CERN

European Organization for Nuclear Research

Category: CP/CPS

Status: For review

Document: CERN Root Certification Authority 2 CP-CPS.docx

Editor: Emmanuel Ormancey;Paolo.Tedesco@cern.ch

Date created: April 8, 2013 14:53

Last updated: January 12, 2015 14:06

Number of pages: 38

CERN Root Certification Authority 2 Certificate Policy and Certificate Practice Statement

Emmanuel Ormancey

Paolo Tedesco

CERN IT/OIS

Version 2.0 Revision 19

Document OID: 1.3.6.1.4.1.96.10.4.2.1.2.0

Table of contents

1 Introduction

1.1 Overview

The European Organization for Nuclear Research (CERN) is an intergovernmental organization having its seat in Geneva, Switzerland[1].

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 root CA of the CERN Grid Certification Authority, which will be referred to as “CERN Root Certification Authority 2” in the rest of this document.

This document is structured according to RFC 3647[2]. 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 Root Certification Authority 2 Certificate Policy and Certificate Practice Statement*. The following ASN.1 Object Identifier (OID) has been assigned to this document: 1.3.6.1.4.1.96.10.4.2.1.2.0.

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
Root CA 2 CP-CPS	.1
Major Version	.2
Minor Version	.0

1.3 PKI participants

1.3.1 Certification authorities

CERN Root Certification Authority 2 issues certificates to the following subordinate certification authorities (CERN CA):

- CERN Grid Certification Authority.

- CERN Certification Authority (for internal CERN use only).

1.3.2 Registration authorities

There is no registration authority for this CA. Only CERN Root Certification Authority 2 Staff can issue certificates, for subordinate certification authorities only.

1.3.3 Subscribers

See 1.3.1

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.

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 only by subordinate CERN CA.

1.4.2 Prohibited certificate uses

All certificate usages not listed in 1.4.1 are prohibited.

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 , http://gridca.cern.ch/gridca

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 Root Certification Authority 2 Manager (see 1.5.2) determines 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:

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

CERN Root Certification Authority 2 information is published at the following addresses:

- http://gridca.cern.ch/gridca
- http://cafiles.cern.ch/cafiles

2.2 Publication of certification information

CERN Root Certification Authority 2 publishes:

- all required certificates to trust this CA
- the CRL (certificate revocation list) for this CA
- all past and current versions of the CP/CPS for this CA

2.3 Time or frequency of publication

- Full CRL is published at least every 6 months, and after each revocation request.
- 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 CERN Root Certification Authority 2 are available to the public as read-only information from this web site: http://cafiles.cern.ch/cafiles.
- CRL updates are done manually by CERN Root Certification Authority 2 Staff.
- Modification of CP and CPS is only allowed to CERN employees with proper authorization by CERN Root Certification Authority 2 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 the following form:

Example: ***CN=CERN Trusted Certification Authority,DC=cern,DC=ch***

3.1.2 Need for names to be meaningful

The CN must be stated as the full name of the subordinate CA.

3.1.3 Anonymity or pseudonymity of subscribers

Subscribers must not be anonymous or pseudonymous. On CERN Root Certification Authority 2 Staff is allowed to request certificates.

3.1.4 Rules for interpreting various name forms

No stipulation.

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 Root Certification Authority 2. The subordinate CA name is reserved and cannot be reused after CA closure or termination.

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

Possession of the private key is verified for certificates issued by this CA by verifying the digital signature on the CSR (certificate signing request).

3.2.2 Authentication of organization identity

No stipulation.

3.2.3 Authentication of individual identity

Only CERN Root Certification Authority 2 Staff is allowed to request certificates on this CA. Authentication is done using CERN Root Certification Authority 2 Staff credentials.

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

Re-key must be executed manually on the CERN Root Certification Authority 2, only by CERN Root Certification Authority 2 Staff. Re-key after expiration is not possible, a new certificate must be requested.

3.3.2 Identification and authentication for re-key after revocation

A revoked certificate cannot be renewed; a new certificate must be requested.

3.4 Identification and authentication for revocation request

Revocations requests must be executed manually on the CERN Root Certification Authority 2, only by CERN Root Certification Authority 2 Staff.

4 Certificate life-cycle operational requirements

4.1 Certificate Application

4.1.1 Who can submit a certificate application

Only CERN Root Certification Authority 2 Staff can request a certificate.

4.1.2 Enrollment process and responsibilities

Certificate requests are submitted manually to CERN Root Certification Authority 2 by CERN Root Certification Authority 2 Staff.

Keys can be generated in two ways:

- Automatically by the CERN Root Certification Authority 2 in case of self-signed root certificate.
- Manually by the subordinate CA requesting a new certificate.

4.2 Certificate application processing

4.2.1 Performing identification and authentication functions

CERN Root Certification Authority 2 Staff uses its credentials to perform all operations.

4.2.2 Approval or rejection of certificate applications

No stipulation.

4.2.3 Time to process certificate applications

No stipulation.

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

No stipulation.

4.4 Certificate acceptance

4.4.1 Conduct constituting certificate acceptance

No stipulation.

