Certificate Policy
and
Certification Practice Statement
CNRS2 (root)

Version 0.1

September 9, 2009

Document OID
1.3.6.1.1.10813.1.1.9.0.1

Online:
http://igc.services.cnrs.fr/

Contents

1. INTRODUCTION

1.1 Overview

This document is a draft. It is structured according to RFC 3647.

It describes the set of rules used by the root CNRS Certification Authority.

1.2 Document name and identification

Document title: Certification Policy and Certification Practice Statement CNRS

Version: 0.1

Date: September 9, 2009

Object Identifier of Document (OID) : 1.3.6.1.1.10813.1.1.9.0.1

1.3 PKI participants

1.3.1 Certification authorities

The "CNRS2 CA" is a root Certification authority operated by the DSI and the UREC of the CNRS. Root CNRS2 CA has a self-signed certificate. It only issue certificate for subordinate CA. Actually, CNRS2 CA has 3 subordinate CAs :

- CNRS2-Standard: This CA issue certificates for general uses to people depending on a CNRS laboratory. It represents about 80 000 persons. Each laboratory has its own Registration Authority
- CNRS2-Plus: This CA issue personal certificates for Registration Authorities.
- CNRS2-Projets: This CA issue certificates to subordinate CAs required by projects in which the CNRS is involved, for example GRID2-FR which is dedicated to the Grid Projects of the CNRS. The project manager decides which people, institutes may get a Certificate. Each sub-CA has it own CP/CPS. Each project has a limited lifetime and may include external organizations.

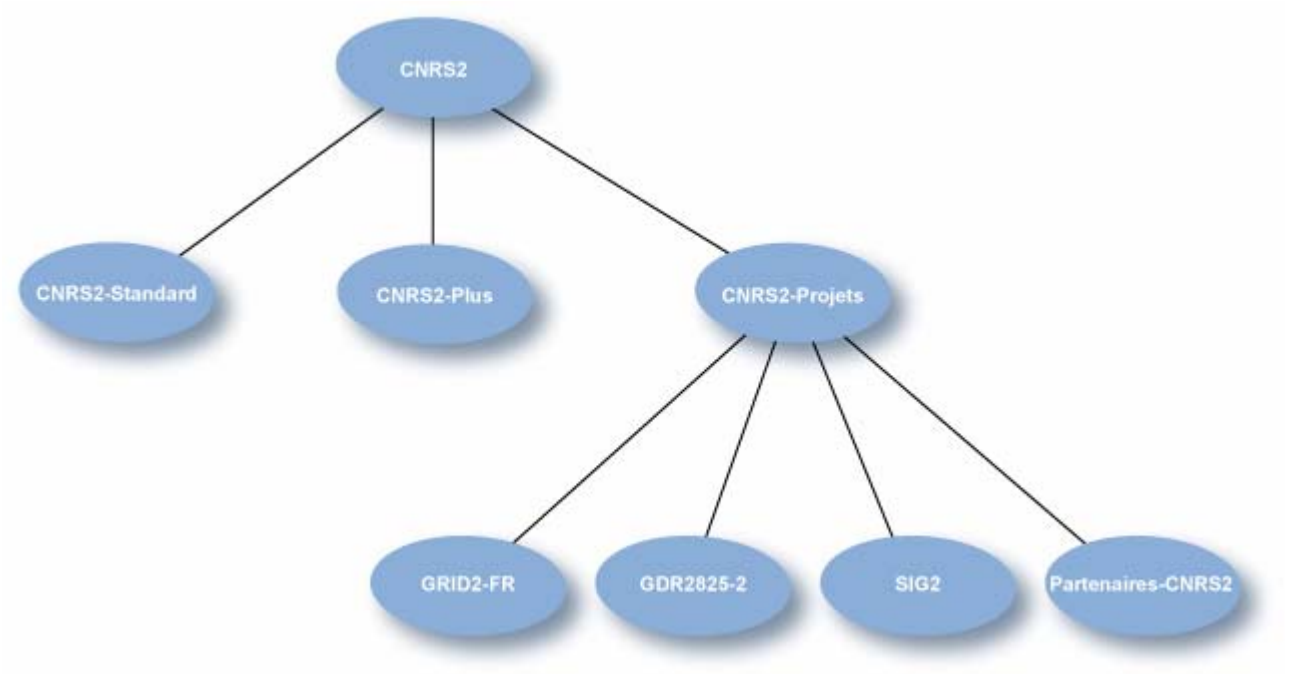

Figure 1: CNRS2 CA and its 3 subordinate CAs

1.3.2 Registration authorities

Registration Authorities are formed by the members of the CNRS CMG staff. They are responsible and decide if it is necessarily to create, renew, let expired or revoke a CA certificate.

