

Certificate Policy and Certification Practice Statement CNRS/CNRS-Projets/Datagrid-fr

Version 0.3 August 2002

Online : <http://www.urec.cnrs.fr/igc/Doc/Datagrid-fr.policy.pdf>

Old versions

Version 0.2 : <http://www.urec.cnrs.fr/igc/Doc/Datagrid-fr.policy.02.pdf>

Version 0.1 : <http://www.urec.cnrs.fr/igc/Doc/Datagrid-fr.policy.01.pdf>

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/CNRS-Projets/Datagrid-fr certification authority.

1.2 Identification

Document name : Certificate Policy and Certification Practice Statement CNRS/CNRS-Projets/Datagrid-fr

Version : 0.1 (draft)

Date : 05/21/2001

1.3 Community and Applicability

1.3.1 Certification authorities

CNRS/CNRS-Projets/Datagrid-fr CA is a branch of the CNRS CAs tree (described in the french document : <http://www.urec.cnrs.fr/securite/articles/PC.CNRS.pdf>).

CNRS CA is the root certification authority. This CA certificate his signed by itseft. It has 3 sub-authorities. Each one has a certificate signed by CNRS CA :

- CNRS-Standard to deliver general use certificates to people in the 1300 laboratories of CNRS. Every laboratory will have his registration authority (by default the director).
- CNRS-Plus to deliver "gold" certificates for administrative use.
- CNRS-Projets : this authority has also sub-authorities, one by project (in which CNRS is involved) who needs a certification authority. Each project has a limited lifetime and may include different organisations. The project manager decides which people may have a certificate.

Datagrid-fr his a sub-authority of CNRS-Projets. The Datagrid-fr certificate is signed by CNRS-Projets.

CNRS, CNRS-Standard, CNRS-Plus, CNRS-Projets CA are managed by CNRS/UREC (<http://www.urec.cnrs.fr>).

1.3.2 Registration authorities

The registration authority of Datagrid-fr is Sophie Nicoud who works with François Etienne in WP6. The registration authority has a CNRS-Plus certificate used to accept, reject, ... certificate requests.

1.3.3 End entités

Datagrid-fr may issue certificates to every people or server involved in the Datagrid project. François Etienne decides if the requestor may or may not have a Datagrid-fr certificate.

1.3.4 Applicability

The person certificates may be used for user authentication and data integrity in various applications : globus or similar grid software, electronic mail, Web server access, ...

The server certificates may be used for server authentication and communication encryption.

1.3 Contact Details

For this document and the CNRS authorities policy and procedures :

Jean-Luc Archimbaud CNRS/UREC Jean-Luc.Archimbaud@urec.cnrs.fr

For Datagrid-fr registration and issuing policy :

Sophie Nicoud CNRS/UREC Sophie.Nicoud@urec.cnrs.fr

François Etienne CPPM François.Etienne@in2p3.fr

2. GENERAL PROVISIONS

2.1 Obligations

2.1.1 CA obligations

The Datagrid-fr CA :

- accepts all requests validated by the registration authority
- creates and delivers certificates to users
- publishes the issued certificates
- accepts all revocations from the registration authority
- issues and publishes a CRL

2.1.2 RA obligations

The Datagrid-fr RA :

- authenticates the person requesting a person certificate
- determines if the person has the right to have a Datagrid-fr person certificate
- sends validated person certificates requests to the CA
- sends validated server certificates requests to the CA
- creates and sends revocation requests to the CA

2.1.3 Subscriber obligations

Subscribers :

- must be involved in the Datagrid project
- must protect their private key and save it

- must immediately notify the Datagrid-fr RA in case of key lost or compromised.

2.1.4 Relying party obligations

Relying party :

- must use the certificate for the permitted usage only
- verify the CRL before validating a certificate

2.1.5 Repository obligations

CNRS/UREC publishes as soon as issued the Datagrid-fr CRL, the user certificates and the server certificates on a Web server.

2.2 Liability

The certification 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 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

2.5 Fees

No fees are charged.

2.6 Publication and Repository

2.6.1 Publication of CA information

<http://igc.services.cnrs.fr/Datagrid-fr/> is a public Web page which permits

- To list and load the CNRS, CNRS-Projets and Datagrid-fr CA certificates and CRLs
- To find and load user and server issued certificates
- To get various informations

2.6.2 Frequency of publication

The user and server certificates are published as soon as they are generated.

The CRL is published every day. It has a one month validity time.