4.4.2 Publication of the certificate by the CA

CERN Root Certification Authority 2 certificate and subordinate CA certificate are published to CERN internal Microsoft Active Directory service, and on this website: http://cafiles.cern.ch/cafiles.

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

The CERN Root Certification Authority 2 Staff assures all participants of the CERN subordinate CA 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,
- 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 Root Certification Authority 2 without changing the old key pair. The information contained in the certificate must be without change or modification, and there must be no suspicion of compromise to the private 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 can only be requested by CERN Root Certification Authority 2 Staff.

4.6.3 Processing certificate renewal requests

No stipulation.

4.6.4 Notification of new certificate issuance to subscriber

No stipulation.

4.6.5 Conduct constituting acceptance of a renewal certificate

No stipulation.

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

Not applicable for this CA and its subordinates. CERN Root Certification Authority 2 rolls over its keys/certificates with overlapping validities to ensure that no certificate re-key is needed.

4.7.1 Circumstance for certificate re-key

Not applicable.

4.7.2 Who may request certification of a new public key

Not applicable.

4.7.3 Processing certificate re-keying requests

Not applicable.

4.7.4 Notification of new certificate issuance to subscriber

Not applicable.

4.7.5 Conduct constituting acceptance of a re-keyed certificate

Not applicable.

4.7.6 Publication of the re-keyed certificate by the CA

Not applicable.

4.7.7 Notification of certificate issuance by the CA to other entities

Not applicable.

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 Root Certification Authority 2 should at least one of the following circumstances be known:

- A certificate contains data that is no longer valid.
- The private key of a subordinate CA has been changed, lost, stolen, published or compromised and/or misused in any other manner.
- The certification service is discontinued.

4.9.2 Who can request revocation

Revocation of certificates can only be done by the CERN Root Certification Authority 2 Staff.

4.9.3 Procedure for revocation request

The certificate will be revoked manually by the CERN Root Certification Authority 2 Staff, who will also publish manually a new CRL.

4.9.4 Revocation request grace period

No stipulation.

4.9.5 Time within which CA must process the revocation request

No stipulation.

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 2.3 apply.

4.9.8 Maximum latency for CRLs (if applicable)

The provisions of section 2.3 apply.

4.9.9 On-line revocation/status checking availability

No stipulation.

4.9.10 On-line revocation checking requirements

No stipulation.

4.9.11 Other forms of revocation advertisements available

No stipulation.

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 Root Certification Authority 2 become compromised, all certificates issued by the CERN Root Certification Authority 2 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

Certificate status services are not supported by the CERN Root Certification Authority 2.

4.10.1 Operational characteristics

Not applicable.

4.10.2 Service availability

Not applicable.

4.10.3 Optional features

Not applicable.

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 Root Certification Authority 2 with the addition of a further period of one year.

4.12 Key escrow and recovery

The CERN Root Certification Authority 2 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 Root Certification Authority 2 is a virtual server (PC) image. It's stored on removable Disk Drives stored in a secure location.

5.1.2 Physical access

Physical access to CERN Root Certification Authority 2 images is restricted to authorized personnel of the CERN Root Certification Authority 2 Staff.

5.1.3 Power and air conditioning

No stipulation.

5.1.4 Water exposures

No stipulation.

5.1.5 Fire prevention and protection

No stipulation.

5.1.6 Media storage

The CERN Root Certification Authority 2 image is kept in several removable storage media (Disk Drives). 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 Root Certification Authority 2 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 Root Certification Authority 2 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 manager 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 of 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 Root Certification Authority 2 Staff.

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

No stipulation.

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 Root Certification Authority 2 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 Root Certification Authority 2 service.

5.4.7 Notification to event-causing subject
No stipulation.

5.4.8 Vulnerability assessments
CERN Root Certification Authority 2 is offline, stored on hard drives in a safe location. All attempts to gain unauthorized access to this location are analyzed.

5.5 Records archival
5.5.1 Types of records archived
The provisions of section 5.4.1 apply.

5.5.2 Retention period for archive
The minimum retention period is 3 years.

5.5.3 Protection of archive
The records archive is accessible to CERN Root Certification Authority 2 Staff 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 Root Certification Authority 2 shall be performed when it will be necessary to issue a new subordinate CA certificate with a validity greater than the remaining validity of the signing certificate.

This will ensure that subordinate certificates will always be issued with their normal validity period, the CERN Root Certification Authority 2 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 subordinate 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 any subordinate CA's private key is (or suspected to be) compromised, the CA will:
    - Inform the 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 Root Certification Authority 2 operators will ensure that recovery procedures are functional and up to date. All CERN Root Certification Authority 2 software and system (Virtual Server image) will be backed up after any modification.

5.7.3 Entity private key compromise procedures

In case the private key of the CERN Root Certification Authority 2 is compromised, the CERN Root Certification Authority 2 Staff will:

- notify RA of all subordinate CAs
- 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 Root Certification Authority 2 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 Root Certification Authority 2 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 Root Certification Authority 2 terminates its services, it will:

- Inform the Registration Authorities 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 Root Certification Authority 2 Staff at the time of termination will be responsible for the subsequent archival of all records as required in section 5.5.2.