1.3.3 Subscribers

CNRS2 CA issue certificates to subordinate CAs. Consequently, role and responsibilities of the subscribers are specified in the CP/CPS of the respective issuing CA.

The certificates issued by a CNRS' subordinate CA must not be used for financial transactions or for purpose contrary the French law.

1.3.4 Relying parties

Relying parties are individuals or machines or services which use certificates of subordinate issuing CAs.

For:

- Individuals
- They work in a CNRS' laboratory or service. They are/aren't CNRS, permanent contract or temporarily, trainee, Ph.D. student, quest…)
- CNRS agents but not working in a CNRS' laboratory
- Agents from an external organization requiring a certificate to collaborate with the CNRS
- Host/Services from a CNRS' laboratory or used for the benefice of the CNRS, or used by agent from the CNRS. Request must be validated by the RA of the unit or the manager of the unit.

They use root CA Certificate to verify the validity of the issuing CA.

1.3.5 Other participants

Other participants are individuals or organizations that are in some way involved with PKI-related services. This is the main goal of the CNRS2-Plus issued certificates.

1.4 Certificate usage

1.4.1. Appropriate certificate uses

The authorized use of the signing key of the CNRS2 CA is limited to sign its own certificate, CRL and the certificates of the subordinate CAs.

1.4.2 Prohibited certificate uses

All uses out of the scope described into the section 1.4.1 are prohibited.

1.5 Policy administration

1.5.1 Organization administering the document

The CNRS2 CP/CPS is written and updated by CNRS/UREC unit:

Alice de Bignicourt

UREC

150, rue de la Chimie

Domaine Universitaire

38041 Grenoble Cedex 9

France

Mail: igc-support@services.cnrs.fr

Web: http://igc.services.cnrs.fr/

1.5.2 Contact person

The following person is the contact for any remark or question about CNRS2 CA:

DSI

TOUR GAIA

RUE PIERRE-GILLES DE GENNES

BP 21902

31319 LABEGE CEDEX

France

Mail: igc-support@services.cnrs.fr

1.5.3 Person determining CPS suitability for the policy

CNRS2 CA Manager Group is responsible for the suitability and applicability of this CP/CPS. Changes or updates are made in accordance of the French law.

1.5.4 CPS approval procedures

CNRS2 CA Manager Group evaluates this document each time there is a modification.

1.6 Definitions and acronyms

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

Certificate

Synonymous with Public Key Certificate.

Certificate Revocation List (CRL)

A time stamped list enumerating revoked certificates which its signed by the CA and available in a public repository.

Certification Authority (CA)

The Public Key Infrastructure (PKI) who issues X509 certificates.

Certification Practice Statement (CPS)

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

Cipher

A cryptographic algorithm used to encrypt and decrypt files and messages.

CNRS

Centre National de la Recherche Scientifique (CNRS) is a French governmental research institute that defines its mission as producing knowledge and making it available to society.

Credentials

Evidence or testimonials governing the user's right to access certain systems (e.g. User name, password…)

CRL

This is the Certificate Revocation List. This list collect all the certificate declared as "invalid certificates". This list is signed and issued by the CA at regular intervals, and is used to validate or invalidate a certificate.

DNS

Domain Name System. The Internet system of holding a distributed register of entity names.

DSI

The Direction des Systèmes d'Information is a direction of the CNRS responsible of the Information System of the institute.

FQDN

Fully Qualified Domain Name

IANA

Internet Assigned Numbers Authority

OID

Object Identifier

PKI

Public Key Infrastructure

Public Key Certificate

A data structure containing the public key of an entity and some other information, which is digitally signed by the CA.

Registration Authority (RA)

A Registration Authority is an person responsible for verifying the identity of the requester and the validity of the request.

Requester

Individuals which have applied a certificate request, and not yet obtained the certificate.

Revocation

This is the act that consist in invalidate a certificate by a CA. (See also CRL)

Sub-CA

This means the subordinate Certification Authority. A CA has created a certificate for another CA. In example: CNRS-Projets is a sub-CA of CNRS.

UREC

Unité des RÉseaux du CNRS which the aim is to promote, develop and organize network services for CNRS.

CNRS2 CA Manager Group (CNRS CMG)

This committee is responsible for the management of the CNRS2 CA. It is composed by agents of the DSI and the UREC described below.

2 PUBLICATION AND REPOSITORY RESPONSIBILITIES

CNRS Grid CMG will publish CP/CPS through the dedicated web site igc.services.cnrs.fr. The documents should be electronically signed to ensure the authenticity, and the integrity.

