SHALL be monitored.

6.8 Timestamping

No stipulation.

7 Certificate, CRL, and OCSP profiles

7.1 Certificate Profile

The CESNET CA SHALL issue certificates in accordance with RFC 5280 [RFC5280].

7.1.1 Version number(s)

The CESNET CA SHALL issue certificates X.509 version 3.

7.1.2 Certificate extensions

The CA certificate of the CESNET CA SHALL use the following extensions:

a) **Basic Constraints** (critical)
CA: true

b) **Key Usage**
Certificate Sign, *CRL Sign*

c) **Subject Key Identifier**
key identifier of the CA

d) **Authority Key Identifier**
key identifier of the parent CA

e) **CRL Distribution Point**
locator of the parent CA CRL

End-entity certificates SHOULD typically use the following extensions:

a) **Basic Constraints** (critical)
CA: false

b) **Key Usage**
Digital Signature, Key Encipherment

c) **Extended Key Usage**
for personal certificates:
- TLS client authentication (OID 1.3.6.1.5.5.7.3.2),
- Email protection (OID 1.3.6.1.5.5.7.3.4)

for server certificates:
- TLS server authentication (OID 1.3.6.1.5.5.7.3.1),
- TLS client authentication (OID 1.3.6.1.5.5.7.3.2) [optional]

d) **Subject Key Identifier**
key identifier of the subscriber

e) **Authority Key identifier**
key identifier of the CESNET CA signing key

f) **Certificate Policies**
Policy ID: *1.3.6.1.4.1.8057.1.2.2.3.1 (this CP/CPS),*
Policy ID: 1.2.840.113612.5.2.2.1 (IGTF's "Authentication Profile for Classic X.509 Authorities with secured infrastructure") [IGTF-Classic]

g) **Authority Information Access**
OCSP: URI: CESNET CA OCSP locator
CA Issuers: URI: locator of the DER-encoded CESNET CA certificate

h) **CRL Distribution Point**
URI: locator of the current DER-encoded CESNET CA CRL

i) **Subject Alternative Name**
for personal certificates:
- *rfc822Name*: email address(es) of the subscriber

for server certificates:
- *dNSName*: DNS name(s) of the server
- *iPAddress*: IP address(es) of the server [optional]

End-entity certificates issued to eduroam® servers SHALL use the following extensions:

j) **Basic Constraints** (critical)
CA: false

k) **Key Usage**
Digital Signature, Key Encipherment

l) **Extended Key Usage**
- *TLS server authentication (OID 1.3.6.1.5.5.7.3.1),*
- *TLS client authentication (OID 1.3.6.1.5.5.7.3.2)*

m) **Subject Key Identifier**
key identifier of the subscriber

n) **Authority Key identifier**
key identifier of the CESNET CA signing key

o) **Certificate Policies**
Policy ID: *1.3.6.1.4.1.8057.1.2.2.3.1 (this CP/CPS),*
Policy ID: 1.3.6.1.4.1.27262.1.13.1.1 (eduroam® Trust Profile [eduroamTP] defined base arc) in certificates issued to all eduroam® servers,
Policy ID: 1.3.6.1.4.1.27262.1.13.1.1.1.2 (current version of eduroam® Trust Profile [eduroamTP]) in certificates issued to eduroam® servers,
Policy ID: 1.3.6.1.4.1.25178.3.1.1 (eduroam® Service Provider as defined in [eduroamTP]) in certificates issued to eduroam® Service Provider servers,
Policy ID: 1.3.6.1.4.1.25178.3.1.2 (eduroam® Identity Provider as defined in [eduroamTP]) in certificates issued to eduroam® Identity Provider servers.

p) **Authority Information Access**
OCSP: URI: CESNET CA OCSP locator
CA Issuers: URI: locator of the DER-encoded CESNET CA certificate

q) **CRL Distribution Point**
URI: locator of the current DER-encoded CESNET CA CRL

r) **Subject Alternative Name**
- *dNSName*: DNS name(s) of the server
- *iPAddress*: IP address(es) of the server [optional]

7.1.3 Algorithm object identifiers

The CESNET CA SHOULD use the following cryptographic algorithms:

RSA Encryption – OID *1.2.840.113549.1.1.4*

SHA1 with RSA Encryption – OID *1.2.840.113549.1.1.5*

7.1.4 Name forms

Subject names of all certificates issued in compliance with this CP/CPS SHALL be constructed according to Section 3.1.1.

