**CERN**

**European Organization for Nuclear Research**

Category: CP/CPS

Status: draft

Document: CERN Grid Certification Authority Certificate Policy and Certificate Practice Statement

Editors: Emmanuel Ormancey, Paolo Tedesco, Alexey Tselishchev, Vincenzo De Notaris, Hannah Short

Date created: January 15, 2015 10:50

Last updated: September 22, 2021 11:00

Number of pages: 45

# CERN Grid Certification Authority Certificate Policy and Certificate Practice Statement

Emmanuel Ormancey, Paolo Tedesco, Alexey Tselishchev, Vincenzo De Notaris, Hannah Short

CERN IT/CDA

Version 5.1, Revision 0

Document OID: 1.3.6.1.4.1.96.10.4.2.2.5.0

## Table of contents

**1. Introduction ........ 8**
1.1. Overview ........ 8
1.2. Document name and identification ........ 8
1.3. PKI participants ........ 8
1.3.1. Certification authorities ........ 8
1.3.2. Registration authorities ........ 9
1.3.3. Subscribers ........ 9
1.3.4. Relying parties ........ 9
1.3.5. Other participants ........ 9
1.4. Certificate usage ........ 9
1.4.1. Appropriate certificate uses ........ 9
1.4.2. Prohibited certificate uses ........ 9
1.5. Policy administration ........ 9
1.5.1. Organization administering the document ........ 9
1.5.2. Contact persons ........ 10
1.5.3. Person determining CPS suitability for the policy ........ 10
1.5.4. CPS approval procedures ........ 10
1.6. Definitions and acronyms ........ 10

**2. Publication and repository responsibilities ........ 12**
2.1. Repositories ........ 12
2.1.1. Certification Authority tools web site ........ 12
2.1.2. Certification Authority web application (soap service) ........ 12
2.2. Publication of certification information ........ 12
2.3. Time or frequency of publication ........ 12
2.4. Access controls on repositories ........ 12

**3. Identification and authentication ........ 14**
3.1. Naming ........ 14
3.1.1. Types of names ........ 14
3.1.2. Need for names to be meaningful ........ 14
3.1.3. Anonymity or pseudonymity of subscribers ........ 14
3.1.4. Rules for interpreting various name forms ........ 14
3.1.5. Uniqueness of names ........ 15
3.1.6. Recognition, authentication, and role of trademarks ........ 15
3.2. Initial identity validation ........ 15
3.2.1. Method to prove possession of private key ........ 15
3.2.2. Authentication of organization identity ........ 15
3.2.3. Authentication of individual identity ........ 15
3.2.4. Non-verified subscriber information ........ 15
3.2.5. Validation of authority ........ 15
3.2.6. Criteria for interoperation ........ 15
3.3. Identification and authentication for re-key requests ........ 15
3.3.1. Identification and authentication for routine re-key ........ 15
3.3.2. Identification and authentication for re-key after revocation ........ 16
3.4. Identification and authentication for revocation request ........ 16

**4. Certificate life-cycle operational requirements ........ 17**
4.1. Certificate Application ........ 17

4.1.1. Who can submit a certificate application 17
4.1.2. Enrolment process and responsibilities 18
4.2. Certificate application processing 19
4.2.1. Performing identification and authentication functions 19
4.2.2. Approval or rejection of certificate applications 20
4.2.3. Time to process certificate applications 20
4.3. Certificate issuance 20
4.3.1. CA actions during certificate issuance 20
4.3.2. Notification to subscriber by the CA of issuance of certificate 20
4.4. Certificate acceptance 20
4.4.1. Conduct constituting certificate acceptance 20
4.4.2. Publication of the certificate by the CA 20
4.4.3. Notification of certificate issuance by the CA to other entities 21
4.5. Key pair and certificate usage 21
4.5.1. Subscriber private key and certificate usage 21
4.5.2. Relying party public key and certificate usage 21
4.6. Certificate renewal 21
4.6.1. Circumstance for certificate renewal 21
4.6.2. Who may request renewal 22
4.6.3. Processing certificate renewal requests 22
4.6.4. Notification of new certificate issuance to subscriber 22
4.6.5. Conduct constituting acceptance of a renewal certificate 22
4.6.6. Publication of the renewal certificate by the CA 22
4.6.7. Notification of certificate issuance by the CA to other entities 22
4.7. Certificate re-key 22
4.7.1. Circumstance for certificate re-key 22
4.7.2. Who may request certification of a new public key 22
4.7.3. Processing certificate re-keying requests 22
4.7.4. Notification of new certificate issuance to subscriber 22
4.7.5. Conduct constituting acceptance of a re-keyed certificate 22
4.7.6. Publication of the re-keyed certificate by the CA 22
4.7.7. Notification of certificate issuance by the CA to other entities 22
4.8. Certificate modification 22
4.8.1. Circumstance for certificate modification 23
4.8.2. Who may request certificate modification 23
4.8.3. Processing certificate modification requests 23
4.8.4. Notification of new certificate issuance to subscriber 23
4.8.5. Conduct constituting acceptance of modified certificate 23
4.8.6. Publication of the modified certificate by the CA 23
4.8.7. Notification of certificate issuance by the CA to other entities 23
4.9. Certificate revocation and suspension 23
4.9.1. Circumstances for revocation 23
4.9.2. Who can request revocation 23
4.9.3. Procedure for revocation request 24
4.9.4. Revocation request grace period 24
4.9.5. Time within which CA must process the revocation request 24
4.9.6. Revocation checking requirement for relying parties 24
4.9.7. CRL issuance frequency (if applicable) 24
4.9.8. Maximum latency for CRLs (if applicable) 24
4.9.9. On-line revocation/status checking availability 24

4.9.10. On-line revocation checking requirements........24
4.9.11. Other forms of revocation advertisements available........24
4.9.12. Special requirements re-key compromise........25
4.9.13. Circumstances for suspension........25
4.9.14. Who can request suspension........25
4.9.15. Procedure for suspension request........25
4.9.16. Limits on suspension period........25
4.10. Certificate status services........25
4.10.1. Operational characteristics........25
4.10.2. Service availability........25
4.10.3. Optional features........25
4.11. End of subscription........25
4.12. Key escrow and recovery........25
4.12.1. Key escrow and recovery policy and practices........25
4.12.2. Session key encapsulation and recovery policy and practices........25

**5. Facility, management and operational controls........27**
5.1. Physical controls........27
5.1.1. Site location and construction........27
5.1.2. Physical access........27
5.1.3. Power and air conditioning........27
5.1.4. Water exposures........27
5.1.5. Fire prevention and protection........27
5.1.6. Media storage........27
5.1.7. Waste disposal........27
5.1.8. Off-site backup........27
5.2. Procedural controls........27
5.2.1. Trusted roles........27
5.2.2. Number of persons required per task........27
5.2.3. Identification and authentication for each role........27
5.2.4. Roles requiring separation of duties........27
5.3. Personnel controls........27
5.3.1. Qualifications, experience, and clearance requirements........27
5.3.2. Background check procedures........28
5.3.3. Training requirements........28
5.3.4. Retraining frequency and requirements........28
5.3.5. Job rotation frequency and sequence........28
5.3.6. Sanctions for unauthorized actions........28
5.3.7. Independent contractor requirements........28
5.3.8. Documentation supplied to personnel........28
5.4. Audit logging procedures........28
5.4.1. Types of events recorded........28
5.4.2. Frequency of processing log........28
5.4.3. Retention period for audit log........28
5.4.4. Protection of audit log........28
5.4.5. Audit log backup procedures........29
5.4.6. Audit collection system (internal vs. external)........29
5.4.7. Notification to event-causing subject........29
5.4.8. Vulnerability assessments........29
5.5. Records archival........29
5.5.1. Types of records archives........29

5.5.2. Retention period for archive ........ 29
5.5.3. Protection of archive ........ 29
5.5.4. Archive backup procedures ........ 29
5.5.5. Requirements for time-stamping of records ........ 29
5.5.6. Archive collection system (internal or external) ........ 29
5.5.7. Procedures to obtain and verify archive information ........ 29
5.6. Key changeover ........ 29
5.7. Compromise and disaster recovery ........ 30
5.7.1. Incident and compromise handling procedures ........ 30
5.7.2. Computing resources, software, and/or data are corrupted ........ 30
5.7.3. Entity private key compromise procedures ........ 30
5.7.4. Business continuity capabilities after a disaster ........ 31
5.8. CA or RA termination ........ 31

