Certificate Policy and Certification Practice Statement

CNRS GRID2-FR

Version 1.1

2009 6th February

Document OID:

1.3.6.1.4.1.10813.1.1.8.1.1

Online:

https://igc.services.cnrs.fr/GRID2-FR

Contents

1. INTRODUCTION

1.1 Overview

This document is a draft. It is structured according to RFC2527.
It describes the set of rules used by CNRS GRID2-FR Certification Authority.

1.1.1 General definitions

Certification Authority (CA)

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

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.

Certification Practice Statement (CPS)

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

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.

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)

An entity responsible for verifying the identity of the requester and the validity of the request.

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.

DSI

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

UREC

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

CNRS Grid CA Manager Group (CNRS Grid CMG)

This committee is responsible for the management of the CNRS GRID2-FR CA.

1.2 Identification

Document title: Certificate Policy and Certification Practice Statement CNRS GRID2-FR
Version: 1.1
Date: 2009 6th February
Object Identifier of Document (OID): 1.3.6.1.4.1.10813.1.1.8.1.1

1.3 Community and Applicability

1.3.1 Certification authorities

CNRS GRID2-FR CA is a subordinate CA of the root CNRS CA (fig. 1).

- Root CNRS2 CA has a certificate signed by itself. It has 3 subordinates CAs. Its CP/CPS is available, in French, at this URL http://www.urec.cnrs.fr/securite/articles/PC.CNRS.pdf . Each subordinate CA has its certificate signed by the root CNRS CA:
- CNRS2-Standard is dedicated to issue general use certificates to people of the 1300 laboratories of CNRS (about 80 000 persons). Each laboratory has its Registration Authority.

- CNRS2-Plus is dedicated to deliver “gold" certificates for Registration Authorities.
- CNRS2-Projets has also subordinate authorities, one by project (in which CNRS is involved) who needs a Certification Authority. All subordinate authority certificate are signed by CNRS2-Projets. Each project has a limited lifetime and may include different organizations and different CP/CPS. The project manager decides which people, institutes may get a certificate. GRID2-FR CA is dedicated to GRID projects in which the CNRS is involved. This CA does not issue certificates to subordinate CA.

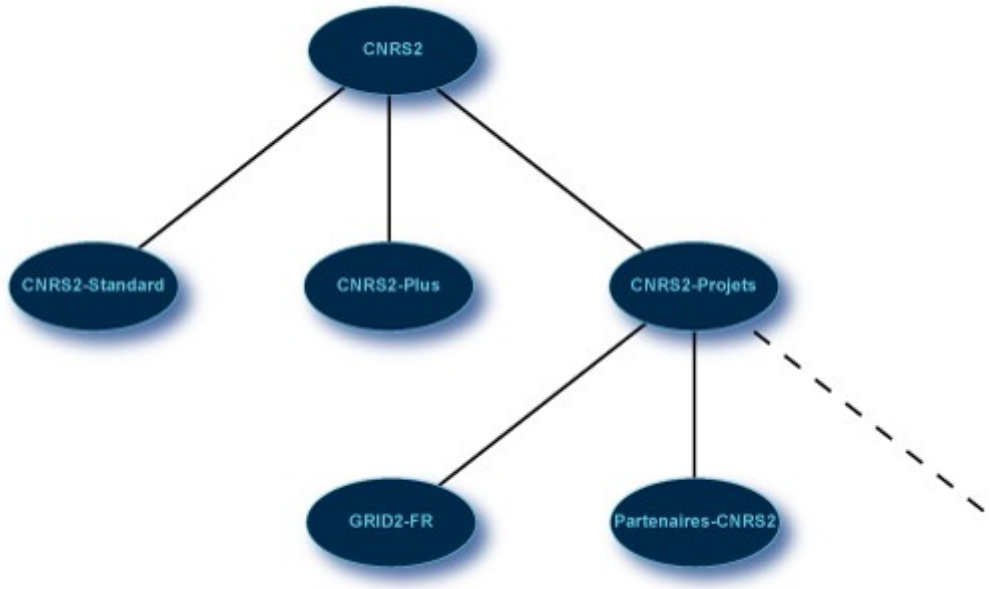

Figure 1: hierarchy of the certification authorities

1.3.2 Registration Authorities

A Registration Authority consists of one RA Manager, some RA and many RA’s Local Representative.