The CERN Root Certification Authority 2 issues ONLY CRLs during its last year (i.e. the maximal lifetime of a subscriber certificate) before the termination; this will allow subscribers' certificates of subordinate CAs to be used until they expire. In that case notice of termination is given no less than one year and 60 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 Certification Authority 2 machine (virtual server).
- The keys for subordinate CAs are generated by software, in the CA Service, or by Hardware in the Hardware Security Module of the subordinate CA.

6.1.2 Private key delivery to subscriber

The CA does not generate private keys for its subordinate CAs and therefore does not deliver private keys to subscribers.

6.1.3 Public key delivery to certificate issuer

Public keys are delivered manually by CERN Root Certification Authority 2 Staff.

6.1.4 CA public key delivery to relying parties

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

6.1.5 Key sizes

Keys of length less than 4096 bits are not accepted. The CERN Root Certification Authority 2 key is 4096 bits length.

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 for certificate signing and CRL signing.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic module standards and controls

No stipulation.

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

No stipulation.

6.2.3 Private key escrow

No stipulation.

6.2.4 Private key backup

The private key is backed up on a Removable Media (DVD-Rom), and stored in a safe location.

6.2.5 Private key archival

Private key archival is not supported.

6.2.6 Private key transfer into or from a cryptographic module

No stipulation.

6.2.7 Private key storage on cryptographic module

No stipulation.

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

No stipulation.

6.2.11 Cryptographic Module Rating

No stipulation.

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 Root Certification Authority 2 Certificate has a validity period of 20 years. The issued subordinate CA certificates have a validity period of 10 years.

6.4 Activation data

6.4.1 Activation data generation and installation

The private key is protected by a strong password.

6.4.2 Activation data protection

Only CERN Root Certification Authority 2 Staff 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 Root Certification Authority 2 is an offline Virtual Server running Microsoft Windows Server 2008 R2 and Microsoft CA 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 Root Certification Authority 2 staff when needed.

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. The CERN Root Certification Authority 2 server is a Virtual Server image stored on removable hard drives.

6.8 Time-stamping

The hardware clock of the offline CERN Root Certification Authority 2 system will be synchronized manually by the CERN Root Certification Authority 2 Staff when the Virtual Server starts.

7 Certificate, CRL, and OCSP profiles

7.1 Certificate profile

All certificates issued by CERN Root Certification Authority 2 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 Root Certification Authority 2.

7.1.2 Certificate extensions

The extensions to the X.509 v3 certificate that shall be present in CERN Root Certification Authority 2 certificates are:

- 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 point: URL and LDAP path.
- Certificate Policies: OID

7.1.3 Algorithm object identifiers

The OIDs for algorithms used for signatures of certificates issued by CERN Root Certification Authority 2 are:

- 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 CA has a unique and unambiguous Distinguished Name (DN). CERN CA prefers that organizations use domain component naming.

- Issuer subject:
    - CN=CERN Root Certification Authority 2,O=cern,C=ch
- Subordinate CA Subject:
    - CN=CERN Trusted Certification Authority 2,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: 1.3.6.1.4.1.96.10.4.2.1.2.0

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 Root Certification Authority 2 creates and publishes X.509 v2 CRLs.

7.2.2 CRL and CRL entry extensions

CERN Root Certification Authority 2 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

7.3 OCSP profile

7.3.1 Version number(s)

No stipulation.

7.3.2 OCSP extensions

No stipulation.

8 Compliance audit and other assessments

8.1 Frequency or circumstances of assessment

CERN Root Certification Authority 2 shall make at least once a year a self-assessment to check the compliance of the operation 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 CERN Root Certification Authority 2 Staff 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 Root Certification Authority 2 Staff 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 Root Certification Authority 2 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 Root Certification Authority 2 staff will make the result publicly available on the web site (http://gridca.cern.ch/gridca) with all relevant details.

9 Other business and legal matters

9.1 Fees

No fees are charged for the CERN Root Certification Authority 2 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 Root Certification Authority 2 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 Root Certification Authority 2 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 Root Certification Authority 2'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 Root Certification Authority 2 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 Root Certification Authority 2 cannot be held responsible for any misuse of its certificate by a subscriber or any

other party who got 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 Root Certification Authority 2 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 Root Certification Authority 2 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 Root Certification Authority 2 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 Root Certification Authority 2 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 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 the web pages (http://cafiles.cern.ch/cafiles) at least 2 weeks before it becomes effective.

CERN Root Certification Authority 2 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 Root Certification Authority 2 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 Root Certification Authority 2 manager.

9.14 Governing law

CERN Root Certification Authority 2 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 Root Certification Authority 2 and its accredited RAs, the use of their services, the acceptance and use of any certificate issued by CERN Root Certification Authority 2 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 Root Certification Authority 2 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 Root Certification Authority 2 will be dealt with immediately by the EUGridPMA.

9.17 Other provisions

No stipulation.

10 Bibliography

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

[2] 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