**6. Technical security controls ........ 32**
6.1. Key pair generation and installation ........ 32
6.1.1. Key pair generation ........ 32
6.1.2. Private key delivery to subscriber ........ 32
6.1.3. Public key delivery to certificate issuer ........ 32
6.1.4. CA public key delivery to relying parties ........ 32
6.1.5. Key sizes ........ 32
6.1.6. Public key parameters generation and quality checking ........ 32
6.1.7. Key usage purposes (as per X.509 v3 key usage field) ........ 32
6.2. Private Key Protection and Cryptographic Module Engineering Controls ........ 33
6.2.1. Cryptographic module standards and controls ........ 33
6.2.2. Private key (n out of m) multi-person control ........ 33
6.2.3. Private key escrow ........ 33
6.2.4. Private key backup ........ 33
6.2.5. Private key archival ........ 33
6.2.6. Private key transfer into or from a cryptographic module ........ 33
6.2.7. Private key storage on cryptographic module ........ 33
6.2.8. Method of activating private key ........ 34
6.2.9. Method of deactivating private key ........ 34
6.2.10. Method of destroying private key ........ 34
6.2.11. Cryptographic Module Rating ........ 34
6.3. Other aspects of key pair management ........ 34
6.3.1. Public key archival ........ 34
6.3.2. Certificate operational periods and key pair usage periods ........ 34
6.4. Activation data ........ 34
6.4.1. Activation data generation and installation ........ 34
6.4.2. Activation data protection ........ 34
6.4.3. Other aspects of activation data ........ 34
6.5. Computer security controls ........ 34
6.5.1. Specific computer security technical requirements ........ 34
6.5.2. Computer security rating ........ 34
6.6. Life cycle technical controls ........ 34
6.6.1. System development controls ........ 34
6.6.2. Security management controls ........ 34
6.6.3. Life cycle security controls ........ 35
6.7. Network security controls ........ 35
6.8. Time-stamping ........ 36

**7. Certificate, CRL, and OCSP profiles ........................................................... 37**
7.1. Certificate profile ........................................................... 37
7.1.1. Version number(s) ........................................................... 37
7.1.2. Certificate extensions ........................................................... 37
7.1.3. Algorithm object identifiers ........................................................... 38
7.1.4. Name forms ........................................................... 38
7.1.5. Name constraints ........................................................... 38
7.1.6. Certificate policy object identifier ........................................................... 38
7.1.7. Usage of Policy Constraints extension ........................................................... 38
7.1.8. Policy qualifiers syntax and semantics ........................................................... 38
7.1.9. Processing semantics for the critical Certificate Policies extension ........................................................... 38
7.2. CRL profile ........................................................... 38
7.2.1. Version number(s) ........................................................... 38
7.2.2. CRL and CRL entry extensions ........................................................... 39

**8. Compliance audit and other assessments ........................................................... 40**
8.1. Frequency or circumstances of assessment ........................................................... 40
8.2. Identity/qualifications of assessor ........................................................... 40
8.3. Assessor's relationship to assessed entity ........................................................... 40
8.4. Topics covered by assessment ........................................................... 40
8.5. Actions taken as a result of deficiency ........................................................... 40
8.6. Communication of results ........................................................... 40

**9. Other business and legal matters ........................................................... 41**
9.1. Fees 41
9.1.1. Certificate issuance or renewal fees ........................................................... 41
9.1.2. Certificate access fees ........................................................... 41
9.1.3. Revocation or status information access fees ........................................................... 41
9.1.4. Fees for other services ........................................................... 41
9.1.5. Refund policy ........................................................... 41
9.2. Financial responsibility ........................................................... 41
9.2.1. Insurance coverage ........................................................... 41
9.2.2. Other assets ........................................................... 41
9.2.3. Insurance or warranty coverage for end-entities ........................................................... 41
9.3. Confidentiality of business information ........................................................... 41
9.3.1. Scope of confidential information ........................................................... 41
9.3.2. Information not within the scope of confidential information ........................................................... 41
9.3.3. Responsibility to protect confidential information ........................................................... 41
9.4. Privacy of personal information ........................................................... 41
9.4.1. Privacy plan ........................................................... 41
9.4.2. Information treated as private ........................................................... 41
9.4.3. Information not deemed private ........................................................... 42
9.4.4. Responsibility to protect private information ........................................................... 42
9.4.5. Notice and consent to use private information ........................................................... 42
9.4.6. Disclosure pursuant to judicial or administrative process ........................................................... 42
9.4.7. Other information disclosure circumstances ........................................................... 42
9.5. Intellectual property rights ........................................................... 42
9.6. Representations and warranties ........................................................... 42
9.6.1. CA representations and warranties ........................................................... 42
9.6.2. RA representations and warranties ........................................................... 42
9.6.3. Subscriber representations and warranties ........................................................... 42

9.6.4. Relying party representations and warranties ....42
9.6.5. Representations and warranties of other participants ....42
9.7. Disclaimers of warranties ....42
9.8. Limitations of liability ....43
9.9. Indemnities....43
9.10. Term and termination....43
9.10.1. Term....43
9.10.2. Termination ....43
9.10.3. Effect of termination and survival....43
9.11. Individual notices and communications with participants ....43
9.12. Amendments ....43
9.12.1. Procedure for amendment ....43
9.12.2. Notification mechanism and period ....43
9.12.3. Circumstances under which OID must be changed ....44
9.13. Dispute resolution provisions....44
9.14. Governing law ....44
9.15. Compliance with applicable law....44
9.16. Miscellaneous provisions ....44
9.16.1. Entire agreement....44
9.16.2. Assignment ....44
9.16.3. Severability ....44
9.16.4. Enforcement (attorneys' fees and waiver of rights)....44
9.16.5. Force Majeure ....44
9.17. Other provisions ....44

**10. Bibliography ....45**

# 1. Introduction

## 1.1. Overview

The European Organization for Nuclear Research (CERN) is an intergovernmental organization having its seat in Geneva, Switzerland[i].

This document is the combined Certificate Policy and Certification Practice Statement of the CERN certification authority capable of issuing certificates for e-Science authentication using the SHA-512 algorithm.

The certification authority will be referred to as “CERN Grid Certification Authority” in the rest of this document.

This document describes the set of procedures followed by the CERN Grid Certification Authority.

This document is structured according to RFC 3647[ii]. The latter does not form part of this document and only the information provided in this document may be relied on.

## 1.2. Document name and identification

This document is named *CERN Grid Certification Authority Certificate Policy and Certificate Practice Statement*. The following ASN.1 Object Identifier (OID) has been assigned to this document: 1.3.6.1.4.1.96.10.4.2.2.5.0

This OID is constructed as shown in the table below:

| | |
|---|---|
| IANA | 1.3.6.1.4.1 |
| CERN | .96 |
| CERN CA | .10 |
| CERN Certification Authority 2 | .4 |
| Documents | .2 |
| Grid CA CP-CPS | .2 |
| Major Version | .5 |
| Minor Version | .0 |

## 1.3. PKI participants

### 1.3.1. Certification authorities

The CERN Grid Certification Authority provides PKI services to CERN Organization users; it does not issue certificates to subordinate Certification Authorities. Its certification relies on CERN Root Certification Authority 2 (CP/CPS document 1.3.6.1.4.1.96.10.4.2.1.1.1, available on web site http://cafiles.cern.ch/cafiles).

### 1.3.2. Registration authorities

The CERN Grid Certification Authority delegates the authentication of individual identity to Registration Authorities (CERN RA). Depending on the nature of a person's association with CERN this could be any one of 3 services:

- For members of personnel, as defined in Administrative Circular 11[iii], except for Unpaid Associates and USERs, registration is carried out by the HR Department.
- For Unpaid Associates and USERs it is carried out by the CERN Users Office.
- For the staff of CERN contractors it is carried out by the Registration Service.

These services complete and validate the data in the CERN HR database after various identity checks. Each person is assigned a status, classifying his relationship with CERN.

### 1.3.3. Subscribers

The CERN Grid Certification Authority issues certificates to:

- Persons (user certificate)
- Computers and services (host certificate)
- Non-human automated clients acting on behalf of human individuals (robot certificate)

The entities eligible for certification by the CERN Grid Certification Authority are:

- CERN users: people with a valid registration in the CERN HR database.
- CERN computers: computers registered in the CERN computer central database.
- CERN robots (non-human automated clients): services and applications that run on behalf of CERN users on CERN Computers.

### 1.3.4. Relying parties

Relying parties are individuals or organizations using the certificates to verify the identity of subscribers and to secure communication with this subscriber. Relying parties may or may not be subscribers within this CA.

### 1.3.5. Other participants

No stipulation.

## 1.4. Certificate usage

### 1.4.1. Appropriate certificate uses

Certificates issued within the scope of this CP may be used by subscribers for purposes of authentication, digital signature and data encryption.

### 1.4.2. Prohibited certificate uses

Any certificate use is permissible only if the limitations in the registration process and therefore the restrictions on the liability are accepted for the intended purpose.

## 1.5. Policy administration

### 1.5.1. Organization administering the document

CERN - European Organization for Nuclear Research

Policy Management Authority (PMA)

CH-1211 Geneva

Switzerland

Tel: +41 22 767 6111

http://www.cern.ch , https://www.cern.ch/ca

### 1.5.2. Contact persons

Emmanuel Ormancey

CERN – IT/OIS

Tel: +41 22 767 1057

Emmanuel.Ormancey@cern.ch

Paolo Tedesco

CERN – IT/OIS

Tel: +41 22 767 0898

Paolo.Tedesco@cern.ch

A mailing list containing CERN CA Managers has been setup to ensure quick response:

cern-ca-managers@cern.ch

### 1.5.3. Person determining CPS suitability for the policy

CERN CA Managers (see 1.5.2) determine CPS suitability for the policy.