2.6.3 Access controls

No access controls to these publications are performed.

2.6.4 Repositories

<http://igc.services.cnrs.fr/Datagrid-fr/>

2.7 Compliance audit

No stipulation

2.8 Confidentiality

CNRS CAs collect subscribers fullname, organisation and unit names, electronic address. These informations are included in the certificate. These informations are not confidential.

CNRS CAs have never access to users or servers private keys. These keys are generated on the users stations and stay there.

3. IDENTIFICATION AND AUTHENTICATION

3.1 Initial Registration

3.1.1 Types of names

Person DN :

C = Country, O = Organisation, OU = Unit, CN = First name Last name /Email = email

Server name DN :

C = Country, O = Organisation, OU = Unit, CN = DNS server name/Email = email
server administrator

3.1.2 Need for names to be meaningful

3.1.3 Rules for interpreting various name forms

3.1.4 Uniqueness of names

3.1.5 Name claim dispute resolution procedure

3.1.6 Recognition, authentication and role of trademarks

3.1.7 Method to prove possession of private key

Person certificate : the public and private keys are generated on the user station when he fills the certificate request form with Netscape or Internet Explorer browser.

Server certificate : the private key and the certificate are sent to the requestor in a encrypted mail.

3.1.8 Authentication of organization identity

The registration authority verifies the organisation identity as member of a recognized organization by the CNRS.

3.1.9 Authentication of individual identity

The registration authority cross-check the person identity with reliable and secure informations coming from official administrative managers recognized by the CNRS.

3.2 Routine Rekey

This will be done by an online procedure with the old certificate check.

3.3 Rekey after Revocation

Same rules than the initial registration.

3.4 Revocation request

Revocation request must be sent by the user in a signed electronic mail if possible. If not, the user must contact the registration authority who verifies the requester identity with similar procedures used in the initial registration..

4. OPERATIONAL REQUIREMENTS

4.1 Certificate Application

Person certificate : the request is submitted using an online procedure. The requestor fills a form with Netscape or Internet Explorer browser. During this step, the 2 keys are generated in the user browser and the CGI program gets the public key (the private key stays on the user station). After this step, to verify the person electronic address, a program sends an email to the person. This one must reply.

Server certificate : the requestor must already have a person certificate. The request is submitted with a similar procedure without the 2 keys generation on the user browser.

Each request is stored in a private queue and a mail is sent to the registration authority.

4.2 Certificate Issuance

When the registration authority receives a request notification mail, he accesses the requests private queue using his CNRS-Plus certificate.

He verifies all the requestor form informations in a way described in 3.1.9 paragraph. If everything is correct, the request is accepted and sent to the Certification Authority (if not, a "negative" mail is sent to the requestor).

If the certificate is a person certificate, the Certification Authority creates the certificate, stores it on a public Web page, and sends an electronic mail to the requestor with the instructions on how to download his certificate.

If the certificate is a server certificate the Certification Authority generates the 2 keys and the certificate using openssl. These informations are then sent to the requestor in an email signed and encrypted with the public key of the requestor.

The Certification Authority publishes the certificate.

4.3 Certificate Acceptance

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) or when the private key is lost (or suspected to be compromised).

4.4.2 Who can request revocation

The certificate holder or any other entity presenting proof of knowledge of the private key compromise or of the subscriber's data variation can request a certificate revocation.

4.4.3 Procedure for revocation request

The registration authority is the only person who can request a certificate revocation. He uses his CNRS-Plus certificate to process this request which is sent to the certificate authority.

Revocation request must be sent by the user to the registration authority in a signed electronic mail if possible. If not, the user must contact the registration authority by another method. The registration authority verifies the requester identity with the same procedures used in the initial registration.

4.4.4 Revocation request grace period

4.4.5 Circumstances for suspension

4.4.6 Who can request suspension

4.4.7 Procedure for suspension request

4.4.8 Limits on suspension period

4.4.9 CRL issuance frequency (if applicable)

The CRL is created every night. Its lifetime is one month.

4.4.10 CRL checking requirements

4.4.11 On-line revocation/status checking availability

The public page <http://igc.services.cnrs.fr/Datagrid-fr/recherche.html> permits to get the CRL and the current status of each datagrid certificate

4.4.12 On-line revocation checking requirements

4.4.13 Other forms of revocation advertisements available

4.4.14 Checking requirements for other forms of revocation advertisements

4.4.15 Special requirements re key compromise

4.5 Security Audit Procedures

4.5.1 Types of event recorded

The following events are recorded :

- Certificate requests (by persons)
- Certificate acceptations (by RA)
- Revocation requests (by RA)

- Certificate issues
- CRL issues

4.5.2 Frequency of processing log

4.5.3 Retention period for audit log

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 and of the RA (IP control access) and a CNRS-Plus certificate is mandatory.

