GRID-FR Personnels CA

Certificate Policy
And
Certification Practice Statement

Document OID : 1.3.6.1.4.1.20326.16140314.7180904.20.1.1

Status: Draft

Version 1.1

December 2017

Table of Content

Document Revision History

Version	Date	Comments
1.0	Sept 11, 2017	Initial Draft
	Sept 26, 2017	Initial Review
1.1	Dec 12, 2017	

1. INTRODUCTION

1.1 Overview

RENATER is the National Research and Education Network (NREN) for France that provides broadband Internet and advanced research computing services to the higher education community in France.
RENATER – hereafter called GRID-FR Service – provides a differentiated set of offers for identity certification for science and research for the purpose of cross-organizational distributed resources access, solely in the context of academic and research and similar, not-commercially competitive, applications. These services are primarily intended for the practitioners of scientific research in France, appropriately taking into account the European and global nature of research and collaboration.

This document is written in accordance with the specifications outlined by RFC3647.

This Certificate Policy and Certification Practice Statement is pertinent to the GRID-FR Personnels CA, which is a subordinate CA of the GRID-FR Root CA, and it is operated by the GRID-FR Service.
This document contains the combined Certificate Policy (CP) and Certificate Practice Statement (CPS) of the GRID-FR Personnels CA stating the applicable rules and procedures for the GRID-FR Certification Authority. GRID-FR Personnels CA is an online CA and operates in accordance with EUGridPMA guidelines for online CAs.

1.2 Document name and identification

Document title: GRID-FR Personnels CA Certification Policy and Certification Practice Statement
Version: 1.0
Date: July 2017
Object Identifier of Document: 1.3.6.1.4.1.20326.16140314.7180904.20.1.1
Where:

IANA	|	1.3.6.1.4.1
Education Nationale	|	20326
PKI	|	16140314
CP/CPS	|	7180904
CA	|	20
Major version	|	1
Minor version	|	1

1.3 PKI participants

1.3.1 Certification authorities

GRID-FR Personnels CA is an on-line Certification Authority. It is a subordinate CA of the self-signed root GRID-FR CA.
These CAs are hosted by the MEN [1] PKI and operated by RENATER (http://www.renater.fr).

[1] French National Education Minister

It ONLY issues personal certificates to the users of French entities, which are involved in activities of FRANCE-GRILLES.

1.3.2 Registration authorities

The function of Registration Authority is made of a RA Manager, RA and RA's Local Representative

- The RA Manager is a RENATER staff member of RENATER CMG. He is responsible to:
  - Manage the RAs and the RA's Local Representative
  - Perform the function of RA for sites with no designated RA, based on RA's Local Representative
- The RA is appointed by the RA Manager to handle certificate requests to a site (a laboratory, institute, unit..). He has the responsibility to accept or refuse a request according to this CP/CPS, after verifying requester identities and the eligibility of the requests. RA must sign an agreement with the GRID-FR Personnels CA, stating his adherence to the CP/CPS.
- A RA's Local Representative is designated for sites with no designated RA. RA Manager can rely on RA's local representative. The RA's Local Representatives is responsible for verifying requester identities in face-to-face and the eligible requests then informs by signed email the RA Manager. The RA's Local Representative must sign an agreement with the GRID-FR Personnels CA, stating his adherence to the CP/CPS.

1.3.3 End Entities

All users from French entities, such as educational institutions, organizations or private companies involved in activities of FRANCE-GRILLES are eligible to obtain personal certificates issued by GRID-FR Personnels CA.

1.3.4 Relying Parties

Relying parties are individuals, which use certificates of GRID-FR Personnels CA. The GRID-FR Personnels CA issued certificates must be used only for GRID and/or CLOUD operations involved in activities of FRANCE-GRILLES.
Relying parties use PKI services in relation with GRID-FR Personnels certificates and reasonably rely on such certificates and/or digital signatures verifiable with reference to a public key listed in a Subscriber's certificate.
To verify the validity of a digital certificate they receive, relying parties must refer to the Certificate Revocation List (CRL) prior to relying on information featured in a certificate to ensure that GRID-FR Personnel CA has not revoked the certificate.

1.3.5 Other participants

No stipulation

1.4 Certificate usage

1.4.1. Appropriate Certificate Usage

The authorized uses of certificates issued by GRID-FR Personnels CA are:

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

- Object-signing

1.4.2 Prohibited certificate uses

The GRID-FR Personnels CA certificates shall not be used for financial transactions or any other use or purpose contrary the French or International law.
All uses out of the scope described into the section 1.4.1 are prohibited. This means that GRID-FR Personnels CA in no way cannot be held responsible for any prohibited use.

1.5 Policy administration

1.5.1 Organization administering the document

This document is administered by the GRID-FR PMA, which is managed by RENATER and hosted by MEN PKI.

The Organization contact details are:

GIP RENATER
23-25 Rue Daviel – 75013 Paris – Tel.: +33 1 53 94 20 30
Email: grid-fr@renater.fr

Operation of the GRID-FR CA is effected by:

GIP RENATER
Université Grenoble Alpes
DGDSI
41 rue des Mathématiques
38400 Saint Martin d'Heres
Email: grid-fr@renater.fr
Web: http://grid-fr.renater.fr

The Policy Management Authority (PMA) of the GRID-FR Service shall be RENATER.

1.5.2 Contact person

The responsible Managers of the GRID-FR Service are:

Claude Gross, claude.gross@renater.fr, postal address as above

The following persons are the contacts for any remark or question about GRID-FR Personnels CA:

Mirvat Aljogami, mirvat.aljogami@renater.fr
Claude Gross, claude.gross@renater.fr
Marc Turpin, marc.turpin@renater.fr

1.5.3 Person determining CPS suitability for the policy

The persons, mentioned in section 1.5.2, are responsible for this policy and works with the EUGridPMA for the review and approval of this CP/CPS.
Changes or updates are made in accordance with the French law.