The RA Manager is a person of the staff of the unit CNRS/UREC. She has the responsibility to accept or reject certificate request by signing with her CNRS2-Plus certificate the certificate requests.

The RA is a person responsible to accept or reject certificate request by signing with her CNRS2-Plus certificate the certificate requests for her institute or unit. There’s RA only for big French institute or unit. This RA work is supervised by the RA Manager.

The RA’s Local Representatives are responsible for verifying requesters’ identities and the eligible requests then informs by signed email the RA Manager. RA’s Local Representatives must sign an agreement with the CNRS GRID2-FR CA, stating their adherence to the CP/CPS.

1.3.3 End entities

CNRS GRID2-FR CA issues certificate to entities which are involved in a GRID project in which CNRS is a partner. Certificates can be issued to a person (user certificate), a computer (host certificate) or a service (service certificate).
The entities that are eligible for certification by the CNRS GRID2-FR CA are :

- French entities:
  - User certificate: All users from French institutes or private companies involved in GRID project with the CNRS.
  - Host certificate: All computers, registered in the DNS database (Domain Name Service), of French institutes or private companies involved in GRID project with the CNRS. The administrator of the computer must have a user certificate.
  - Service certificate: All computers services managed by French persons, of French institutes or private companies involved in GRID project with the CNRS, and running on French computers. The administrator of the service must have a user certificate.
- Not French entities: The eligible entities for certification by the CNRS GRID2-FR CA are institutes or private companies involved with CNRS in a GRID project which have not a national GRID CA. They have to be accredited by the CNRS Grid CA Manager Group (CNRS Grid CMG). These organizations can obtain certificates for:
  - User certificate: All users of the institutes or private companies accredited by the CNRS Grid CMG.
  - Host certificate: All computers, registered in the DNS database (Domain Name Service), of institutes or private companies accredited by the CNRS Grid CMG. The administrator of the computer must have a user certificates.
  - Service certificate: All computers services managed by persons, of institutes or private companies accredited by the CNRS Grid CMG, and running on computers of institutes or private companies accredited by the CNRS Grid CMG. The administrator of the service must have a user certificate.

1.3.4 Applicability

The authorized uses of certificates issued by CNRS GRID2-FR CA are:

- E-mail signing (S/MIME)
- Authentication and encryption of communications (SSL/TLS)
- Network layer encryption (Ipsec)
- Object-signing

The certificates issue by CNRS GRID2-FR CA must not be used for financial transactions or for purpose contrary the French law.

1.4 Contact Details

1.4.1 Specification administration organization

The CNRS GRID2-FR CA is managed by the CNRS Grid CA Manager Group (CNRS Grid CMG). This committee is under the responsibility of the director of the Unité des Réseaux du CNRS (UREC/CNRS).

1.4.2 Contact person

The director of the unit UREC/CNRS:

Bernard Rapacchi, Bernard.Rapacchi@urec.cnrs.fr

For CNRS GRID2-FR CA registration and these CP/CPS:

Alice de Bignicourt, Alice.de-Bignicourt@urec.cnrs.fr

Mirvat Aljogami, Mirvat.Aljogami@urec.cnrs.fr

Gaël Beauquin, Gael.Beauquin@urec.cnrs.fr (1st backup)

Claude Gross, Claude.Gross@urec.cnrs.fr (2nd backup)

2. GENERAL PROVISIONS

2.1 Obligations

2.1.1 CA obligations

The CA must:

- accept all requests validated by the Registration Authorities
- create and delivers certificates to authenticated entities
- notify subscribers of issued certificates
- publish the issued certificates
- log all issued certificates
- accept all revocations from the Registration Authorities
- issue and publishes CRL
- notify subscribers that their personal certificate will expire

2.1.2 RA obligations

The RA:

- authenticates entity requesting certificate according to procedures outlined in this document
- must check that the information provided in the request is correct
- establishes the right of this request
- sends validated certificates requests to the CA
- creates and sends revocation requests to the CA
- follow the policies and procedures described into this document

2.1.3 Subscriber's obligations

The subscribers must:

- be involved in a GRID project in which CNRS is involved
- use their certificate only in the purpose of GRID project
- provide correct information and authorize the publication of their certificate
- accept and adhere conditions described in this document
- protect their private key and save it on an off-line medium protected by a password
- immediately notify the RA in case of key lost, compromised, or suspected to be compromised
- immediately notify the RA in case of certificated information is no longer correct
- protect and keep safe the private key of its certificate

2.1.4 Relying party obligations

Relying parties:

- must read this document
- use the certificate exclusively for the permitted usage described by this document
- notify the CNRS PKI in case of security incidents within a delay of 1 day
- verify the CRL before validating a certificate

2.1.5 Repository obligations

CNRS GRID2-FR CA will publish all information described in section 2.6.1, on its repository (http://igc.services.cnrs.fr/GRID2-FR).
CNRS GRID2-FR CA will publish as soon as issued the CRLs, the certificates issued on its repository.