4.5.5 Audit log backup procedures

The audit log is back up every night.

4.5.6 Audit collection system (internal vs external)

The collection system is an internal UREC system.

4.5.7 Notification to event-causing subject

4.5.8 Vulnerability assessments

4.6 Records Archival

4.6.1 Types of event recorded

The following events are audited :

- Certificate requests (by persons)
- Certificate acceptations (by RA)
- Revocation requests (by RA)
- Certificate issues
- CRL issues

4.6.2 Retention period for archive

4.6.3 Protection of archive

4.6.4 Archive backup procedures

4.6.5 Requirements for time-stamping of records

4.6.6 Archive collection system (internal or external)

4.6.7 Procedures to obtain and verify archive information

4.7 Key changeover

4.8 Compromise and Disaster Recovery

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

4.8.2 Entity public key is revoked

4.8.3 Entity key is compromised

4.8.4 Secure facility after a natural or other type of disaster

4.9 CA Termination

5. PHYSICAL, PROCEDURAL, AND PERSONNEL SECURITY CONTROLS

5.1 Physical Controls

5.1.1 Site location and construction

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

5.1.4 Water exposures

5.1.5 Fire prevention and protection

5.1.6 Media storage

5.1.7 Waste disposal

5.1.8 Off-site backup

5.2 Procedural Controls

5.2.1 Trusted roles

5.2.2 Number of persons required per task

5.2.3 Identification and authentication for each role

5.3 Personnel Controls

5.3.1 Background, qualifications, experience, and clearance requirements

5.3.2 Background check procedures

5.3.3 Training requirements

5.3.4 Retraining frequency and requirements

5.3.5 Job rotation frequency and sequence

5.3.6 Sanctions for unauthorized actions

5.3.7 Contracting personnel requirements

5.3.8 Documentation supplied to personnel

6. TECHNICAL SECURITY CONTROLS

6.1 Key Pair Generation and Installation

6.1.1 Key pair generation

The user (or server) key pair is generated on the user station when he fills the certificate request form with a Netscape or Internet Explorer browser. The CA picks up the public key. The private key stays on the user station.

6.1.2 Private key delivery to entity

6.1.3 Public key delivery to certificate issuer

User or server public key is picked up by the CA during a SSL session.

6.1.4 CA public key delivery to users

The CA certificate (which includes the CA public key) is delivered by a connection to a secure web server : <http://igc.services.cnrs.fr/Datagrid-fr/recherche.html>

6.1.5 Key sizes

By default the key size is 1024 bits, it may be 512 (Netscape ou IE old releases) or 2024 bits. We recommand at least 1024 bits.

6.1.6 Public key parameters generation

6.1.7 Parameter quality checking

6.1.8 Hardware/software key generation

Netscape ou Internet Explorer key generation software are used.

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

Key usages are : Digital Signature, Non Repudiation, Key Encipherment.

6.2 Private Key Protection

The users or servers private keys must be protected and backed up by the users.

Datagrid-fr CA private key is kept, encrypted, in multiple CD-Rom copies stored in different locations. The passphrase to access the private key is known by 4 people.

6.2.1 Standards for cryptographic module

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

6.2.3 Private key escrow

6.2.4 Private key backup

6.2.5 Private key archival

6.2.6 Private key entry into cryptographic module

6.2.7 Method of activating private key

6.2.8 Method of deactivating private key

6.2.9 Method of destroying private key

6.3 Other Aspects of Key Pair Management

6.3.1 Public key archival

6.3.2 Usage periods for the public and private keys

The default user or server certificate lifetime is one year. It may be less.
The Datagrid-fr CA certificate has a lifetime of 10 years.