1.5.4 CPS approval procedures

Changes to the Policy and the Practice Statements are approved by the GRID-FR Service Manager, having consulted with relevant accreditation bodies and representative stakeholder bodies.
The review and approval process must assure that this CP/CPS adheres to RFC 3647.

1.5.5 Modifications of the CP/CPS

Modification of this CP/CPS may be effected at any time in accordance with the procedures specified in section 1.5.4.

1.6 Definitions and acronyms

Conventional PKI definitions apply. The following terms are specific to this document:

GRID-FR	The French National Grid Initiative
GRID-FR Service	The ensemble of services and CAs offered by the GRID-FR
GRID-FR Managers	The individual(s) responsible for the coordination of the GRID-FR policy, its interpretation, adoption, evolution, accreditation, and verification.
GRID-FR Administrators	The individuals responsible for the technical development and implementation of the GRID-FR Service and for ensuring its continued compliance with the Policy and documented Practices
GRID-FR Operators	The individuals that can issue certificate and publish updated revocation information for the specific GRID-FR CA for which they have been granted an operational privilege. For the GRID-FR CA, the only GRID-FR Operators shall be the MEN PKI Administrators, which host the PKI.
GRID-FR Root CA	The self-signed off-line root certification authority of the GRID-FR
MEN	“Ministère de l'Education Nationale” (MEN) is the French Ministry of National Education, Higher Education and Research.
MEN PKI CMG	MEN PKI CA Manager Group This committee is responsible for the management of the MEN PKI. Agents of MEN compose it.
FRANCE GRILLES	France Grilles is a scientific group of interest gathering 8 major research organizations set up in agreement with the European Commission to constitute the French National Grid Initiative. France Grilles is mandated to act on behalf of France within the European Grid Infrastructure boards. France Grilles is operated by the CNRS laboratory named "Institut des Grilles et du Cloud" and oversees the deployment of production grids and clouds at the national level in France.
RENATER	RENATER, French National Research and Education Network, federate telecommunication infrastructures for Research and Education.
RENATER CMG	RENATER CA Manager Group This committee is responsible for the management of the GRID-

	FR CA and its subordinates CAs (GRID-FR Personnels CA, GRID-FR Services CA, and GRID-FR Robots CA). Agents of RENATER compose it.
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 is the Internet system of holding a distributed register of entity names
FQDN	Fully Qualified Domain Name
IANA	Internet Assigned Numbers Authority
PKI	Public Key Infrastructure

2 PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 Repositories

GRID-FR Personnels CA shall publish its certificates, CRLs and this CP/CPS at the online repository, which is accessible at the URL http://grid-fr.renater.fr/
The documents shall be electronically signed to ensure the authenticity, and the integrity.

2.2 Publication of CA information

The GRID-FR Personnels CA shall make the following publicly available on the on-line repository:

- The GRID-FR Personnels CA's PEM, DER, CER and text format of CA certificate.
- The PEM-formatted and DER-formatted CRL.
- A copy of this CP/CPS document and the previous versions.

2.3 Time or frequency of publication

CRL will be updated immediately after revocation is issued.
GRID-FR Personnels CA CRL are issued as soon as a certificate is revoked and at least once a day for a validity time of 15 days.
CP/CPS should be verified every 2 years. Once approved, changes to this document will be published.
Previous versions will remain available on-line.

2.4 Access controls on repositories

GRID-FR Personnels CA imposes no access control restrictions to the published information including policy, certificate, issued certificates and CRL. Excluding reasonable scheduled maintenance and unforeseen failures, the online repository will be available 24/7 basis.

3 IDENTIFICATION AND AUTHENTICATION

3.1 Naming

3.1.1 Types of names

The GRID-FR Personnels CA assigns subject name in its issued certificates as non-empty X.501 distinguished names (DNs). Each assigned subject name identifies a single entity and shall never be re-assigned to any other entity.
The issuerName in the issued certificates shall be set to the name of the GRID-FR Personnels CA, which is represented as a non-empty X.501 DN.

For the GRID-FR Personnel CA the Issuer Distinguished Name is:

/C=FR/O=MENESR/OU=GRID-FR/CN=AC GRID-FR Personnels

The Subject Distinguished Names for Personal certificates consist of the following Components:

Attribute	Abbr.	Value

Organization	O	'GRID-FR'
Country	C	The two letter ISO 3166-1 country code of the relevant Subscriber
Organization	O	The name of the Subscriber
Organizational Unit	OU	The name of the organization unit of the Subscriber
Common Name	CN	A reasonable representation of the name of the Applicant
emailAddress		One on mode rfc822 email address of the Applicant

The Organization (O) and Organization Unit (OU) attributes value in the Subject Distinguished Name are obtained directly from the Subscriber or chosed with him during the registration process, and is validated by the RA Manager.

The Common Name (CN) attribute is obtained from the real full name of the applicant, and the email address should be clearly identified and associated to subscriber domain.

3.1.2 Need for names to be meaningful

The subject name of a personal certificate under this CP/CPS must have a reasonable association with the authenticated name of the subscriber. It must be uniqueness. The CN is obtained from the real full name of the subscriber.

3.1.3 Anonymity or Pseudonymity of subscribers

GRID-FR Personnels CA will neither issue nor sign pseudonymous or anonymous certificates.

3.1.4 Rules for interpreting various name forms

Names should be in ASCII encoding and should contain only alphanumeric and the dot and underscore characters in accordance with section 3.1.1 and 3.1.2

3.1.5 Uniqueness of names

The subject name in a certificate must be unambiguous and unique for each certificate issued by the GRID-FR Personnels CA. If it's not unique, the subscriber must contact the RA and resubmit a request.
A certificate is issued to a single user, if no certificate already exists with the same DN or if the certificate with the same DN expires in one month.

3.1.6 Recognition, authentication, and role of trademarks

No stipulation.

3.2 Initial identity validation

3.2.1 Method to prove possession of private key

The requester must prove possession of the private key, which corresponds to the public key in the certificate request. This is done when the subscriber fills a personal certificate request with his browser via the CA's web portal, 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 on the same host via an URL of the CA's web portal. See section 6.1.1.