2.2 Liability

The CA service is run with a reasonable level of security but is provided on a best effort basis. CNRS will take no responsibility for problems arising from its operation or for the use made of the certificates it provides.
CNRS GRID2-FR CA denies any financial or other kind of responsibility for damages or impairments resulting from its operation.

2.3 Financial responsibility

No financial responsibility is accepted.

2.4 Interpretation and Enforcement

2.4.1 Governing law

This policy is subordinate to all applicable French government laws.

2.5 Fees

No fees are charged for any service provided by CNRS GRID2-FR CA.

2.6 Publication and Repository

2.6.1 Publication of CA information

http://igc.services.cnrs.fr/GRID2-FR is a public repository which provide access to:

- The CNRS2, CNRS2-Projets and GRID2-FR CA certificates
- The CRLs of the CNRS2, CNRS2-Projets and GRID2-FR CA
- All past and current versions of the CP/CPS of the CNRS2 and GRID2-FR CAs
- User certificates issued
- The user guide explaining how end entities should request and get certificate
- Information about the RA

2.6.2 Frequency of publication

The user and server certificates are published as soon as they are issued.
The frequency of the CRL publication is described in the section 4.4.9.

New CP/CPS are published as soon as they are approved.

2.6.3 Access controls

No access controls to these publications are performed.

2.6.4 Repositories

Any information is reachable on its web site: https://igc.services.cnrs.fr/GRID2-FR

2.7 Compliance audit

No stipulation.

2.8 Confidentiality

CNRS GRID2-FR CA collects subscriber's full name, organization, unit names, and e-mail address. This information are included in the certificate and are not confidential.
CNRS GRID2-FR CA collects also subscriber's phone number but doesn't publish it nor includes it in the certificate.
CNRS GRID2-FR CA has never access to certificate private keys.

2.9 Intellectual Property Rights

CNRS asserts no copyrights on information published by the CNRS GRID2-FR CA.

3. IDENTIFICATION AND AUTHENTICATION

3.1 Initial Registration

3.1.1 Types of names

The subject name is an X500 distinguish name. Any subject under this CP/CPS starts with the "O=GRID-FR", following these forms:

- **For a personal certificate:**

- The field Country, C, equal to the country of the institute or private company of the person.
- The field Organization, O, equal to the acronym of the institute or private company of the person.
- The field Organizational Unit, OU, equal to the acronym of the unit of the person.
- The field Common Name, CN, equal to the first name (with the first letter in upper case) of the person, one blank, the last name (with the first letter in upper case) of the person. Characters accepted for the CN are US ASCII letters.

Example: O=GRID-FR, C=FR, O=CNRS, OU=UREC, CN=Sophie Nicoud

- **For a host certificate:**
  - The field Country, C, equal to the country of the institute or private company of the administrator of the machine.
  - The field Organization, O, equal to the acronym of the institute or private company of the administrator of the machine.
  - The field Organizational Unit, OU, equal to the acronym of the unit of the administrator of the machine.
  - The field Common Name, CN, equal to the canonical name of the machine. Characters accepted in the Common Name (CN) are characters accepted by the DNS (Domain Name Service).

Example: O=GRID-FR, C=FR, O=CNRS, OU=UREC, CN=marianne.in2p3.fr

- **For a service certificate :**
  - The field Country, C, equal to the country of the institute or private company of the administrator of the service.
  - The field Organization, O, equal to the acronym of the institute or private company of the administrator of the service.
  - The field Organizational Unit, OU, equal to the acronym of the unit of the administrator of the service.
  - The field Common Name, CN, equal to the full name of the service or the name of the service following slash and the canonical name of the machines. Characters accepted in the Common Name (CN) are characters accepted by the DNS (Domain Name Service).