6.4 Activation Data

6.4.1 Activation data generation and installation

6.4.2 Activation data protection

6.4.3 Other aspects of activation data

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 (all recommended patches are installed)
- The network services are reduced to the minimum
- The servers access is restricted to a few stations
- They are protected by a firewall

6.5.2 Computer security rating

6.6 Life Cycle Technical Controls

6.6.1 System development controls

6.6.2 Security management controls

6.6.3 Life cycle security ratings

6.7 Network Security Controls

6.8 Cryptographic Module Engineering Controls

7. CERTIFICATE AND CRL PROFILES

7.1 Certificate Profile

- A user certificate example :

Version: 3 (0x2)

Serial Number: 72 (0x48)

Signature Algorithm: md5WithRSAEncryption

Issuer: C=FR, O=CNRS, CN=Datagrid-fr

Validity

Not Before: Aug 22 16:41:02 2001 GMT

Not After : Aug 22 16:41:02 2002 GMT

Subject: C=FR, O=CNRS, OU=LAPP,

CN=Dominique Boutigny/Email=boutigny@in2p3.fr

Subject Public Key Info:

Public Key Algorithm: rsaEncryption

RSA Public Key: (1024 bit)

Modulus (1024 bit):

Exponent: 65537 (0x10001)

X509v3 extensions:

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

Netscape Comment:

Certificat Datagrid-fr. Pour toute information se reporter

<http://igc.services.cnrs.fr/Datagrid-fr/>

X509v3 Subject Key Identifier: ...

X509v3 Authority Key Identifier:

keyid: ...

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

serial:02

X509v3 Subject Alternative Name:
email:boutigny@in2p3.fr
X509v3 Issuer Alternative Name:
URI:http://igc.services.cnrs.fr/Datagrid-fr
X509v3 CRL Distribution Points:
URI:http://igc.services.cnrs.fr/cgi-bin/load.crl/CA=Datagrid-fr
Netscape CA Policy Url: http://igc.services.cnrs.fr/Datagrid-fr/CPS/
Signature Algorithm: md5WithRSAEncryption :...

o A server certificate example :

Version: 3 (0x2)
Serial Number: 67 (0x43)
Signature Algorithm: md5WithRSAEncryption
Issuer: C=FR, O=CNRS, CN=Datagrid-fr
Validity
Not Before: Aug 6 12:12:16 2001 GMT
Not After : Aug 6 12:12:16 2003 GMT
Subject: C=FR, O=CNRS, OU=LPC,
CN=biolpc03.in2p3.fr/Email=legre@clermont.in2p3.fr
Subject Public Key Info:
Public Key Algorithm: rsaEncryption
RSA Public Key: (1024 bit) : ...
X509v3 extensions:
X509v3 Basic Constraints: critical
CA:FALSE
Netscape Cert Type:
SSL Server
X509v3 Key Usage: critical
Digital Signature, Non Repudiation, Key Encipherment
Netscape Comment:
Certificat serveur Datagrid-fr
X509v3 Subject Key Identifier: ...
X509v3 Authority Key Identifier:
keyid: ...
DirName:/C=FR/O=CNRS/CN=CNRS-Projets
serial:02
X509v3 Issuer Alternative Name:
URI:http://igc.services.cnrs.fr/Datagrid-fr
X509v3 CRL Distribution Points:
URI:http://igc.services.cnrs.fr/cgi-bin/load.crl/CA=Datagrid-fr
Netscape CA Policy Url:
http://igc.services.cnrs.fr/Datagrid-fr/CPS/
Signature Algorithm: md5WithRSAEncryption : ...

7.1.1 Version number(s)

7.1.2 Certificate extensions

7.1.3 Algorithm object identifiers

7.1.4 Name forms

7.1.5 Name constraints

7.1.6 Certificate policy Object Identifier

7.1.7 Usage of Policy Constraints extension

7.1.8 Policy qualifiers syntax and semantics

7.1.9 Processing semantics for the critical certificate policy extension

7.2 CRL Profile

- A Datagrid-fr CRL example :

Version 1 (0x0)
Signature Algorithm: md5WithRSAEncryption
Issuer: /C=FR/O=CNRS/CN=Datagrid-fr
Last Update: May 28 22:14:42 2001 GMT
Next Update: Jun 27 22:14:42 2001 GMT
Revoked Certificates:
Serial Number: 02
Revocation Date: May 15 06:48:31 2001 GMT
Signature Algorithm: md5WithRSAEncryption
.....

7.2.1 Version number(s)

7.2.2 CRL and CRL entry extensions

8. SPECIFICATION ADMINISTRATION

8.1 Specification change procedures

8.2 Publication and notification policies

The last version of this document is available at :
<http://www.urec.cnrs.fr/securite/articles/Datagrid-fr.policy.pdf>

8.3 CPS approval procedures