2.1 Repositories

Any information is available on its web site: http://igc.services.cnrs.fr/

There is no web site for CAs delivering certificates for sub-CA, but information can be found for CAs delivering certificates for end-entities:

- To reach information about CNRS2-Standard CA: http://igc.services.cnrs.fr/CNRS2-Standard
- To reach information about CNRS2-Plus CA: http://igc.services.cnrs.fr/CNRS2-Plus
- To reach information about GRID2-FR CA, which is a sub-CA of CNRS2-Projets: http://igc.services.cnrs.fr/GRID2-FR

2.2 Publication of certification information

The web site provides information about CNRS2 CA such as:

- The CNRS certificate (display on the screen, in PEM format, in DER format)
- The CRL(display on the screen, in PEM format, in DER format)
- All past and current versions of the CP/CPS
- Links on the subordinate CAs

2.3 Time or frequency of publication

CP/CPS should be verified every 2 years. The CP/CPS must be updated if any information stipulated in it has changed, and published as son as approved.

The certificates are published as soon as issued.

2.4 Access controls on repositories

No access control to these publications is performed

3 IDENTIFICATION AND AUTHENTICATION

3.1 Naming

3.1.1 Types of names

The subject name is an X500 distinguish name. Each certificate issued by the CNRS2 CA has the following subject: C=FR, O=CNRS, CN="CA's name" where:

- C the field for the country which the value is always FR
- the organization which the value is always CNRS
- CN the common name which the value is the name of the subordinate CA.
- Example: C=FR, O=CNRS, CN=CNRS2-Standard

3.1.2 Need for names to be meaningful

The subject name must have a reasonable meaning with the use of the sub-CA.

3.1.3 Anonymity or pseudonymity of subscribers

No anonymity or the use of a pseudonym is allowed.

3.1.4 Rules for interpreting various name forms

See section 3.1.1

3.1.5 Uniqueness of names

The subject name must be unique.

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 private key of the created certificates are managed (in a secure way) by the RA of CNRS.

3.2.2 Authentication of organization identity

No stipulation.

3.2.3 Authentication of individual identity

No user certificate is issued by this CA.

3.2.4 Non-verified subscriber information

No stipulation.

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

No stipulation.

3.3.2 Identification and authentication for re-key after revocation

There is no re-keying available after revocation.

3.4 Identification and authentication for revocation request

A revocation must be request as soon as needed.

- Persons eligible to request a revocation are:
- A member of the CNRS CMG
- The contact of the CNRS2 CA
- Every people who suspect that the private key is compromised or suspecte to be compromised.

The CNRS CMG evaluate if it is needed or not.

4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

The CP/CPS of every subordinated issuing CA defines in detail Subscriber Certificate application.

4.1 Certificate Application

4.1.1 Who can submit a certificate application

See CP/CPS of each sub-CA.

4.1.2 Enrollment process and responsibilities

See CP/CPS of each sub-CA.

4.2 Certificate application processing

Requesters have to prove their identity according the documents as specified by the relevant issuing CA.

4.2.1 Performing identification and authentication functions

See CP/CPS of each sub-CA.

4.2.2 Approval or rejection of certificate applications

See CP/CPS of each sub-CA.

4.2.3 Time to process certificate applications

See CP/CPS of each sub-CA.

4.3 Certificate issuance

4.3.1 CA actions during certificate issuance

Here is the process:

A Certificate Signing Request is submitted to a sub-CA

The sub-CA verify the integrity of the request

On successful control, then the sub-CA issue the certificate and inform the requester.

4.3.2 Notification to subscriber by the CA of issuance of certificate

Requesters are notified by a notification e-mail containing information to get back the certificate.

4.4 Certificate acceptance

4.4.1 Conduct constituting certificate acceptance

See CP/CPS of the concerned sub-CA.

4.4.2 Publication of the certificate by the CA

Certificates are published on the sub-CA's web site as soon as issued. For example, to get a certificate issued by GRID2-FR CA, the web site is http://igc.services.cnrs.fr/GRID2-FR

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

CNRS2 CA issue certificate for CAs and for CAs only. Consequently, certificate usage for end-entities are defined in CP/CPS of each sub-CA.

4.5.2 Relying party public key and certificate usage

See CP/CPS of the concerned sub-CA.

4.6 Certificate renewal

No renewal is supported by the CNRS PKI software.

4.6.1 Circumstance for certificate renewal

No Stipulation.

4.6.2 Who may request renewal

No Stipulation.

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

No Stipulation.

4.6.7 Notification of certificate issuance by the CA to other entities

No Stipulation.

4.7 Certificate re-key

Re-keying are stipulated in the CP/CPS of the according issuing CA.

4.7.1 Circumstance for certificate re-key

No Stipulation.