The subject name of the CESNET CA is

`cn=CESNET CA 3, o=CESNET CA, dc=cesnet-ca, dc=cz.`

7.1.5 Name constraints

The CESNET CA SHALL NOT support the `Name Constraints` extension.

7.1.6 Certificate policy object identifier

This CP/CPS is identified by the OID defined in Section 1.2.

The CESNET CA SHALL use OIDs of other certificate policies in end-entity certificates as specified in Section 7.1.2. These policies MUST NOT contradict this CP/CPS.

7.1.7 Usage of Policy Constraints extension

The CESNET CA SHALL NOT support the `Policy Constraints` extension.

7.1.8 Policy qualifiers syntax and semantics

The CESNET CA SHOULD NOT support the `Policy Qualifier` field of the `Certificate Policies` extension.

7.1.9 Processing semantics for the critical Certificate Policies extension

The CESNET CA SHOULD NOT mark the `Certificate Policies` extension as critical.

7.2 CRL Profile

7.2.1 Version number(s)

The CESNET CA SHALL issue CRLs version 2 as defined in RFC 5280 [RFC5280].

7.2.2 CRL and CRL entry extensions

The CESNET CA SHALL use the following CRL extensions:

a) **CRL Number**:
   sequential number of the CRL
b) **Authority Key Identifier**:
   key identifier of the CESNET CA signing key

7.3 OCSP Profile

7.3.1 Version number(s)

The OCSP service operated by the CESNET CA SHALL use Basic OCSP Response version 1 as defined in RFC 2560 [RFC2560].

7.3.2 OCSP extensions

No stipulation.

8 Compliance audit and other assessment

8.1 Frequency or circumstances of assessment

The CESNET CA SHALL perform an annual compliance audit.

8.2 Identity/qualifications of assessor

The regular audit SHALL be performed by the CESNET CA *Auditor*.

The CESNET CA SHALL enable an audit by a third party when required for its operation support and acceptance. In such case, the entire costs of the audit SHALL be covered by the entity requesting the audit.

8.3 Assessor's relationship to assessed entity

See Section 8.2.

8.4 Topics covered by assessment

The audit SHALL verify the compliance of the CA operations with this CP/CPS.

8.5 Actions taken as a result of deficiency

If any deficiency is discovered, the CESNET CA SHALL take actions needed to bring the documentation, operational procedures and configuration into compliance.

8.6 Communication of results

Results of an audit SHALL be considered private to the CESNET CA.

The CESNET CA MAY release audit results to third parties at its discretion.

9 Other business and legal matters

9.1 Fees

9.1.1 Certificate issuance or renewal fees

No stipulation.

9.1.2 Certificate access fees

No stipulation.

9.1.3 Revocation or status information access fees

No stipulation.

9.1.4 Fees for other services

No stipulation.

9.1.5 Refund policy

No stipulation.

9.2 Financial responsibility

Certificates issued under this CP/CPS SHALL NOT be used for securing financial transactions.

9.2.1 Insurance coverage

The CESNET CA operations are not covered by any insurance.

9.2.2 Other assets

No stipulation.

9.2.3 Insurance or warranty coverage for end-entities

Not supported.

9.3 Confidentiality of business information

9.3.1 Scope of confidential information

The CESNET CA SHALL keep the following information confidential:

- private keys of all participants
- other cryptographic data used for CA operations
- all personal data except for those included in certificates
- internal CA documentation except for audit reports published at the discretion of the CA

9.3.2 Information not within the scope of confidential information

Information included in certificates, CRLs and OCSP responses SHALL NOT be considered confidential.

9.3.3 Responsibility to protect confidential information

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

9.4 Privacy of personal information

9.4.1 Privacy plan

When processing personal data, the CESNET CA operates in compliance with the law of the Czech Republic.

9.4.2 Information treated as private

Any information about subscribers that is not publicly accessible or available through the content of a certificate, a CRL, or an OCSP response SHALL be treated as private information.

9.4.3 Information not deemed private

Any information about subscribers that is publicly accessible or available through the content of a certificate, a CRL, or an OCSP response SHALL NOT be deemed private.

9.4.4 Responsibility to protect private information

All *CA Operators* and *RA Officers* receiving private information SHALL protect such information from compromise and disclosure to third parties.

9.4.5 Notice and consent to use private information

By applying for a certificate a subscriber gives the CA a consent to use his/her private information for providing the PKI services.

9.4.6 Disclosure pursuant to judicial or administrative process

The CESNET CA MAY disclose any confidential or private information to law enforcement officials who exhibit regular warrant

9.4.7 Other information disclosure circumstances

No stipulation.