3.2.2 Authentication of organization identity

The RA Manager checks that the organization is involved into activities of FRANCE-GRILLES.

The RA Manager contacts the project administrator or the training manager.
The organization can point out a member of the organization as a RA.
The RA is a permanent agent of the organization. It is highly recommended that he have knowledge in computer science.
If the organization is unable to point out a RA, it must point out a RA's local representative.
The RA's Local Representative must be a permanent agent of the organization.

3.2.3 Authentication of individual identity

The authentication of the individual identity certificate is done as follow:

- The RA or the RA's Local Representative is responsible to verify the requester identity and asking him if he has effectively put down a certificate request: The user must meet his RA or RA's Local Representative in person, his RA or RA's Local Representative is a person of the unit. The RA or the RA's Local Representative has to identify the requester by checking the unit personal database or by well-known personally the requester. The user must prove that he is involved in activities of FRANCE-GRILLES. The RA or RA's Local Representative is totally responsible for the requester's authentication and the verification of the requester's implication into activities of FRANCE-GRILLES.
- The RA, after verification, decides of the action to be taken (accept or refuse the request).
- The RA's Local Representative informs the RA Manager of the eligibility. Then, the RA Manager decides of the action to be taken (accept or refuse the request).

3.2.4 Non-verified subscriber information

No stipulation.

3.2.5 Validation of authority

See section 3.2.2 & 3.2.3
For entities with no designated RA, the RA manager sends to the RA's Local Representative a confirmation request in a signed email. The RA's Local Representative confirms or does not confirm the validity of the certificate request by answering to the RA manager in a signed email.
For entities with designated RA, the RA accepts or refuses a request according to this CP/CPS and after verifying requester identities and the eligibility of the requests.

3.2.6 Criteria for interoperation

No stipulation.

3.3 Identification and authentication of re-key requests

3.3.1 Identification and authentication for routine re-key

No re-key is available. Routine re-key shall be accomplished using the same procedures as for initial registration.

3.3.2 Identification and authentication for re-key after revocation

There is no re-keying available. Identification and authentication for re-key after revocation shall be accomplished using the same procedures as for initial registration.

3.4 Identification and authentication for revocation request

A revocation must be requested as soon as needed. The persons eligible to request a revocation are:

- A member of RENATER CMG which include RA Manager
- The RA or RA's Local Representative
- Every people who suspect that the private key of his own certificate, or any other certificate issued by the GRID-FR Personnels CA, is compromised or suspected to be compromised.

4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 Certificate Application

4.1.1 Who can submit a certificate application

All users from French entities such as educational institutions, research organizations or private companies involved in activities of FRANCE-GRILLES are eligible to submit personal certificates (user certificates) from the GRID-FR Personnels CA.

4.1.2 Enrolment process and responsibilities

To obtain a personal certificate, the subscriber submits its certificate request using an on-line procedure:

- The requester fills a form with his browser via the CA's web portal. During this step, the user's browser generates the key pair on his machine, then, the server gets the public key (the private key stays in the user browser).
- On the CA web portal, each request is stored in a private queue and notification email is sent to the RA Manager or the requester 's RA.
- When the RA Manager or the RA receives a notification request email, he accesses to the requests' private queue using his personal certificate via the private RA's web site.
- The request must be verified and accepted by the RA Manager or the requester's RA in according of the procedure describes in the section 3.2.3.
- The subscriber receives an email notify him about the issuing of his certificate.

4.2 Certificate application processing

Requesters have to prove their identity according the documents as specified by the relevant issuing CA as described in section 3.2.3

4.2.1 Performing identification and authentication functions

The RA Manager or the RA verifies according to the procedure described in the sections 3.2.3 and 1.3.3 the eligibility and the consistence of the request.

4.2.2 Approval or rejection of certificate applications

If submitting certificate requirements described in the section 4.1.1, and certificate techniques requirements are fulfilled, the certificate request is approved by the RA Manager or by the requester's RA, else the certificate request is rejected and the user is informed.

4.2.3 Time to process certificate applications
The process is performed in the best effort.

4.3 Certificate issuance

4.3.1 CA actions during certificate issuance
Here is the process:

- A Certificate Signing Request is submitted to GRID-FR Personnels CA
- The GRID-FR Personnels CA verifies the request integrity and the sign of the RA
- On successful control, then the GRID-FR Personnels CA issues the certificate and informs the requester.

4.3.2 Notification to subscriber by the CA of issuance of certificate
Requesters are notified by email containing information on how to get back the certificate.

4.4 Certificate acceptance

4.4.1 Conduct constituting certificate acceptance
No stipulation.

4.4.2 Publication of the certificate by the CA
GRID-FR Personnels CA will publish all information on its public repository, which provides access to:

- The certificates of the GRID-FR Root CA and GRID-FR Personnels CA
- The CRLs of the GRID-FR Root CA and GRID-FR Personnels CA
- All past and current versions of the CP/CPS of GRID-FR Root CA and GRID-FR Personnels CA
- The certificates issued by the CA and their status
- The user guide explaining how end entities should request and get certificate
- Information about the RA

GRID-FR Personnels CA will publish as soon as issued the CRLs and the certificates issued on its repository.

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 authorized uses of certificates issued by GRID-FR Personnels CA are:

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

The subscribers must:

- use their certificate only in the purpose of activities of FRANCE-GRILLES
- 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 Manager, his RA or his RA's Local Representative, in case of key lost, compromised, or suspected to be compromised
- immediately notify the RA manager, his RA or his RA's Local Representative, in case of certificated information is no longer correct

The certificates issued by GRID-FR Personnels CA must not be used for financial transactions or for purpose contrary the French law.

4.5.2 Relying party public key and certificate usage

Relying parties:

- must read this document
- use the certificate exclusively for the permitted usage described by this document
- verify the CRL before validating a certificate

4.6 Certificate renewal

4.6.1 Circumstance for certificate renewal

GRID-FR Personnels CA does not support certificate renewal. Re-new a certificate will follow the same procedure as an initial certificate request.