  Example: O=GRID-FR, O=CNRS, OU=UREC, CN=Portal-GPSA

  Or

  O=GRID-FR, C=FR, O=CNRS, OU=UREC, CN=ldap/marianne.in2p3.fr

The acronym for the fields O and OU are chose by the RA in accordance with the RA's Local Representative.

3.1.2 Requirements for names to be meaningful

The subject name must have a reasonable association with the authenticated name of the subscriber. It must be uniqueness.

- For personal certificate: the CN is obtained from the real full name and email address.
- For host certificate: the CN is the host fully qualified name.
- For service certificate: the CN must related to the type of service the certificate is identifying.

3.1.3 Rules for interpreting various name forms

See section 3.1.1.

3.1.4 Uniqueness of names

The subject certificate must be unique; if case of it's not unique, the subscriber must contact the RA and resubmit a request.
Certificates must apply to unique individuals or resources. Subscribers must not share certificates. Request can be applied if, and only if no certificate already exists with the same DN or if the certificate with the same DN expire in tow months.

3.1.5 Name claim dispute resolution procedure

GRID2-FR CA will solve the name claim disputes.

3.1.6 Recognition, authentication and role of trademarks

No stipulation.

3.1.7 Method to prove possession of private key

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. Then, the key pair is stored on the requester's host. He only can get his certificate with the same browser by running a CGI script, via an URL of the CA's web portal.

For server and service certificates:

The user fills a request form on the web portal of the CA. The public and private keys are generated by the CA. Then, the certificate and the private key are sent by the web portal of the CA to the requester in a signed and encrypted email. The private key is not kept by the CA.

3.1.8 Authentication of organization identity

The RA's Local Representatives are responsible for verifying requesters' organization. Each RA's Local Representative is contacted by the RA Manager for each request coming from his unit. Each unit, of each institute, has a RA's Local Representative

3.1.9 Authentication of individual identity

These are the minimum checks run by the RA's Local Representatives and the RA Manager.

For personal certificate:

The user must met his RA's Local Representative in person, his RA's Local Representative is a person of his unit. The RA's Local Representative has to identify the requester by check the personal database of the unit or by well know personally the requester. The user must prove that he is involved in a GRID project, which the CNRS is involved.
The RA's Local Representative informs the RA Manager of the eligible of the request. Then, the RA Manager decides of the action to be take (accept or refuse the request).

For host certificate:

The RA Manager and his Local Representative have to verify that the machine is registered in the DNS database of the requester organization, and, that the field email address provided by the requester is the email of the administrator of the machine.

For service certificate:

The RA Manager and his Local Representative have to verify eligible of the request by checking the host name and the service name, and, verifying that the field email address provided by the requester is the email of the administrator of the service.

3.2 Routine Re-key

Re-keying of certificate will follow the same procedure as an initial certificate request.
For personal certificate, the user is invited, two months before his certificate expiration, to request a new certificate via the CA's web portal. His new request is signed by his personal certificate.

3.3 Re-key after Revocation

There is no re-keying after revocation. Subscribers have to follow the same procedure than an initial certificate request.

3.4 Revocation request

A revocation request must be done as soon as possible it's needed.
Person eligible to request a revocation certificate to the RA Manager are:

- The owner of the certificate
- The RA's Local Representative
- The RA.
- The RA Manager himself.

The owner of the certificate or the RA's Local Representative must contact the RA Manager by two ways:

- by e-mail, if possible signed with a valid certificate
- and by phone or by personal conversation to confirm the e-mail
- The revocation request is done by the RA manger and sent to the CA

4. OPERATIONAL REQUIREMENTS

4.1 Certificate Application

The process are different according to the subscriber is a person, a host or a service.

- For personal certificate: the request is submitted using an on-line procedure.
    1. The requester fills a form with his browser via the CA's web portal. During this step, the key pair is generated by the user browser on his machine, then, the CGI program gets the public key (the private key stays in the user browser).
    2. The e-mail address provided is verified: a program sends an acknowledgement e-mail to this email address.
    3. The requester must reply.
    4. The request must be verified and accepted the RA Manager according to the procedure describes in the section 3.1.9
    5. The user receives an e-mail informing him to get his certificate on the CA's web portal. He gets his certificate in PKCS#12 format.