9.5 Intellectual property rights

CESNET, a. l. e. owns all intellectual property rights associated with this CP/CPS.

9.6 Representations and warranties

9.6.1 CA representations and warranties

The CESNET CA CA SHALL provide PKI services in compliance with this CP/CPS.

9.6.2 RA representations and warranties

A Registration Authority SHALL operate in compliance with this CP/CPS.

9.6.3 Subscriber representations and warranties

A subscriber SHALL in particular:

- provide correct and accurate information to the CA,
- immediately inform the CA about any change of information that has been submitted to the CA,
- act in accordance with this CP/CPS.
- use certificates and other services of the CA only for legal purposes,
- use certificates only for purposes for which they were issued,
- protect their private keys from compromise, loss, disclosure, or any unauthorized use,
- immediately request revocation of a certificate when it is suspected to have been misused.

9.6.4 Relying party representations and warranties

Before relying on a certificate to verify a digital signature, relying parties SHALL check that at the time of the creation of the signature the certificate was valid, has not been revoked and was issued for the given purpose.

9.6.5 Representations and warranties of other participants

No stipulation.

9.7 Disclaimers of Warranties

No stipulation.

9.8 Limitations of Liability

The CESNET CA SHALL NOT be held responsible for circumstances originated in breaching this CP/CPS by subscribers or relying parties.

9.9 Indemnities

No stipulation.

9.10 Term and Termination

9.10.1 Term

This CP/CPS shall become effective seven days after its publication and shall become effective until terminated in accordance with Section 9.10.2.

9.10.2 Termination

This CP/CPS shall remain effective until replaced with a newer version.

9.10.3 Effect of termination and survival

No stipulation.

9.11 Individual notices and communications with participants

The CESNET CA and its Registration Authorities SHALL accept communication from other parties at contact addresses published in the CA's repository (see Section 2.1).

The CESNET CA CA SHALL contact subscribers at their email addresses submitted during the registration process.

9.12 Amendments

9.12.1 Procedure for amendment

Amendments to this CP/CPS MUST be approved by the Policy Administrator (see Section 1.5.2).

9.12.2 Notification mechanism and period

Any new version of this certificate policy SHALL be published at the CA repository at least 7 days before becoming effective.

9.12.3 Circumstances under which OID must be changed

Small changes that will not change the meaning of the certificate policy MAY be applied without changing the policy OID.
Other changes require assigning a new OID for the CP/CPS.

9.13 Dispute resolution procedures

All disputes SHOULD be solved by agreement of the disputing parties. The supreme authority for solving disputes is the director of the CESNET, a. l. e..

9.14 Governing law

The CESNET CA operations SHALL be governed by the law of the Czech Republic.

9.15 Compliance with applicable law

No stipulation.

9.16 Miscellaneous provisions

9.16.1 Entire agreement

No stipulation.

9.16.2 Assignment

No stipulation.

9.16.3 Severability

If any of the provisions of this CP/CPS is found to be invalid or unenforceable, the remainder of this CP/CPS SHALL remain effective.

9.16.4 Enforcement (attorneys' fees and waiver of rights)

No stipulation.

9.16.5 Force Majeure

No stipulation.

9.17 Other provisions

No stipulation.

Bibliography

[RFC3647]: S. Chokhani, W. Ford, R. Sabett, C. Merrill, S. Wu. *Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework.*, November 2003.

[RFC2119]: S. Bradner. *Key words for use in RFCs to Indicate Requirement Levels*, March 1997.

[RFC5280]: D. Cooper, S. Santesson, S. Farrell, S. Boeyen, R. Housley, W. Polk. *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.*, May 2008.

[IGTF-Classic]: David Groep et al. *Authentication Profile for Classic X.509 Public Key Certification Authorities with secured infrastructure*, 2008, http://www.eugridpma.org/guidelines/IGTF-AP-classic-4-3.pdf

[eduroamTP]: Milan Sova et al. *eduPKI Trust Profile for eduroam® Certificates*, 2011, https://www.edupki.org/fileadmin/Documents/eduPKI-Trust-Profile-for-eduroam-certificates-1.1.pdf

[RFC2560]: M. Myers, R. Ankney, A. Malpani, S. Galperin, C. Adams. *X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP*, June 1999.

Appendix A External CAs recognized by the CESNET CA

CAs recognized for authentication of persons

The CESNET CA accepts personal certificates issued by the following external CAs to authenticate persons:

- TERENA Personal CA
  http://www.terena.org/activities/tcs/
- TERENA eScience Personal CA
  http://www.terena.org/activities/tcs/