4.7.2 Who may request certification of a new public key

No Stipulation.

4.7.3 Processing certificate re-keying requests

No Stipulation.

4.7.4 Notification of new certificate issuance to subscriber

No Stipulation.

4.7.5 Conduct constituting acceptance of a re-keyed certificate

No Stipulation.

4.7.6 Publication of the re-keyed certificate by the CA

No Stipulation.

4.7.7 Notification of certificate issuance by the CA to other entities

No Stipulation.

4.8 Certificate modification

No modification after issuing certificate is possible. These kinds of requests are processed as initial requests. If a certificate already exists, this one is revoked and then, subscriber can request a new one.

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

4.9.1 Circumstances for revocation

Certificate of a sub-CA of CNRS2 CA must be revoked as soon as possible if its private key is compromised or suspected to be compromised.

4.9.2 Who can request revocation

The CNRS CMG is available to request revocation.

4.9.3 Procedure for revocation request

Procedure for revocation request is defined in the sub-CA's CP/CPS.

4.9.4 Revocation request grace period

Revocation request grace period is stipulated in the sub-CA's CP/CPS.

4.9.5 Time within which CA must process the revocation request

This information is stipulated in the sub-CA's CP/CPS.

4.9.6 Revocation checking requirement for relying parties

Relying parties must verify the validity of the certificates at all times by using the CRLs, following the all path validation procedure specified in the RFC 3280. CRLs must be downloaded from the PKI's web site.

4.9.7 CRL issuance frequency (if applicable)

The CRL of the root CNRS2 CA is updated at least every 364 days, or as soon as a revocation has been processed.

4.9.8 Maximum latency for CRLs (if applicable)

According to the section 4.9.7, the maximum latency is 1 year less 1 day, so 364 days for a usual year, and 365 days for a leap year.

4.9.9 On-line revocation/status checking availability

No service –such as OCSP – is available at this moment.

4.9.10 On-line revocation checking requirements

Only Registration Authorities can request on-line revocation authenticating them-selves using their own personal certificate.

4.9.11 Other forms of revocation advertisements available

Persons who have lost their private key can contact the registration authority of his/her unit or to request revocation.

4.9.12 Special requirements re key compromise

No stipulation.

4.9.13 Circumstances for suspension

CNRS2 CA does not suspend any certificate.

4.9.14 Who can request suspension

CNRS2 CA does not suspend any certificate.

4.9.15 Procedure for suspension request

CNRS2 CA does not suspend any certificate.

4.9.16 Limits on suspension period

CNRS2 CA does not suspend any certificate.

4.10 Certificate status services

4.10.1 Operational characteristics

CNRS2 CA online repository contains a list of valid certificates, a list of the validation certification chain, and a list of revoked certificates (CRL). All lists are continuously updated.

4.10.2 Service availability

The on-line repository is maintained on best effort basis with intended availability of 24x7.

4.10.3 Optional features

No stipulation.

4.11 End of subscription

End of subscription details are specified in the CP/CPS of the according issuing sub-CA.

4.12 Key escrow and recovery

4.12.1 Key escrow and recovery policy and practices

No escrow or recovery service is supported by the CNRS2 CA.

4.12.2 Session key encapsulation and recovery policy and practices

No stipulation.

5. FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

Stipulations in this section are applicable to this CA. For sub-CAs, refer to the corresponding CA.

5.1 Physical controls

5.1.1 Site location and construction

The CNRS2 CA is located in a controlled access and protected room in the CNRS' DSI building. The address is:

TOUR GAIA

RUE PIERRE-GILLES DE GENNES

BP 21902

31319 LABEGE CEDEX

France

Mail: igc-support@services.cnrs.fr

5.1.2 Physical access

Physical access is granted to the authorized staff only, protected by a badge pass at the entrance of the building, and an another badge pass to the room itself.

5.1.3 Power and air conditioning

Workspace with power facilities is available whenever needed. To create an optimal environment for the system according to generally accepted best practices, this room is air-conditioned.

5.1.4 Water exposures

The building has water sensors in all double floors. Adequate alarming is ensured. The data center is located in an area that has no special exposures.

5.1.5 Fire prevention and protection

The room storing the CA machines has a fire alarm system installed.

5.1.6 Media storage

Back-up of any information (meaning off line and on line information) about CA is backed-up on a secured storage media, and stored it self in a secured place.

5.1.7 Waste disposal

Removable media used by CA are physically destroyed before wasted.

5.1.8 Off-site backup

The system periodically generates a backup of all digital information (data, code, configuration, etc.). The backup contains all information relevant for the CA service in encrypted form. A CD or DVD is created and stored off-site in a bank safe deposit box.