4.6.2 Who may request renewal

Not applicable

4.6.3 Processing certificate renewal requests

Not applicable

4.6.4 Notification of new certificate issuance to subscriber

Not applicable

4.6.5 Conduct constituting acceptance of a renewal certificate

Not applicable

4.6.6 Publication of the renewal certificate by the CA

Not applicable

4.6.7 Notification of certificate issuance by the CA to other entities

Not applicable

4.7 Certificate re-key

Re-keying of certificate will follow the same procedure as an initial certificate request.
Expiration warnings will be sent to subscribers:

- 1 month before expiration,
- 2 weeks before expiration,
- 1 week before expiration,
- 1 day before expiration

4.7.1 Circumstance for certificate re-key

The user is invited, one month before his certificate expiration, to request a new personal certificate via the CA's web portal. The subscriber must have a valid GRID-FR Personnels personal certificate and presents it to the GRID-FR Personnels CA web server.

4.7.2 Who may request certification of a new public key
The user requesting a new certificate is authenticated with its actual valid user certificate. If the certificate is expired or revoked, there is no re-keying possible. The user has to request a certificate as an initial request. The same requirements described in the section 4.1.1 are necessarily.

4.7.3 Processing certificate re-keying requests
Re-keying requests shall be processed following the same procedures as for a new certificate issuance.

4.7.4 Notification of new certificate issuance to subscriber
See section 4.3.2.

4.7.5 Conduct constituting acceptance of a re-keyed certificate
See section 4.3.1.

4.7.6 Publication of the re-keyed certificate by the CA
See section 4.4.2.

4.7.7 Notification of certificate issuance by the CA to other entities
No Stipulation.

4.8 Certificate modification

4.8.1 Circumstance for certificate modification
GRID-FR Personnels CA does not support certificate modification. If a valid certificate is already existing, this on is revoked, and then a subscriber requests a new certificate instead as for initial requests.

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
A certificate must be revoked as soon as possible in the following circumstances:

- The subject CA does not apply the obligations binding by virtue of this policy.

- The certificate is not required any more by the subject CA.
- The private key is lost, compromised or suspected to be compromised.
- The information in the certificate is modified, wrong or inaccurate.
- The entity to which the certificate has been issued has been retired or no longer existed.
- The subscriber doesn't comply with this policy.
- The certificate is not required any more by the entity subscriber.
- The CA ceases to function in compliance of its own policy.
- The CA changes its policy without approval of RENATER CMG.
- The CA doesn't comply with new cryptography international requirements.

4.9.2 Who can request revocation

A member of the RENATER CMG, RA, or RA's Local Representative, the certificate owner or any entity who suspects the occurrence of any of the circumstances for revocation listed in section 4.9.1 are available to request revocation.

4.9.3 Procedure for revocation request

The certificate owner can revoke himself his own certificate directly on the GRID-FR Personnels CA website using the revocation code provided during the certificate issuance. He can also request for revocation via the CA web portal, or by contacting the RA Manger, his RA, or the RA's Local Representative. In the last case, the Local Representative must contact RA Manger as soon as possible to request revocation.

Upon receipt of a revocation request, the RA Manger or the RA shall:

1. Verify the circumstances for revocation
2. Verify the identity of the revocation requester in accordance with the section 4.9.2

If all the conditions are met, RA Manager or requester's RA shall then revoke the certificate.

4.9.4 Revocation request grace period

There is no grace period in the case of revocation, if the circumstances for revocation are identifying, the revocation request is approved as soon as possible but not later than within one business day.

4.9.5 Time within which CA must process the revocation request

Once the revocation is approved, the certificate is immediately revoked and the CRL is renewed, and published.

4.9.6 Revocation checking requirement for relying parties

Relying parties must download the CRL from the online repository at least once a day and implement its restrictions while validating certificates.

4.9.7 CRL issuance frequency

The CRL of the GRID-FR Personnels CA is updated every 24 hours and is valid 15 days.

4.9.8 Maximum latency for CRLs

The maximum latency to publish CRL following its generation is 30 minutes.

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
No stipulation.

4.9.11 Other forms of revocation advertisements available
No stipulation.

4.9.12 Special requirements re-key compromise
No stipulation.

4.9.13 Circumstances for suspension
GRID-FR Personnels CA does not suspend any certificate.

4.9.14 Who can request suspension
GRID-FR Personnels CA does not suspend any certificate.

4.9.15 Procedure for suspension request
GRID-FR Personnels CA does not suspend any certificate.

4.9.16 Limits on suspension period
GRID-FR Personnels CA does not suspend any certificate.

4.10 Certificate status services

4.10.1 Operational characteristics
The 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
The subscription ends if the certificate is not re-keyed or re-newed before its expiry date or once the certificate has been revoked.

4.12 Key escrow and recovery

4.12.1 Key escrow and recovery policy and practices
No key escrow or recovery services are provided. The key owner must take all steps to prevent loss.

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 machine hosting the GRID-FR Personnels CA shall be located in a closed, secure and safe location.

5.1.2 Physical access

Physical access to the sensitive functions of the infrastructure is strictly limited to the authorized nominated staff only.
Physical access to the components supporting these functions is limited to persons authorized by the establishment of a physical security perimeter, allowing the roles separation between the various parties involved.
Access traceability is ensured, physical intrusion detection measures are implemented, particularly via the use of cameras, and physical security measures are also in place to limit access to sensitive materials.

5.1.3 Power and air conditioning

Electricity supply and air conditioning systems are implemented in order to ensure services availability. The materials used to carry out the services are operated according to conditions defined by their suppliers.

5.1.4 Water exposures

Adequate alarming is ensured. The datacenter is located in an area that has no special exposures, and the systems installations have no exposure to flooding or other liquid flows.

5.1.5 Fire prevention and protection

The datacenter is equipped with fire safety system and fire control system.