### 1.5.4. CPS approval procedures

The document shall be submitted to EUGridPMA for acceptance and accreditation.

## 1.6. Definitions and acronyms

The following definitions and associated abbreviations are used in this document:

| | |
|---|---|
| CERN status | Classification of a person’s relationship with CERN. Examples are STAFF, USER, UPAS (unpaid associate), ENTC (employee of a CERN contractor) |
| CERN user | A person registered in the CERN HR database with an active status. |
| CERN USER | (**Note the uppercase USER**). A CERN user registered with the status “USER” in the CERN HR database. This status corresponds to people employed by an external institute who are participating in a CERN experiment. |
| Certificate | Equivalent to Public Key Certificate. |

| | |
|---|---|
| Certification Authority (CA) | An entity trusted by one or more users to create and assign public key certificates and be responsible for them during their whole lifetime. |
| 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 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 and made freely available in a public repository. |
| 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. |
| Policy Management Authority (PMA) | An entity establishing requirements and best practices for Public Key Infrastructures. |
| Registration Authority (RA) | An entity that is responsible for identification of the end entity, but that does not sign or issue certificates (i.e. an RA is delegated certain tasks on behalf of a CA). In this document the term “CERN RA” is equivalent to RA. |

# 2. Publication and repository responsibilities

## 2.1. Repositories

### 2.1.1. Certification Authority tools web site

The tools to use the services provided by the CERN Grid Certification Authority are provided through a website at the following address: http://ca.cern.ch/ca

The website can be accessed securely (using one of the secure application-layer protocols) with a web-browser by CERN users (as defined in 1.3.3).

The site is accessible with any browser, but the services provided vary with the browser and the operating system being used. The details on browser support are published in one of the sections of the help pages on the website.

### 2.1.2. Certification Authority web application (soap service)

The application provides means of communication between a CERN computer (as defined in 1.3.3) and the CERN Grid Certification Authority, using one of the secure application-layer protocols.

The purpose of the application is to allow automation and scripting of host certificate requests.

The web application can only be used by CERN Users meeting the conditions described in section 4.2.1. The list of supported protocols is defined by CERN CA managers.

## 2.2. Publication of certification information

The files and information required to use the services provided by the CERN Grid Certification Authority are provided through a website at the following address: http://cafiles.cern.ch/cafiles

The files distributed through this site include:

Certificates of the root and intermediate certification authorities

Certificate revocation lists (CRLs) of the root and intermediate certification authorities

All past and current versions of the CP-CPS documents of the root and intermediate certification authorities

## 2.3. Time or frequency of publication

- Full CRL is published every 24 hours, and after each request of revocation of a certificate for security reasons.
- New versions of CP/CPS are published as soon as they have been approved.

## 2.4. Access controls on repositories

- CRL, CP and CPS for the CERN Grid Certification Authority are available to the public as read-only information from the web site: http://cafiles.cern.ch/cafiles.
- CRL updates are fully automated and under the control of the CERN Grid Certification Authority.
- Modification of CP and CPS is only allowed to CERN employees with proper authorization by CERN CA Managers.

# 3. Identification and authentication

## 3.1. Naming

### 3.1.1. Types of names

The subject name in certificates issued by this CA is a X.500 distinguished name. A “DN” has one of the following forms:

- For a person: full name, unique ID and login name of the subject:
  ***CN=FullName,CN=id,CN=login,OU=Users,OU=Organic Units,DC=cern,DC=ch***
- For a host or a service: the optional service name and host DNS name (FQDN).
  ***CN=[servicename/]host1.cern.ch,OU=Computers,DC=cern,DC=ch***
- For a robot certificate: “Robot:” string followed by a meaningful *description* of the robot OR by *full name* of robot’s requester, unique ID and login name of the robot. If robot’s requester full name is not present in the DN an additional component containing email address that will be used to contact the responsible team is included in the certificate:

  ***[E=teamEmail],CN=”Robot:”RobotName|RequesterName,CN=id,CN=login,OU=Users,OU=Organic Units,DC=cern,DC=ch***

### 3.1.2. Need for names to be meaningful

The Subject Name in a certificate must have a reasonable association with the authenticated name of the subscriber: it contains a unique ID of the user to ensure uniqueness.

For host certificates, the CN must be stated as the fully qualified domain name (FQDN) of the host, preceded by the optional service name.

For robot certificates, the very first CN must start with “Robot:” and should include the full name of robot’s requestor OR a reasonable description of the robot. In the latter case an additional component E must include an email address that will be used to contact the team responsible for the robot.

### 3.1.3. Anonymity or pseudonymity of subscribers

Subscribers must not be anonymous or pseudonymous. The CERN RA validates identity of subscribers.

### 3.1.4. Rules for interpreting various name forms

Many languages have special characters that are not supported by the ASCII character set used to define the subject in the certificate. To work around this problem local substitution rules can be used:

- In general national characters are represented by their ASCII equivalent. E.g. é, è, à, ç are represented by e, e, a, c.
- The German “umlaut” characters may receive special treatment: ä, ö, ü are represented by either ae, oe, ue or a, o, u.

### 3.1.5. Uniqueness of names

The Subject Name included in the CN part of a certificate must be unique for all certificates issued by the CERN Grid Certification Authority. The login name is given to user during CERN User registration process.

This login name is then reserved and cannot be reused after user account closure or deletion.

### 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 requestor of a certificate proves the possession of the private key by signing the certificate request with the private key before submitting it to the CERN Grid Certification Authority.

The CERN Grid Certification Authority verifies the possession of the private key by accepting only signed certificate requests.

### 3.2.2. Authentication of organization identity

No stipulation.

### 3.2.3. Authentication of individual identity

Certificates are issued only to CERN users with a status for which the registration process requires that they present themselves physically at the appropriate registration service.

- The user is required to present his ID card or Passport and this is checked against the data in the CERN HR database.
- On initial registration, in order to get an access card, he is required to present his passport for checking before his photograph is taken for incorporation in his access card.
- The period of validity of the access card depends on the status of the person and the termination date of his contract/registration. The maximum validity period is five years and the holder must present himself in person to get it renewed.

### 3.2.4. Non-verified subscriber information

None.

### 3.2.5. Validation of authority

No stipulation.

### 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

Expiration warnings are sent to subscribers before re-key time. Re-key must be executed directly on the CERN Grid Certification Authority secure website (http://ca.cern.ch/ca), after classic authentication with credentials or certificate authentication.

Re-key after expiration is not possible, and the user has to request a new certificate.

### 3.3.2. Identification and authentication for re-key after revocation

A revoked certificate cannot be renewed; user has to request a new certificate.

## 3.4. Identification and authentication for revocation request

Revocation requests can be executed directly on the CERN Grid Certification Authority secure website (http://ca.cern.ch/ca), after classic authentication with credentials or certificate authentication.

# 4. Certificate life-cycle operational requirements

## 4.1. Certificate Application

### 4.1.1. Who can submit a certificate application

Certificate requests can be submitted by users or machines.

To request a **certificate of any kind** a user must:

- Be registered in CERN's central HR database, with one of the categories for which physical presence at the appropriate registration service is required (see section 3.2.3)
    - Members of Personnel as defined in Administrative Circular 11 (status: STAF, FELL, PDAS, PJAS,USAS, CASS, UPAS, USER, DOCT, TECH, ADMI, SUMM, CHIL, APPR, COAS, GPRO, VISC, TRNE)
    - Employee of a CERN contractor (status: ENTC)
    - Participant to an experiment (status: PART)
    - Honorary members (status: EXTN with reason HONO)
- Have a CERN computer account and register an email address.

Additional constraints apply to specific certificate types.

To request a **host certificate** a user must:

- Be registered in CERN's central network database (LANBD) as administrator or responsible of the computer, or be member of the group declared as responsible of the computer in LANDB

To request a **robot certificate** a user must:

- Be the owner of a special CERN Service Account
    - The Service Account must forward messages to the owner, or to a responsible group
    - The list of service accounts that are eligible to get a robot certificate is defined by CERN CA staff and is stored in an LDAP-based store
- Authenticate, using the CERN Service Account, to the CERN Grid Certification Authority secure website (http://ca.cern.ch/ca) and submit a request, following confirmation that:
    - The robot certificate will be used in a completely automated environment.
    - The robot certificate will be used without human interventions. Robot certificates should be used only inside scripts and applications that are scheduled and running on a regular basis.
- The website will validate all the requirements for the request.
- If the request is successfully validated, the requestor will be able to submit a certificate request as defined in 3.2.1.