This process guarantees that the off-site storage of all data from the PKI environment is fully encrypted.

5.2 Procedural controls

5.2.1 Trusted roles

The CNRS'PKI software requires 2 trusted roles: "Registration Authority role", and "super Registration Authority role".

- The Registration Authorities validate certificates for end-entities,
- The super-Registration Authorities validate certificates for Registration Authorities. Super Registration Authorities own a certificate issued by CNRS2-Plus CA, and the scope is to issue only CNRS2-Plus certificates.

Administrators of the system have a total control of the hardware, operating system, and software management. On the other hand, cryptographic information, like the private key of the CA, or the CA itself, is under control of restricted personnel.

5.2.2 Number of persons required per task

All the CNRS' PKI software is managed and supported (including role-driven) by:

Access to the machines: 3 employees for network access configuration and CA maintenance and management tasks

Operations: 2 employees for system administration, CA operation

Validating certificates Signing Request: depending on the CA. Refer to the CP/CPS of the appropriated CA

5.2.3 Identification and authentication for each role

Within the CNRS PKI CA software, identification and authentication for all roles is performed using CNRS certificates.

5.2.4 Roles requiring separation of duties

No stipulation

5.3 Personnel controls

5.3.1 Qualifications, experience, and clearance requirements

Only persons who are technically and professionally qualified are granted to access.

5.3.2 Background check procedures

CNRS' CA is managed by employees of the CNRS. Background of each employee of the CNRS must to do not contain any criminal record.

5.3.3 Training requirements

During the year, there is at least one training for the new Registration Authorities and Super Registration Authorities. This meeting includes information about cryptographically concepts, security issues, and familiarized the trainees to the interface of the CNRS' PKI software.

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

If unauthorized action is performed using a CNRS certificate, CNRS CMG will statute and if necessarily, will revoke the "dirty" certificate.

5.3.7 Independent contractor requirements

Contractors who require any access to the CA, operations, or to become a RA must proof their qualification. If not, contractors must follow the training.

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 audited:

- Certificate requests
- Rejected certificate requests
- Certificate signing
- Certificate issues
- Certificate revocation
- CRL issues
- Boots, shutdowns and reboots of CA machines
- E-mails sent and received by CNRS-PKI software

5.4.2 Frequency of processing log

Logs are processed persistently, and archived every month. Archives are kept as long as possible, and never deleted.

5.4.3 Retention period for audit log

Logs are kept as long as possible, and never deleted.

5.4.4 Protection of audit log

Different accesses are granted depending of your role:

- Full access to the CA administrators
- Restricted access to the managed unit for RAs and Super RAs authenticated by their certificates and access controlled by IP address.

5.4.5 Audit log backup procedures

The audit log is back up every night on an off-line medium.

5.4.6 Audit collection system (internal vs. external)

The audit log collection system is an internal UREC/CNRS system.

5.4.7 Notification to event-causing subject

No stipulation.

5.4.8 Vulnerability assessments

All the CNRS' PKI (meaning this CA and all the sub-CA) are monitored all the time (24x7).

5.5 Records archival

5.5.1 Types of records archived

The following events are audited:

- Certificate requests
- Rejected certificate requests
- Certificate signing
- Certificate issues
- Certificate revocation
- CRL issues
- Boots, shutdowns and reboots of CA machines
- E-mails sent and received by CNRS-PKI software

5.5.2 Retention period for archive

Logs are processed persistently, and archived every month. Archives are kept as long as possible, and never deleted.

5.5.3 Protection of archive

Different accesses are granted depending of your role:

- Full access to the CA administrators
- Restricted access to the managed unit for RAs and Super RAs authenticated by their certificates and access controlled by IP address.

5.5.4 Archive backup procedures

The archives are backed up every night on an off-line medium.

5.5.5 Requirements for time-stamping of records

The on-line machines are synchronized to a NTP stratum 2 time server. The off-line machine is manually synchronized.

5.5.6 Archive collection system (internal or external)

The audit log collection system is an internal UREC/CNRS system.

5.5.7 Procedures to obtain and verify archive information

Archive information can be requested to the CNRS CMG members. The contacted member provide information to the requester.

5.6 Key changeover

To avoid interruption of validity of subordinate keys, the new CA private key is generated one or two year before the expiration of the old key, depending of the life time of the certificates issued to the end-entities by the sub-CA. The new public key is available on the one-line repository, and new certificates can be issued.

5.7 Compromise and disaster recovery

5.7.1 Incident and compromise handling procedures

In this case of the CA equipment is damaged but (the CA private key is not destroyed, corrupted or suspected to be corrupted) the CA operators have to re-establish as quickly as possible from backup or scratch.