5.1.6 Media storage

All media containing the private key or copies of private key of the CA are kept in the locked safe. All other media related to the CA including the offline and online systems are kept in a safe and locked cabinet. The all are stored in a secured place.

5.1.7 Waste disposal

Waste carrying potential confidential information is physically destroyed before being trashed.

5.1.8 Off-site backup

The system generates periodically a backup of all digital information (data, code, configuration, etc.). The backup contains all information relevant for the CA service in encrypted form.
This process guarantees that the off-site storage of all data from the PKI environment is fully encrypted.
Off-site backup insure a quick PKI services recovery following a disaster or a serious event.

5.2 Procedural controls

5.2.1 Trusted roles

All persons with access to the systems hosting the GRID-FR Personnels CA will be employees of MEN who are members of the MEN PKI CMG.
Administrators of the system have a total control of the hardware, operating system, and software management. Cryptographic information, like the private key of the CA, or the CA itself, is under control of restricted personnel of MEN PKI CMG and RENTAER CMG.
All roles related to the CA operations are performed by CA Administrators who are members of RENATER CMG.

5.2.2 Number of persons required per task

Multiple roles can be assigned to the same person, if this holding does not compromise the security of the functions implemented.
All the MEN 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 persons for system administration, CA operation
- Validating certificates Signing Request : for entities with no designated RA, the GRID-FR Personnels RA Manager and the RA's Local Representative are required. The RA's Local Representative must confirm the information specified into the request, and the GRID-FR Personnels RA Manager validates it by signing. For other entities the RA is required.

5.2.3 Identification and authentication for each role

In the MEN PKI CA software, identification and authentication for all roles are performed using secure access control materials (certificates, accounts, etc.) that identify these roles and their corresponding rights.

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.
Each person involved in the CA infrastructure and PKI process is informed of its responsibilities regarding PKI services and processes related to system security and personnel control.

5.3.2 Background check procedures

Employees of the MEN manage MEN PKI. Background of each employee must not contain any criminal record.
The background of each additional RENATER CMG administrator is also assessed.

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
If an unauthorized action is observed, the CA manager may revoke the privileges concerned.

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, shut-downs and reboots of the off-line CA machines
- E-mails sent and received by MEN-PKI software

5.4.2 Frequency of processing log
Logs are processed persistently, and archived every month.

5.4.3 Retention period for audit log
Logs are kept as long as possible.

5.4.4 Protection of audit log
Different accesses are granted depending of the role:

- Full access for the GRID-FR Operators (PKI administrators)
- Privileged access for GRID-FR Service manager is also granted
- Restricted access for CA Administrators, and to the managed unit for RA Manager and 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 secure medium.

5.4.6 Audit collection system (internal vs. external)
The audit log collection system is an internal MEN system.

5.4.7 Notification to event-causing subject
No stipulation.

5.4.8 Vulnerability assessments
All the MEN PKI (meaning this CA) are monitored all the time (24x7).

5.5 Records archival

5.5.1 Types of records archived

The following events are audited:

- All certificate application data including certification and revocation
- All certificates and CRLs or certificate status records generated
- The login/logout/reboot of the issuing machine.
- The logs for all PKI component entities.

5.5.2 Retention period for archive

The CA certificate (public key) and all issued certificates will be kept for a period of 5 years after their expiry.
The logs treated in section 5.4 are archived for a period of 7 years after their generation.
All other data listed in section 5.5.1 are archived at least 10 years.

5.5.3 Protection of archive

Appropriate measures are in place to protect data from manipulation and deletion.
During all the times of their preservation, archives and backups are totally protected, accessible only to authorized persons, and its can be consulted and exploited.
Only full accesses for PKI administrators and privileged access for GRID-FR Service manager is also granted.

5.5.4 Archive backup procedures

The archives are backed up every night on an offline secure medium.

5.5.5 Requirements for time-stamping of records

The online machines are synchronized to a NTP stratum 2 time server. The offline machine is manually synchronized.

5.5.6 Archive collection system (internal or external)

The audit log collection system is an internal MEN system. See section 5.5.3

5.5.7 Procedures to obtain and verify archive information

Archive information can be requested to the MEN PKI CMG members. The contacted member provides information to the requester.

5.6 Key changeover

GRID-FR Personnels CA's private signing key is changed periodically. The overlap between the old key and the new one is for at least one year. From that time on, the newly generated signing key signs any new certificates. During that period, the old CA certificate must be valid to verify all certification chain of old and valid end entity certificates signed by its private key and also to sign CRL, until expiry of all certificates signed by it.

5.7 Compromise and disaster recovery

5.7.1 Incident and compromise handling procedures

In the event of an incident, which compromises the integrity of the GRID-FR Personnels CA, the CA personnel shall initiate an incident analysis immediately. Further steps to be undertaken will depend on the outcome of the analysis. If private key is damaged, see section 5.7.3.

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

The CA will take best effort precautions to enable recovery.
In order to be able to resume operation as fast as possible after the compute basis of the CA is corrupted, the following steps shall be performed:

1. All CA software shall be backed-up on a dedicated removable media after a new release of any of its components is installed.
2. All data files of the CA signing server shall be backed-up on a dedicated removable medium after each change, before the session is closed.

If any part of the running system is corrupted, a functioning hardware shall be loaded with the latest state of the software and data backed-up on a read-only medium and estimated to be uncorrupted. If not all encrypted copies of the GRID-FR Personnels CA private key are destroyed or lost, and are not compromised, the operation shall be re-established as soon as possible without need to revoke all issued certificates.

5.7.3 Entity private key compromise procedures

In the event of private key compromise GRID-FR Personnels CA shall immediately revoke the corresponding certificate and stop accepting certificate applications. Subscribers will also be informed of this incident. Circumstances that led to the compromise will then be fixed and eliminated. A new key and certificate for the CA will then be re-created and operations restarted with a new certificate.

5.7.4 Business continuity capabilities after a disaster

After a disaster, MEN PKI CMG shall take the appropriate decision to establish a new PKI service, recover its systems from backup and restart operations in a best effort.