A certificate request can be submitted automatically by a host, if the machine is configured to perform certificate autoenrollment. Host certificates autoenrollment can be enabled for a particular machine in the following ways:

- By a user registered as responsible or main user of the device in the CERN Network Database, or member of a group that is declared as responsible or main user for the device, using the CERN Grid Certification Authority secure website (http://ca.cern.ch/ca)
- By a user with root access to the machine, invoking a secure web application

Each time the autoenrollment settings for a machine are changed, the details of the operation are audited in an internal database. Details audited include unique identifiers for the machine and the requestor, time of the operation and type of operation performed.

### 4.1.2. Enrolment process and responsibilities

Depending on the certificate type, certificate requests can be submitted in one or more of the following ways:

- Through an online procedure on the CERN Grid Certification Authority secure website (http://ca.cern.ch/ca), using a web browser.
- To a secure API on the CERN Grid Certification Authority web application (http://ca.cern.ch/ca-services), using an automated interface.

The user authenticates with the credentials given by the CERN computer registration, or using the user or robot certificate.

For **user certificates**, requests can be submitted via an online procedure on the CERN Grid Certification Authority secure website (http://ca.cern.ch/ca), using a web browser.

The key pairs are generated by the web browser locally on the user's machine.
The certificate (public key signed by the CA) can only be downloaded using the same browser, including the key pair, on the same machine, through a secure URL on the CERN Grid Certification Authority website.
Depending on the used browser, key pairs and CSRs are generated using the *keygen*[iv] html tag when properly supported, ActiveX controls for Internet Explorer and JavaScript (using the Forge[v] library) when other methods are not available.

For **host or service certificates**, requests can be submitted by the machine or service administrator in the following ways:

- Creating a key pair and certificate request file in PKCS#10[vi] format using the *OpenSSL*[vii] package or the CertReq[viii] tool (available for Windows machines only), then submitting the certificate request file to the CERN Grid Certification Authority secure website (http://ca.cern.ch/ca).
  The private key is kept by the host or service administrator.
- Generating a key pair and a certificate request automatically, through JavaScript code running on the browser.
  The private key is kept in the client process and never transmitted to the Certification Authority.
  The certificate is downloaded by the browser after a successful request. The process

then bundles the certificate with the private key and makes it available to the user as a download link.

- Creating a key pair and certificate request file in PKCS#10[ix] format using the *OpenSSL*[x] package or the CertReq[xi] tool (available for Windows machines only), then submitting the certificate request file to the CERN Grid Certification Authority through a secure web application (http://ca.cern.ch/ca-services).
  The private key is kept by the host or service administrator.
  The certificate is returned by the web application after a successful request.

If **certificates autoenrollment** is enabled on a machine, the host certificate is requested by a process running periodically on the machine (like a Windows service or a Cron job).
The process verifies if the machine is configured for host certificates autoenrollment and either of these conditions is met:
- No host certificate is present on the machine
- Host certificates present on the machine are either expired or have an expiration date in a certain amount of time
If the conditions above are met, the process automatically creates a key pair and certificate request file, signs the request and submits it to the CERN Grid Certification Authority in one of these two ways:
- directly to the Certification Authority, using the built-in Windows autoenrollment service
- through a secure web service
The service submitting the request authenticates using the Kerberos credentials of the machine. These Kerberos credentials are associated with a specific network address and a single host name through the Network Database, with a registered user and/or responsible group.

The subject of the issued certificate will be the fully qualified domain name of the machine performing the request.

The Subject Alternative Names extensions of the issued certificate will contain:

- The DNS name of the machine
- A set of DNS names configured for the machine by a responsible user (as defined in the Network Database) through the CERN Grid Certification Authority secure website.

Subject and subject alternative names will only be in the .cern.ch domain.

For **robot certificates**, requests can be submitted in one way:

- The requestor of a robot certificate generates key pair and certificate request file in PKCS#10 format using OpenSSL package, submits certificate request file to the CERN Grid Certification Authority secure website (http://ca.cern.ch/ca) using special service account credentials (See clause 4.1.1). The certificate can be downloaded using a browser by a secure URL on the CERN Grid Certification Authority website.

## 4.2. Certificate application processing

### 4.2.1. Performing identification and authentication functions

Users must have a CERN computer account with valid credentials in order to authenticate to the CERN Grid Certification Authority secure website (http://ca.cern.ch/ca) and request a certificate.

Users authentication is performed using the CERN Single Sign On infrastructure, using any available authentication method (username and password, certificate authentication and so on). A new authentication is forced when accessing the CERN Grid Certification Authority website, to avoid re-use of a Single Sign On token previously obtained authenticating to another CERN website.

Once the user is authenticated, additional constraints are checked to authorize the request, depending on the type of certificate being requested, as defined in section 4.1.1.

### 4.2.2. Approval or rejection of certificate applications

Certificate requests are automatically approved or rejected by the CERN Grid Certification Authority infrastructure by verifying that all the issuance conditions are met, in particular:

- The requester must meet the requirements expressed in 4.1.1
- The key used to sign the request must meet the requirements expressed in 6.1.5

Since host certificates are only issued for machines registered in the CERN Network Database, additional restrictions enforced by the Network Database on the validity of host names implicitly apply to host certificates issued by the CERN Grid Certification Authority. In particular:

- Valid subjects and subject alternative names are restricted to the cern.ch domain
- Names are checked against a blacklist maintained by the CERN Network Database administrators that prevents potentially dangerous host names from being approved

Additionally, a host certificate request must contain a Subject Alternative Name extension with the DNS name of the machine that is the subject of the certificate.

### 4.2.3. Time to process certificate applications

Certificate issuing and processing is done instantly: identity verification has been made previously by the CERN RA, and is mandatory to proceed with the request for a certificate.

## 4.3. Certificate issuance

### 4.3.1. CA actions during certificate issuance

No stipulation.

### 4.3.2. Notification to subscriber by the CA of issuance of certificate

Certificate request is done using CERN Grid Certification Authority secure website, in a wizard form or using CERN Grid Certification Authority web application providing an interface to a secure API for scripted certificate application processing. The last step of the wizard provides a link to download the issued certificate. Web application delivers the certificate in a text output securely sent to the requester.

## 4.4. Certificate acceptance

### 4.4.1. Conduct constituting certificate acceptance

No stipulation.

### 4.4.2. Publication of the certificate by the CA

User Certificates are published to CERN internal Microsoft Active Directory service, to allow authentication on various CERN websites and applications.

User Certificates are also published in CERN internal Exchange Mail Server address book: Certificate can be used to encrypt mails.

### 4.4.3. Notification of certificate issuance by the CA to other entities

No stipulation.

## 4.5. Key pair and certificate usage

### 4.5.1. Subscriber private key and certificate usage

By accepting the certificate the subscriber assures all participants of the CERN Grid Certification Authority and all parties relying on the trustworthiness of the information contained in the certificate that:

- A basic understanding exists of the use and purpose of certificates.
- All data and statements given by the subscriber with relation to the information contained in the certificate are truthful and accurate.
- The private key will be maintained in a safe and secure manner.
- No unauthorized person has or will ever have access to the private key. In particular, the private key of a user certificate must not be shared with anyone else than the certificate owner
- The certificate will solely and exclusively be put to such uses as are in accordance with this Certificate Policy,
- Immediate action will be undertaken on the subscriber’s part to revoke the certificate if information in the certificate no longer proves to be correct or if the private key is missing, stolen, or is in any other way compromised.

### 4.5.2. Relying party public key and certificate usage

Every person using a certificate issued within the framework of this CP for verification signature or for purposes of authentication or encryption

- must verify the validity of the certificate before using it,
- must use the certificate solely and exclusively for authorized and legal purposes accordance with this CP, and
- should have a basic understanding of the use and purpose of certificates.

## 4.6. Certificate renewal

Renewal of certification involves the issuance of a new certificate to the subscriber by the CERN Grid Certification Authority with a new key pair. CERN Grid Certification Authority doesn’t permit renewal without re-key.

### 4.6.1. Circumstance for certificate renewal

Application for certificate renewal can only be made if the certificate has not reached the end of its validity period, and has not been revoked.

### 4.6.2. Who may request renewal

Renewal of a certificate must always be requested by the subscriber.

### 4.6.3. Processing certificate renewal requests

The processing of certificate renewal requests is conducted in accordance with the provisions of section 4.3. The provisions of section 3.3.1 govern the procedures for identification and authentication for certificate renewal.

### 4.6.4. Notification of new certificate issuance to subscriber

The provisions of section 4.3.2 apply.

### 4.6.5. Conduct constituting acceptance of a renewal certificate

The provisions of section 4.4.1 apply.

### 4.6.6. Publication of the renewal certificate by the CA

The provisions of section 4.4.2 apply.

### 4.6.7. Notification of certificate issuance by the CA to other entities

The provisions of section 4.4.3 apply.

## 4.7. Certificate re-key

Basically, the provisions of section 4.6 apply here. However, in the case of a re-key a new key pair will be used.