If private key is damaged, see section 5.7.3.

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

The root CNRS2 CA and its sub –CAs are backed-up every night.

5.7.3 Entity private key compromise procedures

If an entity's private key is compromised, its relevant RA or other person, as described in section 4.9.2, must request a revocation as described in section 4.9.3.

5.7.4 Business continuity capabilities after a disaster

The CNRS CMG will take the appropriate decision to establish a new PKI service in a best effort.

5.8 CA or RA termination

5.8.1 CA termination

In case of the CA's private key is lost, destroyed, compromised or suspected to be compromised, the CA will:

- CA certificate is revoked
- Stop issuing certificate and CRLs
- Inform all subscribers, all relying parties, RAs and cross-certifying CAs
- Make information of its termination widely available
- Destroy all copies of its private key
- Generate a new CA key pair, a new certificate and CA will make all this information available on the CA portal.
- Notify the relevant security contact
- Notify all relaying parties

5.8.2 RA termination

If the RA's private key is compromised, the RA:

- informs the CA
- requests a revocation of its certificate
- requests a new certificate as an initial registration.

6. TECHNICAL SECURITY CONTROLS

6.1 Key pair generation and installation

6.1.1 Key pair generation

The key pair for the "CNRS2 CA" (Root CA Key) has been created off line dedicated machine and stored on an off-line medium, kept on a secured locked place.

The key pairs for the subordinated issuing CAs of the CNRS2 CA (Issuing CA Keys) have been generated on the same machine.

6.1.2 Private key delivery to subscriber

The key pairs are generated as described below:

- For personal certificate: When the user fills the certificate request form, on the web portal of the CA, with his browser, the public and private keys are generated by his browser on his machine.
- For server and service certificates: The key pair is generated by the CA. The certificate is stored by the CA, but the private key is not kept by the CA.

No private key is kept by the CA.

6.1.3 Public key delivery to certificate issuer

Personal public keys are picked up by the CA during an SSL session via the web portal.

6.1.4 CA public key delivery to relying parties

The CA certificate is available via the CA web portal: http://igc.services.cnrs.fr/

6.1.5 Key sizes

The CNRS2 CA uses a 2048 bit RSA key.

All sub-CAs use 2048 bit RSA key.

6.1.6 Public key parameters generation and quality checking

No subscriber certificates are issued from the CNRS2 CA.

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

The signing key of this CA and its subordinated issuing CAs are the only keys permitted for signing certificates and CRLs and have the keyCertSign and CRLSign key usage bit set.

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

CNRS2 CAs are not available for giving keys in an escrow or accepting escrow copies of keys of other parties.

6.2.4 Private key backup

The end entities private keys must be protected and backed up on an off-line medium by the owner.

CA private key is kept, encrypted, in multiple CD-Rom copies stored in different secure locations. The pass phrase to access the private keys is known by four people.

6.2.5 Private key archival

See section 6.2.4

6.2.6 Private key transfer into or from a cryptographic module

See section 6.2.4

6.2.7 Private key storage on cryptographic module

The CA private key is stored encrypted, on an off-line medium.

6.2.8 Method of activating private key

The activation of the CA private key is done by providing the pass phrase.

6.2.9 Method of deactivating private key

No stipulation.

6.2.10 Method of destroying private key

After CA is over (see section 5.8.1) and after the archival period for archives has expired, all media that contain the private key of the CA will be securely and permanently destroyed.

6.2.11 Cryptographic Module Rating

No stipulation.

6.3 Other aspects of key pair management

6.3.1 Public key archival

See section 6.2.4

6.3.2 Certificate operational periods and key pair usage periods

The root CNRS2 CA certificate has a lifetime of 20 years.

6.4 Activation data

All private keys are protected by a pass phrase known by the authorized persons.

6.4.1 Activation data generation and installation

The pass phrase length is at least of 15 characters. It is composed by letters, numbers and signs, and has no repetitive keystrokes.

6.4.2 Activation data protection

The pass phrase is known by the staff members. A modification into the staff implies the pass phrase will be changed.

6.4.3 Other aspects of activation data

No stipulation.

6.5 Computer security controls

6.5.1 Specific computer security technical requirements

CA servers are dedicated servers:

- Their operating systems are maintained at a high level of security on which are applied all recommended patches
- The network services are reduced to the bare minimum
- The servers access is restricted to a few stations protected behind a firewall
- The machines used to run web portal and to hold on-line repositories are behind a firewall.

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 CNRS2 CA root machine is not connected to any kind of network. Its private key is only used to sign the subordinate CAs' certificates.

6.8 Time-stamping

No stipulation.