5.8 CA or RA termination

Upon permanent termination of GRID-FR Personnels CA, the CA will:

1. Inform the EUGridPMA, France Grilles, and all affected entities.
2. Inform all subscribers, all relying parties, and RAs.
3. Announce termination on GRID-FR's website.
4. Terminate the issuance and distribution of certificates and CRLs.
5. Archive all relevant information in accordance with section 5.5.
6. Revoke all certificates.
7. Notify relevant security contacts.
8. Destroy all copies of its private keys.
9. Notify as widely as possible the end of the service.
10. Notify the relevant security contact.

6. TECHNICAL SECURITY CONTROLS

6.1 Key pair generation and installation

6.1.1 Key pair generation

key pairs for the GRID-FR Personnels CA are generated exclusively by RENATER CMG during the key ceremony attended by the representatives of MEN PKI CMG with the presence of neutral witnesses. The CA private key are generated and stored on an offline dedicated system (HSM), which is stored in a safe facility in accordance with section 5.1.
The key ceremony take place under the control of three people. Following their generation, the secret shares are handed over to those holders designated in advance for

this trusting role. Secrecy shares of at least two of these three persons are required for access to private keys.
For personal certificates, Internet browsers are used to generate key pair.

6.1.2 Private key delivery to subscriber
GRID-FR Personnels CA does not generate private keys and therefore does not deliver private keys since they are directly generated on a browser of the machine that the subscriber used to apply his personal certificate request via the CA web portal.

6.1.3 Public key delivery to certificate issuer
The subscriber's personal certificate public key is collected by the CA during a SSL session via the CA web portal.

6.1.4 CA public key delivery to relying parties
GRID-FR Personnels CA public keys can be downloaded from the online repository

6.1.5 Key sizes
The signing keys of GRID-FR Personnels CA used RSA encryption algorithm and a SHA-256 hashing mechanism, and the key size is at least 3072 bits.

6.1.6 Public key parameters generation and quality checking
GRID-FR Personnels CA will refuse to certify public keys not matching its quality requirements.
The end entity certificates should be issued with a key-size at minimum 2048 bits.

6.1.7 Key usage purposes (as per X.509 v3 key usage field)
GRID-FR Personnels CA keys may be used for certificate signing and for CRL signing.
Personal certificate's keys may be used for authentication, non-repudiation, digital signature, data encryption and session key establishment.

6.1.8 Hardware/software key generation
Each subscriber and responsible person should take reasonable steps to ensure that the key pair is generated with an reputable algorithms and with a sufficiently high entropy.
The CA key pair is generated on an offline HSM media using a recent and trustworthy version of the OpenSSL software package.
For personal certificates, Internet browsers are used to generate key pair. It is up to the subscriber to ensure that the key pair is generated using trustworthy software on a machine that is free from intrusions.

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
Private keys associated to personal certificates should never be shared or under multi-person control. Each user is responsible for his own private key associated to his own certificate.
The CA private key is only under the control of restricted personnel belong to RENTAER CMG and MEN PKI CMG, who are the activation data holders.

6.2.3 Private key escrow
The GRID-FR Personnels CA does not escrow any keys.

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. See section 6.2 & 3.2.1.
The CA private key is kept, in files in an encrypted form (AES, 3DES), in multiple secure offline media stored in different secure locations. The pass phrase to access the private keys is known by three people.

6.2.5 Private key archival
The CA private key is never archived beyond its active use or post the termination of the CA. It is only backed up during its validity period as per section 6.2.4.
The end entities private keys must be protected and backed up on an off-line medium by the owner.

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 dedicated medium. See section 6.1.1 and 6.2.4.

6.2.8 Method of activating private key
The CA private key is activated on an offline dedicated system by providing a pass phrase of at least 15 characters, which known by three people. The activation is performed during a key ceremony with the presence of at least two of these three persons in the activation data holder trust roles as per section 6.1.1.

6.2.9 Method of deactivating private key
No Stipulation.

6.2.10 Method of destroying private key
Following termination of CA operations, all copies of the private key will be securely destroyed according to the current best practice for the destruction of sensitive materials.

6.2.11 Cryptographic Module Rating
No Stipulation.

6.3 Other aspects of key pair management

6.3.1 Public key archival
The CA certificate (public key) and all issued certificates are archived 5 years after their expiry.
As per section 5.5.2.

6.3.2 Certificate operational periods and key pair usage periods
The GRID-FR Personnels CA's certificate shall have a validity period of no longer than 24 years.

The end-entities certificates issued by the GRID-FR Personnels CA have a lifetime no longer than 12 months, and no longer than the lifetime of the GRID-FR Personnels CA certificate itself.

6.4 Activation data

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

For CA private key, the activation data are protected from disclosure by a combination of cryptographic mechanisms and physical access control.
The pass phrase used to activate CA private key is known only by authorized staff members, so it is up to them to protect this pass phrase. A minimum of two on three members is required to access the private key. A modification into the staff implies the pass phrase to be changed.
For end entity certificate (personal certificate), the user is responsible to protect the activation data for its own private key, and should keep it confidentially.

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 with a reinforced authentication system
- The machines used to run web portal and to hold on-line repositories are behind a firewall.

6.5.2 Computer security rating

The GRID-FR Personnels CA PKI system designed according the recommendations of the CEN CWA 14167-1 document: "Security requirement for managing digital certificates trustworthy system for electronic signatures."

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 on-line protected management server is protected by sub-network specific port-filtering firewalls specific to its subnet, and additionally by system-local network access tables. Only ports that are connected to services offered on the specific system are opened, all others are closed.

6.8 Time-stamping

Time stamping of certificates will be done based on the internal system clock, which is synchronized as described in section 5.5.5.

7. CERTIFICATE, CRL, AND OCSP PROFILES

7.1 Certificate profile

7.1.1 Version number(s)

All certificates shall be formatted as X.509 version 3 certificates.