CERN Grid Certification Authority enforces re-key at least once a year.

### 4.7.1. Circumstance for certificate re-key

The provisions of section 4.6.1 apply.

### 4.7.2. Who may request certification of a new public key

The provisions of section 4.6.2 apply.

### 4.7.3. Processing certificate re-keying requests

The provisions of section 4.6.13 apply.

### 4.7.4. Notification of new certificate issuance to subscriber

The provisions of section 4.6.4 apply.

### 4.7.5. Conduct constituting acceptance of a re-keyed certificate

The provisions of section 4.6.5 apply.

### 4.7.6. Publication of the re-keyed certificate by the CA

The provisions of section 4.6.6 apply.

### 4.7.7. Notification of certificate issuance by the CA to other entities

The provisions of section 4.6.7 apply.

## 4.8. Certificate modification

Certificates must not be modified. In case of changes, the old certificate must be revoked, and a new certificate must be requested.

### 4.8.1. Circumstance for certificate modification

No stipulation.

### 4.8.2. Who may request certificate modification

No stipulation.

### 4.8.3. Processing certificate modification requests

No stipulation.

### 4.8.4. Notification of new certificate issuance to subscriber

No stipulation.

### 4.8.5. Conduct constituting acceptance of modified certificate

No stipulation.

### 4.8.6. Publication of the modified certificate by the CA

No stipulation.

### 4.8.7. Notification of certificate issuance by the CA to other entities

No stipulation.

## 4.9. Certificate revocation and suspension

This section explains the circumstances under which a certificate should be revoked. No provision is made for the suspension (temporary invalidity) of certificates. Once a certificate has been revoked, it may not be renewed or extended.

### 4.9.1. Circumstances for revocation

Certificates must be revoked by the CERN Grid Certification Authority should at least one of the following circumstances be known:

- A certificate contains data that is no longer valid.
- The private key of a subscriber has been changed, lost, stolen, published or compromised and/or misused in any other manner.
- The subscriber has lost the grounds for entitlement.
- The subscriber does not comply with the terms and conditions of the CP.
- The CERN Grid Certification Authority or RA does not comply with the terms and conditions of the CP or the CPS.
- The certification service is discontinued.
- The CERN Grid Certification Authority private key is compromised.

Certificates may be revoked by the CERN Grid Certification Authority should at least one of the following circumstances be known:

- The subscriber no longer needs a certificate.

### 4.9.2. Who can request revocation

Any subscriber may request the CERN Grid Certification Authority to revoke his certificate. The subscriber must choose a revocation reason among the following:

- Certificate superseded: the certificate is no longer needed.
- Security reasons: the certificate is known or suspected to be compromised. If this option is chosen, the requester will also need to provide a brief description of the security incident, which will be submitted to the CERN Computer Security Team to evaluate the security risk for the CERN computing infrastructure.

Acceptance of a revocation request of a certificate is conditional on the successful identification and authentication of the subscriber in accordance with section 3.4.

The CERN RA is also allowed to ask a certificate revocation from CERN CA Staff, in case of compromise of a key.

The CERN CA staff can revoke any certificate for security reasons.

### 4.9.3. Procedure for revocation request

If the conditions to acceptance of the request (see section 4.9.2) are met, the certificate will be revoked.

### 4.9.4. Revocation request grace period

Should circumstances for revocation of a certificate exist (see section 4.9.1), the subscriber is obliged to notify the CERN Grid Certification Authority immediately of the same, and to initiate revocation of the certificate.

### 4.9.5. Time within which CA must process the revocation request

The CERN Grid Certification Authority will process a request for revocation of a certificate instantly if the conditions to acceptance of the request (see section 4.9.2) are met.

### 4.9.6. Revocation checking requirement for relying parties

The provisions of section 4.5.2 apply.

### 4.9.7. CRL issuance frequency (if applicable)

The provisions of section 0 apply.

### 4.9.8. Maximum latency for CRLs (if applicable)

The provisions of section 0 apply.

### 4.9.9. On-line revocation/status checking availability

CERN Grid Certification Authority provides an on-line procedure where the validity of the user’s certificate can be verified, by simply login in the CERN Grid Certification Authority Web Site located at http://ca.cern.ch/ca and clicking “*Certificate Authentication [details]*” link. This procedure shows the current user certificate status.

Revocation can be requested online on CERN Grid Certification Authority Web site at http://ca.cern.ch/ca by the user himself.

CRLs are available from the URL given in the associated CPS section 2.1.

### 4.9.10. On-line revocation checking requirements

Prior to every usage of the certificate, its validity should be checked. The relevant standards are given in section 7.2 (CRL Profile) and section 7.3 (OCSP Profile) of the CPS.

### 4.9.11. Other forms of revocation advertisements available

Currently no other forms of revocation advertisements are available.

### 4.9.12. Special requirements re-key compromise

Should a private key become compromised, the certificate so affected shall immediately be revoked. Should the private key of the CERN Grid Certification Authority become compromised, all certificates issued by the CERN Grid Certification Authority shall be revoked.

### 4.9.13. Circumstances for suspension

Suspension of certificates is not supported.

### 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

An Online Certificate Status Protocol service is available at http://ocsp.cern.ch/ocsp.

### 4.10.1. Operational characteristics

The service is provided through the Microsoft Online Responder and Web Proxy Cache services, standard components of Microsoft's PKI infrastructure in Windows Server 2008.

### 4.10.2. Service availability

The service is currently installed on a single server, and should be permanently available except during server maintenance operations.

High availability will be provided, if needed, configuring the service in a clustered configuration with additional servers.

### 4.10.3. Optional features

No optional features are available.

## 4.11.End of subscription

The term of the contractual relationship is given by the period of validity as indicated in the certificate.

The minimum period for the archiving of documents and certificates corresponds to the period of validity of the certificate of the CERN Grid Certification Authority with the addition of a further period of one year.

## 4.12.Key escrow and recovery

The CERN Grid Certification Authority does not support key escrow and recovery.

### 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

The CERN Grid Certification Authority is hosted in CERN Computer Center.

### 5.1.2. Physical access

Physical access to CERN Grid Certification Authority is restricted to authorized personnel of the CERN CA.

### 5.1.3. Power and air conditioning

The critical CERN Grid Certification Authority equipment is connected to uninterrupted power supply units, and CERN Computer Center is running uninterrupted air conditioners.

### 5.1.4. Water exposures

No floods are expected in CERN Computer Center.

### 5.1.5. Fire prevention and protection

CERN Computer Center is equipped with various smoke and fire detectors.

### 5.1.6. Media storage

The CERN Grid Certification Authority key is kept in several removable storage media (Smart Cards, see 6.2.4). Backup copies of CA related information are kept on CD-Roms or DVD-Roms. Removable media are stored in a secure location.

### 5.1.7. Waste disposal

All CERN Grid Certification Authority paper waste MUST be shredded. Electronic media MUST be physically/mechanically destroyed before disposal.

### 5.1.8. Off-site backup

No off-site backups are currently performed.

## 5.2. Procedural controls

### 5.2.1. Trusted roles

No stipulation.

### 5.2.2. Number of persons required per task

One CERN CA staff only is required.

### 5.2.3. Identification and authentication for each role

No stipulation.

### 5.2.4. Roles requiring separation of duties

No stipulation.

## 5.3. Personnel controls

### 5.3.1. Qualifications, experience, and clearance requirements

The role of the CA requires a suitably trained person that is familiar with the importance of a PKI, and who is technically and professionally competent. There are no background checks or clearance procedures for trusted or other roles.

### 5.3.2. Background check procedures

No stipulation.

### 5.3.3. Training requirements

Internal training is given to CERN CA and RA operators.

### 5.3.4. Retraining frequency and requirements

No stipulation.

### 5.3.5. Job rotation frequency and sequence

No stipulation.

### 5.3.6. Sanctions for unauthorized actions

No stipulation.

### 5.3.7. Independent contractor requirements

No stipulation.

### 5.3.8. Documentation supplied to personnel

Personnel assigned to the CA operation have access to a restricted part of the CERN Grid Certification Authority website were all operational procedures can be found, as well as this document.

## 5.4. Audit logging procedures

### 5.4.1. Types of events recorded

The following events are recorded in the CA log:

- Backup and restore the CA database
- Change CA configuration
- Change CA security settings
- Issue and manage certificate requests
- Revoke certificates and publish CRLs
- Store and retrieve archives keys

The following events are recorded in the server log:

- Login/Logout
- Reboot

### 5.4.2. Frequency of processing log

Log is 300MB size, and is automatically archived to a file when 100% full.

### 5.4.3. Retention period for audit log

Logs are kept on CD-Rom/DVD-Rom for at least 3 years.

### 5.4.4. Protection of audit log

Audit logs are only accessible to the administrators of CERN CA and to authorized audit personnel.

### 5.4.5. Audit log backup procedures

Every archive log file is burned on a CD-Rom or a DVD-Rom.