7. CERTIFICATE, CRL, AND OCSP PROFILES

7.1 Certificate profile

7.1.1 Version number(s)

Version number of the root CA certificate is **X.509 v3**

7.1.2 Certificate extensions

Extensions of the root CA certificate:

- X509v3 Basic Constraints:
  - CA:TRUE
- X509v3 Subject Key Identifier:
  - 50:97:B6:0D:F7:AC:33:17:AF:F1:1D:46:3C:6B:3B:FF:00:A0:E5:E5
- X509v3 Authority Key Identifier:
  - keyid: 50:97:B6:0D:F7:AC:33:17:AF:F1:1D:46:3C:6B:3B:FF:00:A0:E5:E5
  - DirName:/C=FR/O=CNRS/CN=CNRS2
  - serial:00
- X509v3 Key Usage:
  - Certificate Sign, CRL Sign

Extensions for sub-CAs of the root CA:

Only the "X509v3 Subject Key Identifier" extension varies from extensions of the root CNRS2 CA.

7.1.3 Algorithm object identifiers

See section 1.2

7.1.4 Name forms

All certificates issued by this CA and all the sub-CAs of this CA contain a full X.500 distinguish name of the certificate issuer and certificate subject in the issuer. Each Distinguish Name must be in an X.501 form, Printable String.

7.1.5 Name constraints

See section 3.1.1

7.1.6 Certificate policy object identifier

Each certificate must reference a policy OID, and may contain several as long as none of the policy constraints conflict.

For information see chapter 7.1.2 of this document.

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)

Version number of the root CA CRL is **X.509 v1**

7.2.2 CRL and CRL entry extensions

No stipulation.

7.3 OCSP profile

No service – such as OCSP – is available at this moment.

7.3.1 Version number(s)

No service – such as OCSP – is available at this moment.

7.3.2 OCSP extensions

No service – such as OCSP – is available at this moment.

8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS

Compliance Audits and other assessments determinate if the CNRS2 CA performs in accordance with the present CP/CPS.

CNRS CMG should perform compliance audit, and will not publish the report.

8.1 Frequency or circumstances of assessment

Only substantial changes in CP/CPS or changes in the technical security controls will be notified to all relevant relying parties and to the public on-line repositories. It will also be announced widely available.

Users will not be informed in advance of changes to CNRS2 CA's CP/CPS.

8.2 Identity/qualifications of assessor

The last version of this document is available from the on-line repositories of the each sub-CA issuing certificates to end-entities:

- CNRS2-Standard CA: http://igc.services.cnrs.fr/CNRS2-Standard
- CNRS2-Plus CA: http://igc.services.cnrs.fr/CNRS2-Plus
- GRID2-FR CA, which is a sub-CA of CNRS-Projets: http://igc.services.cnrs.fr/CNRS-GRID2-FR
- Etc.

8.3 Assessor's relationship to assessed entity

Auditors should be independent of the CNRS CMG.

8.4 Topics covered by assessment

Auditors will conduct the compliance audits according to the EUGridPMA recommendations.

8.5 Actions taken as a result of deficiency

Depending on severity and urgency, all issues will be entered into the CNRS PKI system either as incidents or as problems and tracked accordingly.

8.6 Communication of results

Report of the compliance audit shall be communicated to the CNRS CMG.

Within 30 days of receiving the compliance audit results the, CNRS CMG will prepare a statement regarding the open issues and present, if necessarily, a new CP/CPS.

9. OTHER BUSINESS AND LEGAL MATTERS

9.1 Fees

No fees shall be charged.

9.1.1 Certificate issuance or renewal fees

No fees shall be charged.

9.1.2 Certificate access fees

No fees shall be charged.

9.1.3 Revocation or status information access fees

No fees shall be charged.

9.1.4 Fees for other services

No fees shall be charged.

9.1.5 Refund policy

No fees shall be charged.

9.2 Financial responsibility

No financial responsibility is accepted.

9.2.1 Insurance coverage

No financial responsibility is accepted.

9.2.2 Other assets

No financial responsibility is accepted.

9.2.3 Insurance or warranty coverage for end-entities

No financial responsibility is accepted.

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

CNRS2 CA collects subscriber's information such as:

- full name
- organization
- unit names (if there is)
- e-mail address
- Phone number

9.4.2 Information treated as private

CNRS2 CA collects also subscriber's phone number but doesn't publish it nor includes it in the certificate.

CNRS2 CA has never access to certificate private keys.

9.4.3 Information not deemed private

Subscriber's full name, organization, unit names (if there is), e-mail address are included in the certificate and are not confidential. Only RA and CNRS CMG have access to this information stored into the request. Once the request is validated, only CNRS CMG has access to this information.