7.1.2 Certificate extensions

The CA certificate of the GRID-FR Personnels CA shall have the following extensions:

Basic Constraints	Critical, CA:True
Key Usage	Critical, Certificate Sign, CRL Sign
Subject Key Identifier	keyid:*identifier*

The certificates issued to end entity (user certificate) shall have the following extensions:

Basic Constraints	Critical, CA:False
Key Usage	Digital Signature, Non Repudiation, Key Encipherment, Data Encipherment, Key Agreement
Extended Key Usage	TLS Web Client Authentication, Email Protection
Netscape Cert Type	**NSclient, NSemail, NSobjsign**
Subject Key Identifier	*The keyID identifier of the subscribers public key*
Authority Key Identifier	keyid:*identifier*
CRL Distribution Points	URL:http://crl.grid-fr.pncn.education.gouv.fr/ac-grid-fr-personnels.crl
Certificate Policies Policy	Policy: 1.3.6.1.4.1.20326.16140314.7180904.20.1.1 Policy: 1.2.840.113612.5.2.2.1 Policy: 1.2.840.113612.5.2.3.3.3

where the *identifier* shall be composed of the 160-bit SHA-1 hash of the value of the BIT STRING containing the pertinent public key (excluding the tag, length, and number of unused bits) as per option 1 of section 4.2.1.2 of RFC 5280.

7.1.3 Algorithm object identifiers

The appropriate object identifiers shall be included in the certificates.
For GRID-FR Personnels CA, the algorithm identifier shall be sha256WithRSAEncryption (1.2.840.113549.1.1.11).

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
Each certificate musts reference a policy OID, and may contain several as long as none of the policy constraints conflict.
To be compliant with the classic Authentication Profile, the extension certificate Policies is the concatenation of the OID of this policy (the CP/CPS under which the certificate is issued) and also the base OID of the classic Authentication Profile 1.2.840.113612.5.2.2.1, and the OID of natural person entity 1.2.840.113612.5.2.3.3.3
For more information see section 7.1.2 & 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 GRID-FR Personnel CA CRL is X.509 v2 compliant with RFC5280.

7.2.2 CRL and CRL entry extensions
No stipulation.

7.3 OCSP profile
The GRID-FR Personnels CA does not operate an authoritative OCSP service.

7.3.1 Version number(s)
Not applicable.

7.3.2 OCSP extensions
Not applicable.

8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS

8.1 Frequency or circumstances of assessment
The GRID-FR Personnels CA will ensure that all its procedures and processes are carried out in compliance with the provisions of this CP/CPS. To this end, it shall at least once a year perform a self-assessment to check the compliance of the operation with the CP/CPS document in effect, and effectuate a review of staff.
The GRID-FR Personnels CA accepts to be audited by qualified external peers, by bodies to which is has been accredited, and by qualified relying parties in order to verify its compliance with the rules and procedures prescribed herein. The requesting party must cover any costs associated with such audit.

8.2 Identity/qualifications of assessor
The auditor should be an expert in the domain of assessing public key infrastructures and familiar with the requirements of the CP/CPS. He should have the necessary knowledge to do this task correctly.

8.3 Assessor's relationship to assessed entity
Auditors should be independent of the RENATER CMG.

8.4 Topics covered by assessment
Auditors will conduct the compliance audits according to the present CP/CPS as well as the EUGridPMA recommendations.

8.5 Actions taken as a result of deficiency
Depending on nature, severity, and urgency of a deficiency, RENATER CMG may decide to temporarily suspend the CA services, revoke the certificate issued by the CA, or take any other action, which it considers appropriate.
All issues will be entered into the MEN PKI system either as incidents or as problems and tracked.

8.6 Communication of results
Report of the compliance audit shall be communicated to the RENATER CMG.
Within 30 days of receiving the compliance audit results, RENATER CMG will prepare a statement regarding the open and present issues. If necessarily, a new CP/CPS will be produced

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 for access to certificate.

9.1.3 Revocation or status information access fees
No fees shall be charged for access to certificate status information or CRLs.

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
The GRID-FR Personnels CA, in its validation of individual and organizational identity, will collect personal data about subscribers. This data collection is subject to the French Personal Data Protection Act (Loi Informatique et Libertés). The subscriber acknowledges that the stated data is being collected by the CA and permits storage of any such data in the secure repository intended in section 5 according to the stipulations made therein.
Apart from the published certificates, certificate revocation lists, and the information on the online repository, the GRID-FR Personnels CA considers all data confidential.

9.3.2 Information not within the scope of confidential information
Information included in certificates and CRLs shall not be considered confidential.

9.3.3 Responsibility to protect confidential information
RENATER CMG shall not disclose confidential information unless so specified in this policy (to auditors and assessors), unless to its Managers, Administrators and Operators, and unless required by law or regulation.

9.4 Privacy of personal information

9.4.1 Privacy plan
GRID-FR Personnels CA maintains a minimum of personal data just to ensure that the same identity is not reassigned to a different entity and treats these data in accordance with French Law.
GRID-FR Personnels CA collects subscriber's information such as

- full name
- organization name, and unit name (if exist)
- email address

Data owners can request access to information regarding all their data at any time, and all reasonable requests to correct and/or amend the data will be processed promptly. Due to the nature of the service, it has a legitimate interest in recording the information recorded as per section 3.2.3 for as long as the certificate is valid plus the audit log retention period.

9.4.2 Information treated as private
Any information not explicitly made public is treated as private information. The CA protects private information using appropriate safeguards and an appropriate degree of care.

9.4.3 Information not deemed private
The following information collected by the GRID-FR Personnels CA is deemed not to be private:

1. Subscriber's full name
2. Subscriber's organization email address
3. Subscriber's organization name, and unit name (if exist).
4. Subscriber's certificate

9.4.4 Responsibility to protect private information

RENATER CMG including RA Manager and RAs are responsible to protect private information from compromise and prevent from using it or disclosing it to third parties.

9.4.5 Notice and consent to use private information

RENATER 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

RENATER CMG may be forced to disclose confidential information to law enforcement agencies in France or in Europe.