### 5.4.6. Audit collection system (internal vs. external)

Audit collection is internal to CERN CA service.

### 5.4.7. Notification to event-causing subject

No stipulation.

### 5.4.8. Vulnerability assessments

CERN CA is constantly (24x7) monitored and all attempts to gain unauthorized access to any of the services are logged and analyzed.

## 5.5. Records archival

### 5.5.1. Types of records archives

The CERN Grid Certification Authority keeps record of:

- All certificate requests
- All issued certificates
- All revoked certificates
- Certificate Revocation Lists
- Login and reboot information of the servers operating the infrastructure

### 5.5.2. Retention period for archive

The minimum retention period is 3 years.

### 5.5.3. Protection of archive

The records archived is accessible to CERN CA personnel only.

### 5.5.4. Archive backup procedures

Records are archives on removal media (CD-Rom, DVD-Rom) and are stored in a restricted access area.

### 5.5.5. Requirements for time-stamping of records

All records are saved with an automatically generated time stamp.

### 5.5.6. Archive collection system (internal or external)

Archiving system is CERN internal.

### 5.5.7. Procedures to obtain and verify archive information

No stipulation.

## 5.6. Key changeover

The rekeying of the CERN Grid Certification Authority certificate shall be performed 14 months in advance of the certificate expiration date, as the maximum validity of issued end-entity certificates is of 400 days.

This will ensure that end-entity certificates will always be issued with their normal validity period, as the CERN Grid Certification Authority automatically reduces the validity of issued certificates to avoid that their validity extends beyond the expiration date of the signing certificate.

After the rekey, all newly issued end-entity certificates will be signed by the new certificate.

The old CA certificate will be available for its normal validity period, and will be used only to sign the CRL containing the revocation information for the certificates signed with the old CA certificate.

In parallel, a new CRL will be distributed, signed with the new CA certificate. The new CRL will contain revocation information for the certificates signed with the new CA certificate.

## 5.7. Compromise and disaster recovery

### 5.7.1. Incident and compromise handling procedures

- If the keys of an end entity are lost or compromised, the CERN RA must be informed immediately in order to revoke the certificate. The owner of the certificate can do this by himself using the CERN Grid Certification Authority website (http://ca.cern.ch/ca).

- If CERN Grid Certification Authority's private key is (or suspected to be) compromised, the CA will:

    - Inform the Registration Authorities, subscribers and relying parties of which the CA is aware.

    - Terminate the certificates and CRL distribution services for certificates and CRLs issued using the compromised key.

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

The CERN CA operators will ensure that recovery procedures are functional and up to date.

All CERN Grid Certification Authority software and system will be backed up (encrypted backup) on a daily basis. In case of corruption or hardware failure, a new functioning hardware will be installed and the latest working and not-corrupted state of the CERN Grid Certification Authority software and data will be restored.

If needed, the CERN Grid Certification Authority issuing Private Key stored in the Hardware Security Module will be restored according HSM's restore procedures (see 6.2.4), therefore operations should restart without any certificate revocation.

### 5.7.3. Entity private key compromise procedures

In case the private key of the CERN Grid Certification Authority is compromised, the CERN CA will:

- notify CERN RA
- make a reasonable effort to notify subscribers
- terminate issuing and distribution of certificates and CRLs
- request revocation of the compromised certificate
- generate a new CERN Grid Certification Authority key pair and certificate and publish the certificate in the repository
- revoke all certificates signed using the compromised key
- publish the new CRL on the CERN Grid Certification Authority repository.

### 5.7.4. Business continuity capabilities after a disaster

The plans for business continuity and disaster recovery for research activities and education are applicable.

## 5.8. CA or RA termination

Before CERN Grid Certification Authority terminates its services, it will:

- Inform the Registration Authorities, subscribers and relying parties the CA is aware;
- Make information of its termination widely available;
- Stop issuing certificates
- Revoke all certificates
- Generate and publish CRL
- Destroy its private keys and all copies

An advance notice of at least 60 days will be given in the case of scheduled termination. The CERN CA Manager at the time of termination will be responsible for the subsequent archival of all records as required in section 5.5.2.

The CERN Grid Certification Authority issues ONLY CRLs during its last 400 days (i.e. the maximal lifetime of a subscriber certificate) before the termination; this will allow subscribers' certificates to be used until they expire. In that case notice of termination is given no less than 460 days prior to the actual termination, i.e. no less than 60 days before the CA ceases to issue new certificates.

# 6. Technical security controls

## 6.1. Key pair generation and installation

### 6.1.1. Key pair generation

- The key pair for the CERN Root Certification Authority 2 is generated by authorized CA staff on the offline CERN Root CA machine (see CERN Root Certification Authority 2 CP/CPS document).
- The keys for CERN Grid Certification Authority are generated by software, in the CA Service, or by Hardware in the Hardware Security Module.
- Each subscriber generates the key pair using a Web Browser or *OpenSSL* package (see 4.1.2).

### 6.1.2. Private key delivery to subscriber

Each subscriber generates the key pair using a Web Browser or OpenSSL package (see 4.1.2). The CA does not generate private keys for its subscribers and therefore does not deliver private keys to subscribers.

### 6.1.3. Public key delivery to certificate issuer

Subscribers' public keys are delivered through the CERN Grid Certification Authority secure website http://ca.cern.ch/ca or through the automated interface of the CERN Grid Certification Authority secure web application (see chapter 2).

### 6.1.4. CA public key delivery to relying parties

The CERN Grid Certification Authority public key is delivered to subscribers through the secure website http://ca.cern.ch/ca (see chapter 2).

### 6.1.5. Key sizes

Keys of length less than 2048 bits are not accepted. The CERN Grid Certification Authority key is 4096 bits long.

### 6.1.6. Public key parameters generation and quality checking

No stipulation.

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

The keys may be used according to the type of certificate:

- With an end-entity certificate for
  - authentication
  - non-repudiation
  - data and key encipherment
  - message integrity
  - session establishment
  - proxy creation and signing
- With an RA certificate (certificate issued to Registration Authority) for
  - some activities needed for the work of an RA agent

- With the CA certificate
    - certificate signing
    - CRL signing

The CA’s private key is the only key that can be used for signing certificates and CRLs.

## 6.2. Private Key Protection and Cryptographic Module Engineering Controls

### 6.2.1. Cryptographic module standards and controls

CERN Grid Certification Authority private key is protected by a HSM Safenet ProtectServer External 4.2, FIPS140-2 Level 3 certified.

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

No stipulation.

### 6.2.3. Private key escrow

Private keys must not be escrowed.

### 6.2.4. Private key backup

The private key is backed up from the HSM module using the ‘multiple custodians method’: the key is split into multiple shares and then distributed to multiple custodians. The shares are encrypted (wrapped) by a second key called the wrapping key which is selected at random.

The scheme to split the key into multiple shares is done in such a way that the original key will only be recovered with the co-operation of all the custodians.

Each custodian is a smart card secured by a password PIN. Smart Card reader is connected to the parallel port on the back of the HSM. All PIN and Key exchange sessions between the smart card and the HSM are encrypted.

Each smart card has its own PIN number and user name and belongs to one CERN CA Staff who is responsible for it.

The restore procedure is the same as backup. All custodians (smart cards) are read one by one by the HSM.

### 6.2.5. Private key archival

Private key archival is not supported.

### 6.2.6. Private key transfer into or from a cryptographic module

Keys are never exposed from the HSM in clear form. All key transfers are encrypted, and occur only during backup and restore procedures (see 6.2.4).

### 6.2.7. Private key storage on cryptographic module

Keys are stored in a battery-backed secure key storage. A battery provides back-up power to the tamper-sensing electronics when no system power is available. Any detected tamper event, including battery removal or disconnection of the secure key storage from HSM, will immediately activate key memory erasure.

### 6.2.8. Method of activating private key

No stipulation.

### 6.2.9. Method of deactivating private key

No stipulation.

### 6.2.10. Method of destroying private key

Keys could be destroyed by erasure of appropriate key container or using user initiated tamper which causes all data on the HSM to be erased.

### 6.2.11. Cryptographic Module Rating

HSM is FIPS140-2 Level 3 certified.

## 6.3. Other aspects of key pair management

### 6.3.1. Public key archival

Public key archival is not supported.

### 6.3.2. Certificate operational periods and key pair usage periods

The CERN Grid Certification Authority Certificate has a validity period of 10 years.

The issued user certificates have a validity period of 400 days.

## 6.4. Activation data

### 6.4.1. Activation data generation and installation

The private key is generated by the HSM module, following HSM instructions and using the HSM Administrator toolkit. A strong password is also required to generate the key pair.

### 6.4.2. Activation data protection

Only CERN CA Staff are allowed and can activate the CA private key.

### 6.4.3. Other aspects of activation data

No stipulation.