- For host and service certificates: the requester must already have a personal certificate issued by the GRID2-FR CNRS CA.
    1. The requester fills a form with his browser, including his personal certificate, via the CA web portal.
    2. The request must be verified and accepted the RA Manager in according of the procedure describes in the section 3.1.9
    3. The requester receive an email signed and encrypted including the private key and the certificate.

On the CA web portal, each request is stored in a private queue and a notification e-mail is sent to the RA Manager.

4.2 Certificate Issuance

When the RA Manager receives a notification request email, he accesses to the requests' private queue using his personal CNRS2-Plus certificate via the private RA's web site.
The RA Manager verifies according to the procedure described in the sections 3.1.9 and 1.3.3 the eligible and the consistence of the request.

- If the requirements are fulfilled, the RA approves the request by signing the request with his personal CNRS2-Plus certificate.
- Else, the request is destroyed end the requester is informed.

The CA publishes the certificate on its repository.

4.3 Certificate Acceptance

No stipulation.

4.4 Certificate Suspension and Revocation

4.4.1 Circumstances for revocation

A certificate will be revoked when:

- the information it contains is no longer correct or suspected to be incorrect
- the subscriber's private key is lost or suspected to be compromise
- the subscriber doesn't need the certificate any more
- the subscribed is suspected to have violated his obligations.

4.4.2 Who can request revocation

A certificate revocation can be requested by:

- The RA, RA Manager and the RA's Local Representatives
- The holder of the certificate
- Any other entity presenting proof of knowledge of circumstance described in section 4.4.1.

4.4.3 Procedure for revocation request

The RA and RA Manager are the only person who can request a certificate revocation to the CA.
They use their CNRS2-Plus certificate to process this request via the RA's web site.
The request of certificate revocation must be done by one of these following ways:

- By sending email to his RA's Local Representative, RA or the RA Manager
- By request personally or by phone to his RA's Local Representative, RA or to the RA Manager

The RA must verifies the requester identity and the proof of his request, as described in section 4.4.1.
The revocation will occurs as soon as possible.

4.4.4 Revocation request grace period

There is no grace period. Once the revocation request sent by the RA is received by the CA, the CA processes immediately to the revocation and the publication of the new CRL.

4.4.5 Circumstances for suspension

No suspension is supported.

4.4.6 Who can request suspension

No stipulation.

4.4.7 Procedure for suspension request

No stipulation.

4.4.8 Limits on suspension period

No stipulation.

4.4.9 CRL issuance frequency

The CRLs are issued each time a certificate is revoked and at least every night with a validity period of 30 days.

4.4.10 CRL checking requirements

Before use of a certificate, a relying party must validate it against the most recently issued CRL.

4.4.11 On-line revocation/status checking availability

The web portal of the CA allows to get CRL and the current status of each certificate.

4.4.12 On-line revocation checking requirements

No stipulation.

4.4.13 Other forms of revocation advertisements available

No stipulation.

4.4.14 Checking requirements for other forms of revocation advertisements

No stipulation.

4.4.15 Special requirements re key compromise

No stipulation.

4.5 Security Audit Procedures

4.5.1 Types of event recorded

The following events are recorded:

- Certificate requests
- Certificate acceptations
- Certificate issues
- Revocation requests
- CRL issues
- Boots and shutdowns of CA machines

4.5.2 Frequency of processing log

Log files are processed at least one per month.

4.5.3 Retention period for audit log

The logs are kept as long as possible.

4.5.4 Protection of audit log

The CA operators and the RA are the only people who can view audit logs. Access to the audit log is restricted to the machines of CA operators, the RAs (IP control access). Moreover, a CNRS2-Plus certificate is mandatory.

4.5.5 Audit log backup procedures

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

4.5.6 Audit collection system (internal vs external)

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

4.5.7 Notification to event-causing subject

No stipulation.

4.5.8 Vulnerability assessments

No stipulation.

4.6 Records Archival

4.6.1 Types of event recorded

The following events are audited:

- Certificate requests
- Certificate acceptations
- Certificate issues
- Revocation requests
- CRL issues

- Boots, shutdowns and reboots of CA machines
- E-mails sent and received by CNRS-PKI software

4.6.2 Retention period for archive

The archives are kept as long as possible.

4.6.3 Protection of archive

Only the authorized staff is granted to access this information.

4.6.4 Archive backup procedures

The archive is backed up every night on an off-line medium.

4.6.5 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.

4.6.6 Archive collection system (internal or external)

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

4.6.7 Procedures to obtain and verify archive information

No Stipulation.