9.4.7 Other information disclosure circumstances

No stipulation.

9.5 Intellectual property rights

This document is formatted according to RFC [RFC3647] - S. Chokani, W. Ford, R. Sabett, C. Merrill, S. Wu (2003).
No intellectual property rights are claimed on issued certificates or certificate revocation lists.
Parts of this document have been copied from the CP/CPS documents of other EUGridPMA members mainly:

1. DutchGrid Root CP/CPS
2. KENET ROOT CA CP/CPS

9.6 Representations and warranties

9.6.1 CA representations and warranties

Except as stated in this CP/CPS or in a separate agreement with RENATER and the MEN, neither RENATER, nor any of the RENATER parties, nor the MEN, nor any MEN PKI Managers, Administrators or Operators makes any representations regarding its services.
The GRID-FR Personnels CA represents to the extent specified in this CP/CPS that it:

- complies with this CP/CPS;
- the certificates issued by the GRID-FR Personnels CA will be issued solely in compliance with this CP/CPS;
- it will maintain an on-line accessible repository containing the published information with an intended continuous availability.

9.6.2 RA representations and warranties

The RENATER CMG and all the RAs will act in accordance with the provisions in this CP/CPS.

9.6.3 Subscriber representations and warranties
Subscribers represent and warrant that certificates are only used for purposes compatible with section 1.4.

9.6.4 Relying party representations and warranties
Each relying party represents that, before relying on any certificate of the GRID-FR Personnels CA, it shall have read, understood, and act in compliance with this CP/CPS, that it has appropriate knowledge of PKI and appropriate technical implementations to validate certificates issued by the GRID-FR Personnels CA, and that it shall have obtained the up-to-date certificate status information as published by the GRID-FR Personnels CA and act in accordance therewith.
Each relying party shall represent that it bears the sole responsibility for reliance on any certificate issued by the GRID-FR Personnels CA, any such reliance is at its own risk, and that it has thereto executed an appropriate risk assessment.
Relying parties shall notify the RENATER CMG in case of security incidents within a delay of 1 day, and verify the CRL before validating a certificate.

9.6.5 Representations and warranties of other participants
No stipulations.

9.7 Disclaimers of warranties
All certificates and any related materials, software, publications, and service are provided 'as-is' and 'as available', without any warranties. To the maximum extent permitted by law, the GRID-FR Service, RENATER, RENATER partners, RENATER personnel, MEN, and all others involved in the GRID-FR Service disclaim all express and implies warranties and liabilities, including all warranties of merchantability, fitness for a particular purpose, and non-infringement. Neither the GRID-FR Service, RENATER, RENATER partners, RENATER personnel, MEN, not any others involved in the GRID-FR Service warrant that any service, product, certificate or other artifact will meet any expectations or that access to certificates will be timely or error-free, or that it is available at any time. The GRID-FR Personnels CA may discontinue any service at any time following the provisions of section 5.8.

9.8 Limitations of liability
The GRID-FR Service, RENATER, RENATER partners, RENATER personnel, MEN, and all others involved in the GRID-FR Service decline any liability for damages incurred by any subscriber, relying party, or third party relying on the certificates or information issued or published by the GRID-FR Personnels CA or GRID-FR Service. 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 GRID-FR Personnels CA.

9.9 Indemnities
No fees shall be charged.

9.10 Term and termination

9.10.1 Term
This CP/CPS and any amendments are effective when published in the on-line repository as per the date there stated, and will remain in effect until replaced with a newer version or withdrawn.

9.10.2 Termination
This CP/CPS will remain in effect until replaced with a newer version or withdrawn.

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
Individuals can communicate with the GRID-FR Personnels CA using the information provided in section 1.5.2.

9.12 Amendments

9.12.1 Procedure for amendment
This CP/CPS is reviewed annually at the time of the self-audit. Posting an updated version of the CP/CPS to the on-line repository makes amendments.
Corrections of spelling mistakes or typing errors, which do not alter the meaning of the CP/CPS, are authorized without notifications.

9.12.2 Notification mechanism and period
The RENATER CMG will post changes to this CP/CPS in its on-line repository. It will inform any bodies to which it has been accredited and that request prior notification for changes to the CP/CPS in a timely fashion in accordance with the provisions of section 1.5.5 before the new CP/CPS becomes effective.

9.12.3 Circumstances under which OID must be changed
The significant changes to the CP/CPS to be determined by the RENATER CMG will require the modification of the OID described in section 1.2 and affirmed in section 7.1.6.

9.13 Dispute resolution provisions
Legal disputes arising from the operation of the MEN PKI will be resolved according to the French Law.

9.14 Governing law
The interpretation, construction, and validity of this policy shall be governed by the French laws.

9.15 Compliance with applicable law
This CP/CPS is subject to all applicable laws and regulations.

9.16 Miscellaneous provisions

9.16.1 Entire agreement
This CP/CPS constitutes the entire agreement between the RENATER CMG and the GRID-FR Personnels CA and any other party, unless a more specific agreement is in place. If such an agreement has provisions that differ from this CPS, the more specific agreement takes precedence, but only with respect to that party. No others may rely on such a more specific agreement, or bring action to enforce such agreement.

9.16.2 Assignment
Any entities operating under this CP/CPS may not re-assign their rights or obligations without consent of the RENATER CMG. RENATER CMG has the right to assign and delegate its operation under this CP/CPS to any entities of its choice.

9.16.3 Severability
The remainder of the CP/CPS provision remains valid and applicable even if there is a provision deemed invalid and not applicable.

9.16.4 Enforcement (attorneys' fees and waiver of rights)
The requirements defined in the CP/CPS must be applied without any possible wavier of rights exemption.

9.16.5 Force Majeure
The GRID-FR Personnels CA cannot be held liable for any indirect damage and interruption of its services, which is caused by an occurrence beyond the RENATER CMG or MEN PKI CMG's reasonable control.

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

[INFN CA CP/CPS] Version 2.3.1 February, 28 2008