## 6.5. Computer security controls

### 6.5.1. Specific computer security technical requirements

The server hosting CERN Grid Certification Authority is running Microsoft Windows 2008 Enterprise Edition and Microsoft Certificate Services. No other services or software are loaded or operated on this server. The server will receive occasional patches and other adjustments by the CERN CA Managers or authorized CERN Staff.

### 6.5.2. Computer security rating

No stipulation.

## 6.6. Life cycle technical controls

### 6.6.1. System development controls

No stipulation.

### 6.6.2. Security management controls

No stipulation.

### 6.6.3. Life cycle security controls

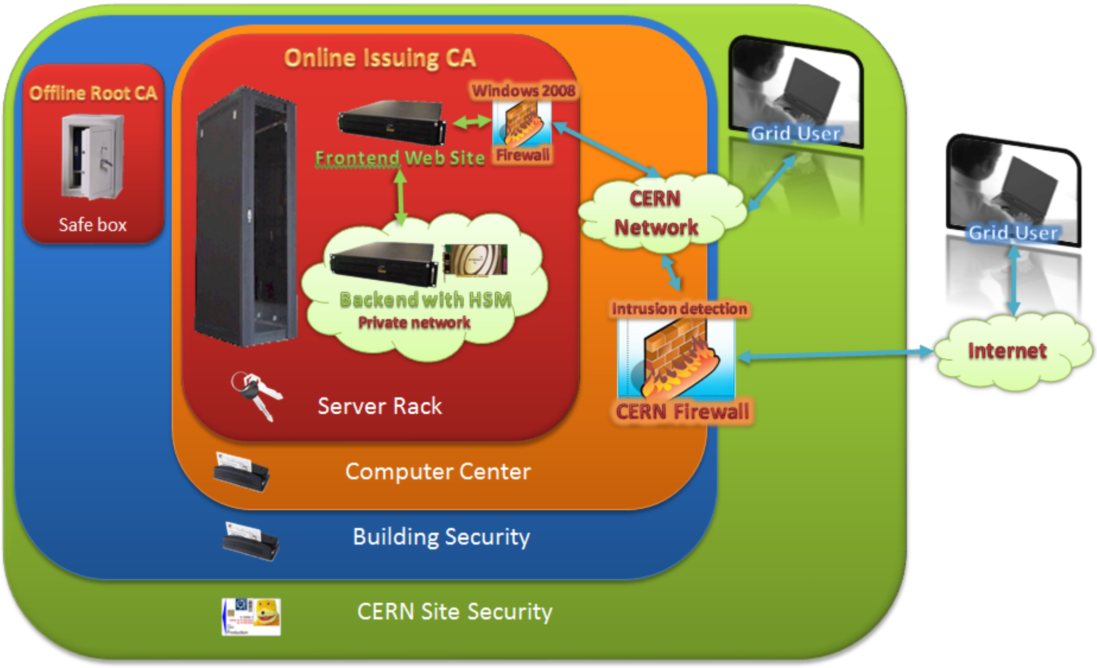
No stipulation.

## 6.7. Network security controls

The CERN Root Certification Authority 2 is offline, and must not be connected to any computer network under any circumstances (see CERN Root CA CP/CPS document).

The CERN issuing CA Frontend contains the CA website and CA secure web application.It is connected to CERN network, and is protected by CERN Firewall, configured and maintained according to the recommendations of the CERN Security team, for protection from off-site sources. It is also protected by its own software Firewall (Microsoft Windows 2008 firewall) for protection against CERN network sources.

The CERN Issuing CA backend contains the CA service, and is connected with a private network to a Hardware Security Module (see 6.2). It is directly connected to the Frontend, and has no direct connection to CERN network. Hardware Security Module has a local network address, is connected to CERN Issuing CA backend only and can't be accessed from CERN or external network. Operations available for CERN Issuing CA backend are only limited to signing operations. Administrative operations on Hardware Security Module can only be performed by CERN CA managers directly during physical interaction (i.e. connection of a display and a keyboard) with the Hardware Security Module.


Online Issuing CA
Offline Root CA
Safe box
Windows 2008
Frontend Web Site
Firewall
CERN Network
Grid User
Grid User
Backend with HSM
Private network
Intrusion detection
Internet
CERN Firewall
Server Rack
Computer Center
Building Security
CERN Site Security

## 6.8. Time-stamping

All time stamping of entries created on the online servers at the CERN CA is based on the network time provided by the time servers of CERN, which are synchronized with *Navstar Global Positioning System* (GPS).

# 7. Certificate, CRL, and OCSP profiles

## 7.1. Certificate profile

All certificates issued by CERN CA conform to the Internet PKI profile (PKIX) for X.509 certificates as defined by RFC 3280.

### 7.1.1. Version number(s)

Only X.509 version 3 certificates are issued by CERN Grid Certification Authority.

### 7.1.2. Certificate extensions

The extensions to the X.509 v3 certificate that shall be present in CERN Grid Certification Authority certificates are:

For natural person and robot certificates:

- Subject Key Identifier: hash
- Authority Key Identifier: keyid
- Key Usage (critical): Digital Signature, Key Encipherment
- Enhanced Key Usage: Encrypting File System (1.3.6.1.4.1.311.10.3.4), Secure Email (1.3.6.1.5.5.7.3.4), Client Authentication (1.3.6.1.5.5.7.3.2)
- CRL Distribution Points: ldap URI and http URI.
- Certificate Policies: OID of this CP (see 7.1.6) and OID of the Authentication Profile for Classic X.509 Public Key Certification Authorities with secured infrastructure[xii]
- Subject Alternative Name: RFC822 Name (email address), Principal Name (CERN login, i.e. login@cern.ch)

For host certificates:

- Subject Key Identifier: hash
- Authority Key Identifier: keyid
- Key Usage (critical): Digital Signature, Key Encipherment
- Extended Key Usage: Server Authentication (1.3.6.1.5.5.7.3.1)
- CRL Distribution Points: ldap URI and http URI.
- Certificate Policies: OID of this CP (see 7.1.6) and OID of the Authentication Profile for Classic X.509 Public Key Certification Authorities with secured infrastructure[xiii]
- Subject Alternative Name: DNSName(s).

For CA certificates:

- Basic Constraints: critical ca: true;
- Subject Key Identifier: hash
- Authority Key Identifier: keyid

- Key Usage: critical, digitalSignature, nonRepudiation, KeyCertSign, cRLSign
- Extended Key Usage timeStamping
- CRL Distribution Points: ldap URI and http URI.
- Certificate Policies: OID

### 7.1.3. Algorithm object identifiers

The OIDs for algorithms used for signatures of certificates issued by CERN Grid Certification Authority are according to:

- hash function: sha512 2.16.840.1.101.3.4.2.3
- encryption: rsaEncryption 1.2.840.113549.1.1.1
- signature: sha512RSA 1.2.840.113549.1.1.13

### 7.1.4. Name forms

Each entity issued by CERN Grid Certification Authority has a unique and unambiguous Distinguished Name (DN). CERN CA prefers that organizations use domain component naming.

- Issuer subject:
    - CN=CERN Grid Certification Authority,DC=cern,DC=ch
- End Entity Subject:
    - CN=FullName,CN=id,CN=login,OU=Users,OU=Organic Units,DC=cern,DC=ch
    - CN=FQDN,OU=Computers,DC=cern,DC=ch

### 7.1.5. Name constraints

There are no other name constraints than those that are to be derived from the stipulations in 7.1.4, 3.1.1 and 3.1.2.

### 7.1.6. Certificate policy object identifier

The OID of this CP is: 1.3.6.1.4.1.96.10.4.2.2

### 7.1.7. Usage of Policy Constraints extension

No stipulation.

### 7.1.8. Policy qualifiers syntax and semantics

No stipulation.

### 7.1.9. Processing semantics for the critical Certificate Policies extension

No stipulation.

## 7.2. CRL profile

### 7.2.1. Version number(s)

CERN Grid Certification Authority creates and publishes X.509 v2 CRLs signed with SHA-512 algorithm.

### 7.2.2. CRL and CRL entry extensions

CERN Grid Certification Authority issues complete CRLs for all certificates issued by itself. The CRL includes the date by which the next CRL shall be issued. A new CRL must be issued before this date if new revocations are issued.

The CRL extensions that shall be included are:

- The Authority Key Identifier
- The CRL Number

The CRL entry extensions that will be included are:

- CRL Reason Code
- Invalidity Date

# 8. Compliance audit and other assessments

## 8.1. Frequency or circumstances of assessment

CERN Grid Certification Authority shall make at least once a year a self-assessment to check the compliance of the operation with the CP/CPS document in effect.

The CA shall at least once a year assess the compliance of the procedures of each RA with the CP/CPS document in effect.

## 8.2. Identity/qualifications of assessor

No stipulation.

## 8.3. Assessor's relationship to assessed entity

The assessments are made by personnel of CERN CA or members of the CERN community. An external audit can be performed by any academic institution or relying party. If other trusted CAs or relying parties request an external assessment, the costs of the assessment must be paid by the requesting party, except for the costs of CERN CA personnel and infrastructure.