4.7 Key changeover

To avoid interruption of validity of subordinate keys, the new CA private key is generated one year before the expiration of the old key. The new public key is available on the one-line repository, and new certificates can be issued.

4.8 Compromise and Disaster Recovery

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

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 4.8.3.

4.8.2 Entity public key is revoked

See section 4.8.3.

4.8.3 Entity key is compromised

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

- Terminate (see section 4.8.5)
- 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

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.

If an entity's private key is compromised, its relevant RA or other person, as described in section 4.4.2, must request a revocation as described in section 4.4.3.

4.8.4 Secure facility after a natural or other type of disaster

In the case of a disaster, the CNRS CA will take whatever action it deems appropriate.

4.8.5 CA Termination

Before CNRS PKI terminates its services, it shall:

- 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 of copies of its private key

5. PHYSICAL, PROCEDURAL, AND PERSONNEL SECURITY CONTROLS

5.1 Physical Controls

5.1.1 Site location and construction

The CNRS PKI is located at the DSI/CNRS.

5.1.2 Physical access

RA and CA machines are in a controlled environment where access is restricted to authorized people.

5.1.3 Power and air conditioning

The computer center room has suitable conditioned system. And the repository machines are connected to any available building backup power.

5.1.4 Water exposures

See section 4.8.1.

5.1.5 Fire prevention and protection

See section 4.8.1.

5.1.6 Media storage

See section 4.8.1.

5.1.7 Waste disposal

See section 4.8.1.

5.1.8 Off-site backup

See section 4.8.1.

5.2 Procedural Controls

No Stipulation.

5.2.1 Trusted roles

No Stipulation.

5.2.2 Number of persons required per task

No Stipulation.

5.2.3 Identification and authentication for each rôle

No Stipulation.

5.3 Personnel Controls

All access to the servers and applications is only allowed to the granted personnel.

5.3.1 Background, qualifications, experience, and clearance requirements

The access is granted to person that is familiar with the importance of PKI, and who is technically and professionally competent.

5.3.2 Background check procedures

No Stipulation.

5.3.3 Training requirements

No Stipulation.

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 Contracting personnel requirements

No Stipulation.

5.3.8 Documentation supplied to personnel

No Stipulation.

6. TECHNICAL SECURITY CONTROLS

6.1 Key Pair Generation and Installation

6.1.1 Key pair generation

The key pair 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.

6.1.2 Private key delivery to entity

Private keys are generated as described in section 6.1.1. No private keys are 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 users

The CA certificate is available via the CA web portal: https://igc.services.cnrs.fr/GRID2-FR

6.1.5 Key sizes

By default, the key size is 1024 bits but it may be 2048 bits if the requester needs.

6.1.6 Public key parameters generation

No Stipulation.

6.1.7 Parameter quality checking

No Stipulation.

6.1.8 Hardware/software key generation

For personal certificates,Internet browsers are used to generate the key pair.
For server and service certificates, OpenSSL commands are used to generate the key pair.

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

Personal certificate's keys may be used for authentication, non repudiation, digital signature, data encryption and session key establishment.
Server and service certificate's keys may be used for authentication, non repudiation, data encryption and session key establishment.
CA certificate's keys can only used for signing certificates and CRLs.

6.2 Private Key Protection

6.2.1 Standards for cryptographic module

No Stipulation.

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

No Stipulation.

6.2.3 Private key escrow

CNRS 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 entry into cryptographic module

See section 6.2.4

6.2.7 Method of activating private key

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

6.2.8 Method of deactivating private key

No stipulation.

6.2.9 Method of destroying private key

After CA is over (see section 4.8.5) 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.

6.3 Other Aspects of Key Pair Management

6.3.1 Public key archival

See section 6.2.4

6.3.2 Usage periods for the public and private keys

The default subscriber's certificate lifetime is one year. It may be less depending of the lifetime's contract of the subscriber.
The GRID2-FR CNRS CA certificate has a lifetime of 10 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 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 ratings

No Stipulation.

6.7 Network Security Controls

The CNRS CA root machine is not connected to any kind of network. Its private key is only used to sign the subordinate CAs' certificates.
The subordinate GRID2-FR CA machines are protected behind a firewall.

6.8 Cryptographic Module Engineering Controls

No Stipulation.