9.4.4 Responsibility to protect private information

Persons whom access to private information (see section 9.4.3) secure it from compromise and prevent from using it or disclosing it to third parties.

9.4.5 Notice and consent to use private information

CNRS CMG and all RAs will only use private information if a subscriber has given full consent in the course of the registration process. All collected information will be subject to the French law.

9.4.6 Disclosure pursuant to judicial or administrative process

CNRS CMG will release private information on judicial or other authoritative order.

9.4.7 Other information disclosure circumstances

No stipulation.

9.5 Intellectual property rights

CNRS asserts no copyrights on information published by the CNRS2 CA.

9.6 Representations and warranties

9.6.1 CA representations and warranties

CNRS CMG ensures compliance of the root CNRS2 CA with all the terms stated in this CP/CPS.

9.6.2 RA representations and warranties

Refer to the sub-CA issuing certificates for end-entities.

9.6.3 Subscriber representations and warranties

Refer to the sub-CA issuing certificates for end-entities.

9.6.4 Relying party representations and warranties

Refer to the sub-CA issuing certificates for end-entities.

9.6.5 Representations and warranties of other participants

Refer to the sub-CA issuing certificates for end-entities.

9.7 Disclaimers of warranties

Except for the warranties stated herein including related agreements for this, CNRS CMG disclaims any and all other possible warranties, conditions, or representations (express, implied, oral or written) including any warranty of merchantability.

9.8 Limitations of liability

- CNRS2 CA guarantees to control the identity of the certification requests according to the procedures described in this document
- CNRS2 CA guarantees to control the identity of the revocation requests according to the procedures described in this document
- CNRS2 CA is run on a best effort basis and does not give any guarantees about the service security or suitability
- CNRS2 CA shall not be held liable for any problems arising from its operation or improper use of the issued certificates
- CNRS2 CA denies any kind of responsibilities for damages or impairments resulting from its operation.

9.9 Indemnities

No fees shall be charged.

9.10 Term and termination

9.10.1 Term

This Certificate Policy and Certification Practice Statement and respective amendments become effective as they are published on the CNRS' PKI website at http://igc.services.cnrs.fr/.

9.10.2 Termination

This CP/CPS will cease to have effect when a new version is published on the CNRS' PKI website.

9.10.3 Effect of termination and survival

All terms regarding confidentiality of personal and other data will continue to apply without restriction after termination. Also, the termination shall not affect any rights of action or remedy that may have accrued to any of the parties up to and including the date of termination.

9.11 Individual notices and communications with participants

CNRS CMG can notice by e-mail or on web pages unless specified otherwise in this CP/CPS.

9.12 Amendments

9.12.1 Procedure for amendment

No stipulation.

9.12.2 Notification mechanism and period

No stipulation.

9.12.3 Circumstances under which OID must be changed

No stipulation.

9.13 Dispute resolution provisions

Legal disputes arising from the operation of the CNRS2 CA will be resolved according to the French Law.

9.14 Governing law

No stipulation.

9.15 Compliance with applicable law

No stipulation.

9.16 Miscellaneous provisions

9.16.1 Entire agreement

No stipulation.

9.16.2 Assignment

No stipulation.

9.16.3 Severability

No stipulation.

9.16.4 Enforcement (attorneys' fees and waiver of rights)

No stipulation.

9.16.5 Force Majeure

No stipulation.

9.17 Other provisions

No stipulation.

10. Bibliography

[CERN Certification Authority Certificate Policy and Certification Practice Statement] version 2.3, November 8th 2004 http://service-grid-ca.web.cern.ch/service-grid-ca/cp_cps/cp_cps.html

[DOE Grids Certificate Policy and Certificate Practice Statement] http://www.doegrids.org/

[OpenSSL] - http://www.openssl.org/

[SiGNET CA CP/CPS] September 21st 2004 version 0.3 (draft) -

[RFC2459] - R. Housley, W. Ford, W. Polk and D. Solo, Internet X.509 Public Key Infrastructure Certificate and CRL Profile, RFC 2459, January 1999

[RFC2527] - S. Chokani and W. Ford, Internet X.509 Infrastructure Certificate Policy and Certification Practices Framework, RFC 2527, March 1999

[RFC3647] - S. Chokani, W. Ford, R. Sabett, C. Merrill, S. Wu, Internet X.509 Infrastructure Certificate Policy and Certification Practices Framework, RFC 2527, November 2003

[Global Grid Forum Certificate Policy Model] http://caops.es.net

[UK e-Science Certification Authority Certificate Policy and Certification Practice Statement] October 30th 2003

[SEE-GRID CA CP/CPS] Version 1.1, September 2004

[SwissSign Platinum CP/CPS] Version 2.1.0 Date April 28th, 2008