## 8.4. Topics covered by assessment

The audit will verify that the services provided by the CA comply with the latest approved version of the CP/CPS.

## 8.5. Actions taken as a result of deficiency

In case of a deficiency, the CERN CA responsible will announce the steps that will be taken to remedy the deficiency, including a timetable. If a discovered deficiency has direct consequences on the reliability of the certification process, the certificates (suspected to be) issued under the influence of this problem shall be revoked immediately.

## 8.6. Communication of results

The CERN CA staff will make the result publicly available on the CERN CA web site with all relevant details.

# 9. Other business and legal matters

## 9.1. Fees

No fees are charged for the CERN Grid Certification Authority certification service and therefore there are no financial encumbrances.

### 9.1.1. Certificate issuance or renewal fees

See 9.1.

### 9.1.2. Certificate access fees

See 9.1.

### 9.1.3. Revocation or status information access fees

See 9.1.

### 9.1.4. Fees for other services

See 9.1.

### 9.1.5. Refund policy

See 9.1.

## 9.2. Financial responsibility

No Financial responsibility is accepted for certificates issued under this policy.

### 9.2.1. Insurance coverage

No stipulation.

### 9.2.2. Other assets

No stipulation.

### 9.2.3. Insurance or warranty coverage for end-entities

No stipulation.

## 9.3. Confidentiality of business information

### 9.3.1. Scope of confidential information

No stipulation.

### 9.3.2. Information not within the scope of confidential information

No stipulation.

### 9.3.3. Responsibility to protect confidential information

No stipulation.

## 9.4. Privacy of personal information

### 9.4.1. Privacy plan

CERN Grid Certification Authority does not retain any specific private information. All required information is taken from CERN central registration databases, therefore CERN User services privacy plan applies.

### 9.4.2. Information treated as private

See 9.4.1.

### 9.4.3. Information not deemed private

See 9.4.1.

### 9.4.4. Responsibility to protect private information

See 9.4.1.

### 9.4.5. Notice and consent to use private information

See 9.4.1.

### 9.4.6. Disclosure pursuant to judicial or administrative process

See 9.4.1.

### 9.4.7. Other information disclosure circumstances

See 9.4.1.

## 9.5. Intellectual property rights

CERN Grid Certification Authority does not claim any intellectual property rights on certificates which are issued.

Parts if this document are inspired or even copied (in no particular order) from the CNRS, the Baltic Grid, pkIRISGrid, SWITCH and may indirectly derive from documents they draw from.

Anybody may freely copy from any version of the CERN Grid Certification Authority's Certificate Policy and Certification Practices Statement provided they include an acknowledgment of the source.

## 9.6. Representations and warranties

### 9.6.1. CA representations and warranties

No stipulation.

### 9.6.2. RA representations and warranties

No stipulation.

### 9.6.3. Subscriber representations and warranties

No stipulation.

### 9.6.4. Relying party representations and warranties

No stipulation.

### 9.6.5. Representations and warranties of other participants

No stipulation.

## 9.7. Disclaimers of warranties

CERN Grid Certification Authority uses software and procedures for the authentication of entities that, to the best of its knowledge, perform as required by this CP/CPS document. However it declines any warranty as to their full correctness. Also CERN Grid Certification Authority cannot be held responsible for any misuse of its certificate by a subscriber or any other party in possession of the corresponding private key, and of any unchecked acceptance of any of its certificates by a relying party.

Any relying party that accepts a certificate for any usage for which it was not issued does so on its own risk and responsibility.

## 9.8. Limitations of liability

CERN Grid Certification Authority declines any liability for damages incurred by a relying party accepting one of its certificates, or by a subscriber whose valid certificate is refused or whose revoked certificate is unduly accepted by a relying party.

It also declines any liability for damages arising from the non-issuance of a requested certificate, or for the revocation of a certificate initiated by the CA or the appropriate RA acting in conformance with this CP/CPS.

## 9.9. Indemnities

CERN Grid Certification Authority declines any payment of indemnities for damages arising from the use or rejection of certificates it issues.

End entities shall indemnify and hold harmless CERN Grid Certification Authority and all appropriate RAs operating under this CP/CPS against all claims and settlements resulting from fraudulent information provided with the certificate application, and the use and acceptance of a certificate which violates the provisions of this CP/CPS document.

## 9.10.Term and termination

### 9.10.1. Term

This document becomes effective after its publication on the Web site of the CERN Grid Certification Authority starting at the date announced there.

No term is set for its expiration.

### 9.10.2. Termination

This CP/CPS remains effective until it is superseded by a newer version.

### 9.10.3. Effect of termination and survival

Its text shall remain available for at least 5 years after the last certificate issued under this CP/CPS expires or is revoked.

## 9.11.Individual notices and communications with participants

All e-mail communications between the CA and its accredited RAs must be signed with a certified key.

All e-mail communications between the CA or an RA and a subscriber must be signed with a certified key in order to have the value of a proof. All requests for any action must be signed.

## 9.12.Amendments

### 9.12.1. Procedure for amendment

Amendments to this CP/CPS must undergo the same procedures as for the initial approval (see 1.5.4). Rephrasing provisions to improve their understandability as well as pure spelling corrections are not considered amendments.

### 9.12.2. Notification mechanism and period

The amended CP/CPS document shall be published on CERN Grid Certification Authority Web pages at least 2 weeks before it becomes effective.

CERN Grid Certification Authority will inform its subscribers and all relying parties it knows of by means of an e-mail.

### 9.12.3. Circumstances under which OID must be changed

Substantial changes shall cause the OID to be changed. The decision is made by the CERN Grid Certification Authority manager and submitted to the EUGridPMA for approval.

## 9.13. Dispute resolution provisions

Disputes arising out of the CP/CPS shall be resolved by the CERN CA manager.

## 9.14. Governing law

CERN Grid Certification Authority and its operation are subject to the French and Swiss laws. All legal disputes arising from the content of this CP/CPS document, the operation of CERN Grid Certification Authority and its accredited RAs, the use of their services, the acceptance and use of any certificate issued by CERN Grid Certification Authority shall be treated according to French and Swiss laws.

## 9.15. Compliance with applicable law

All activities relating to the request, issuance, use or acceptance of a CERN Grid Certification Authority certificate must comply with the French and Swiss laws.

Activities initiated from or destined for another country than France or Switzerland must also comply with that country's law.

## 9.16. Miscellaneous provisions

### 9.16.1. Entire agreement

This CP/CPS document supersedes any prior agreements, written or oral, between the parties covered by this present document.

### 9.16.2. Assignment

No provisions.

### 9.16.3. Severability

Should a clause of the present CP/CPS document become void because it is conflicting with the governing law (see 9.14) or because it has been declared invalid or unenforceable by a court or other law-enforcing entity, this clause shall become void (and should be replaced as soon as possible by a conforming clause), but the remainder of this document shall remain in force.

### 9.16.4. Enforcement (attorneys' fees and waiver of rights)

No stipulation.

### 9.16.5. Force Majeure

Events that are outside the control of CERN Grid Certification Authority will be dealt with immediately by the EUGridPMA.

## 9.17. Other provisions

No stipulation.

# 10. Bibliography

[i] The European Organization for Nuclear Research – http://www.cern.ch

[ii] S. Chokani, W. Ford, R. Sabett, C. Merrill and S. Wu, “Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework”, RFC 3647, November 2003 - http://www.ietf.org/rfc/rfc3647.txt

[iii] CERN Administrative Circular 11 (this document might require a valid CERN account, or a CERN network connection to be accessed):

http://cern.ch/humanresources/internal/admin_services/admincirc/English.doc/AC-111.pdf

[iv] HTML: The Markup Language: keygen – key-pair generator/input control: http://www.w3.org/TR/html-markup/keygen.html

[v] Forge: A native implementation of TLS (and various other cryptographic tools) in JavaScript: https://github.com/digitalbazaar/forge

[vi] Certification Request Syntax Specification, Version 1.7: https://tools.ietf.org/html/rfc2986

[vii] OpenSSL Project: https://www.openssl.org/

[viii] Microsoft Technet: Certreq: https://technet.microsoft.com/en-us/library/dn296456.aspx

[ix] Certification Request Syntax Specification, Version 1.7: https://tools.ietf.org/html/rfc2986

[x] OpenSSL Project: https://www.openssl.org/

[xi] Microsoft Technet: Certreq: https://technet.microsoft.com/en-us/library/dn296456.aspx

[xii] Authentication Profile for Classic X.509 Public Key Certification Authorities with secured infrastructure Version 4.3, OID 1.2.840.113612.5 https://www.eugridpma.org/guidelines/IGTF-AP-classic-4-3.pdf

[xiii] Authentication Profile for Classic X.509 Public Key Certification Authorities with secured infrastructure Version 4.3, OID 1.2.840.113612.5 https://www.eugridpma.org/guidelines/IGTF-AP-classic-4-3.pdf