7. CERTIFICATE AND CRL PROFILES

7.1 Certificate Profile

7.1.1 Version number(s)

X509v3 (0x2)

7.1.2 Certificate extensions

Extensions set in a user certificate:

- X509v3 Basic Constraints: CRITICAL CA:FALSE
- Netscape Cert Type: SSL Client, S/MIME, Object Signing
- X509v3 Key Usage: CRITICAL Digital Signature, Non Repudiation, Key Encipherment, Data Encipherment, Key Agreement
- Netscape Comment: Certificat GRID2-FR. For more information, see http://igc.services.cnrs.fr/GRID2-FR/

- X509v3 Subject Key Identifier: Keyid
- X509v3 Authority Key Identifier:

keyid:EC:3D:4B:C1:78:A9:DD:02:EC:A3:5F:14:13:C4:B8:74:86:AA:4E:6B

DirName:/C=FR/O=CNRS/CN=CNRS2-Projets

serial:03

- X509v3 Certificate Policies: Policy: 1.3.6.1.4.1.10813.1.1.8.1.1
- X509v3 Subject Alternative Name: email: canonical email of the user
- X509v3 CRL Distribution Points:

URI:http://crls.services.cnrs.fr/GRID2-FR/getder.crl

1.3.6.1.4.1.7650.1: unicoreClient

Extensions set in host and service certificates:

- X509v3 Basic Constraints: CRITICAL CA:FALSE
- Netscape Cert Type: SSL Client, SSL Server
- X509v3 Key Usage: CRITICAL Digital Signature, Non Repudiation, Key Encipherment, Data Encipherment, Key Agreement
- Netscape Comment: Certificat serveur GRID2-FR
- X509v3 Subject Key Identifier: Keyid
- X509v3 Authority Key Identifier:

keyid:EC:3D:4B:C1:78:A9:DD:02:EC:A3:5F:14:13:C4:B8:74:86:AA:4E:6B

DirName:/C=FR/O=CNRS/CN=CNRS2-Projets

serial:03

- X509v3 Certificate Policies: Policy: 1.3.6.1.4.1.10813.1.1.8.1.1
- X509v3 Subject Alternative Name: email: email of the host or service administrator
- X509v3 CRL Distribution Points:

URI:http://crls.services.cnrs.fr/GRID2-FR/getder.crl

1.3.6.1.4.1.7650.1: unicoreNJS

Extensions set in the CA certificate:

- X509v3 Basic Constraints: CRITICAL CA:TRUE
- X509v3 Subject Key Identifier: Keyid

27:96:48:27:EE:21:B6:F2:AF:B1:2D:7D:FA:F7:D7:48:25:70:95:93

- X509v3 Authority Key Identifier:

keyid:64:7C:98:3E:D1:A8:EE:BE:23:DC:07:8F:E6:67:D1:8F:9A:81:67:C0

DirName:/C=FR/O=CNRS/CN=CNRS2

serial:01

- X509v3 Key Usage: CRITICAL Certificate Sign, CRL Sign
- X509 CRL Distribution Points:

URI:http://crls.services.cnrs.fr/CNRS2-Projets/getder.crl

7.1.3 Algorithm object identifiers

No stipulation.

7.1.4 Name forms

See section 3.1.1.

7.1.5 Name constraints

See section 3.1.2.

7.1.6 Certificate policy Object Identifier

See section 1.2.

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 policy extension

No stipulation.

7.2 CRL Profile

7.2.1 Version number(s)

X509 v1 (0x0)

7.2.2 CRL and CRL entry extensions

No stipulation.

8. SPECIFICATION ADMINISTRATION

8.1 Specification change procedures

Only substantial changes in CP/CPS or changes in the technical security controls will be notified to all relevant relying parties, all cross-certifying CAs and to the public on-line repositories. It will also be announced widely available.
Users will not be informed in advance of changes to CNRS CA's CP/CPS.

8.2 8.2 Publication and notification policies

The last version of this document is available from the on-line repository of the CA:
https://igc.services.cnrs.fr/GRID2-FR/

8.3 CPS approval procedures

The CNRS Grid CA Manager Group grants any change of the CP/CPS.
For other changes, CNRS Grid CMG is responsible for the CP/CPS.

9. 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
[Global Grid Forum Certificate Policy Model] http://caops.es.net
[UK e-Science Certification Authority Certificate Policy and Certification Practice Statement] October 30th 2003