NorduGrid CA
Certificate Policy and
Certification Practice Statement

Version 0.1

Contents

1 Introduction

1.1 Overview

This document – structured according to RFC2527 [3] – describes the set of rules and procedures followed by the NorduGrid CA.

1.2 Identification

Document title: NorduGrid Certificate Policy and Certification Practice Statement

Document version: 0.1

Document date: December 2004

Object Identifier assigned: 1.3.6.1.4.1.11604.1.1.1.1

1.3 Community and Applicability

1.3.1 Certification authorities

The NorduGrid CA does not issue certificates for subordinate Certification Authorities.

1.3.2 Registration authorities

The NorduGrid CA delegates identification and authorization of certificate subjects to trusted individuals (Registration Authorities).

1.3.3 End entities

The NorduGrid CA issues certificates for entities affiliated to academia in the Nordic Countries: Denmark, Norway, Sweden and Finland.

1.3.4 Applicability

The certificates may be used for any application that is suitable for X.509 certificates.

1.4 Contact Details

1.4.1 Specification administration organization

The NorduGrid CA is administered by the Niels Bohr Institute as part of the NorduGrid collaboration activities by Anders Wäänänen.

1.4.2 Contact person

The primary contact for this CP/CPS is:

Anders Wäänänen
The Niels Bohr Institute
Blegdamsvej 17 DK-2100 Copenhagen Ø
Denmark
Phone: +45 35325301
Fax: +45 35325016
Email: ca@nbi.dk

1.4.3 Person determining CPS suitability for the policy

Not applicable.

2 General Provisions

2.1 Obligations

2.1.1 CA obligations

The NorduGrid CA will operate a certification authority service in accordance with all provisions of this CP and associated CPS. It's obligations include:

- issue certificates based on the requests from entitled subscribers, validated by an appointed Registration Authority
- notify the subscriber of the issuing of the certificate
- accept revocation requests according to the procedures outlined in this document
- authenticate entities requesting the revocation of a certificate
- issue and publish Certificate Revocation Lists (CRLs)

2.1.2 RA obligations

The NorduGrid CA delegates the tasks of identification and authorization of certificate subjects to Registration Authorities. Their obligations include:

- authenticate entity which makes the certification request, according to the procedures outlined in this document
- verify that the information provided in the certificate request is correct and that the requester has the characteristics specified in Section 1.3.3
- accept revocation requests, according to the procedures outlined in this document
- notify the NorduGrid CA of all revocation requests
- provide information to the subscriber on how to properly maintain a certificate and the corresponding private key.

2.1.3 Subscriber obligations

Subscribers must:

- read and adhere to the procedures published in this document;
- generate a key pair using a trustworthy method;
- take reasonable precautions to prevent any loss, disclosure or unauthorized use of the private key associated with the certificate, including selecting a suitable passphrase and protecting it from others;
- notify immediately the NorduGrid CA in case of loss or compromise of the private key.

2.1.4 Relying party obligations

Relaying parties must:

- understand and accept this CP and associated CPS;
- verify the CRL before validating a certificate;
- use the certificates for the permitted purposes only.

2.1.5 Repository obligations

The NorduGrid CA will make the Certificate Revocation List available from the NorduGrid web site: http://www.nordugrid.org/ as soon as it is issued.

2.2 Liability

The NorduGrid CA only guarantees issue and revoke certificates according to the practices described in this document. No other liability, implicit or explicit, is accepted. In particular the NorduGrid CA:

- will not give any guarantees about the security or suitability of the service: the certification service is run with a reasonable level of security, but it is provided on a best effort only basis;
- doesn't warrant its procedures and will take no responsibility for problems arising from its operation, or for the use made of the certificates it provides;
- denies any financial or any other kind of responsibilities for damages or impairments resulting from its operation.

2.2.1 CA liability

See section 2.2

2.2.2 RA liability

See section 2.2

2.3 Financial responsibility

The NorduGrid CA assumes no financial responsibility with respect to use or management of any issued certificate.

2.3.1 Indemnification by relying parties

No stipulation.

2.3.2 Fiduciary relationships

No stipulation.

2.3.3 Administrative processes

Administrative processes pertaining to this CP/CPS shall be determined by the CA.

2.4 Interpretation and Enforcement

2.4.1 Governing law

Interpretation of this CP and CPS is according to Danish laws.

2.4.2 Severability, survival, merger, notice

Should it be determined that one section of this document is incorrect or invalid, its other sections shall remain in effect until the document is amended.

2.4.3 Dispute resolution procedures

The PMA shall resolve any disputes associated with the use of the certificates issued by this CA.

2.5 Fees

No fees are charged.

2.5.1 Certificate issuance or renewal fees

No stipulation.

2.5.2 Certificate access fees

No stipulation.

2.5.3 Revocation or status information access fees

No stipulation.

2.5.4 Fees for other services such as policy information

No stipulation.

2.5.5 Refund policy

No stipulation.

2.6 Publication and Repository

2.6.1 Publication of CA information

Information about NorduGrid CA and how to request certificates is available via the NorduGrid web site. Also available is:

- NorduGrid CA certificate
- Certificate Revocation List
- a copy of this policy
- other relevant information

The CA does not publish any information about issued certificates.

2.6.2 Frequency of publication

The Certificate Revocation List is usually published as soon as it is issued. Issuing is usually done along with signing certificates and at least every month.

2.6.3 Access controls

The NorduGrid CA web site has read access for everybody.

2.6.4 Repositories

2.7 Compliance audit

No external audit will be accepted, only a self-assessment by the NorduGrid CA that its operation is according to this Policy.

2.7.1 Frequency of entity compliance audit

No stipulation.

2.7.2 Identity/qualifications of auditor

No stipulation.

2.7.3 Auditor's relationship to audited party

No stipulation.

2.7.4 Topics covered by audit

No stipulation.

2.7.5 Actions taken as a result of deficiency

No stipulation.

2.7.6 Communication of results

No stipulation.

2.8 Confidentiality

The NorduGrid CA collects subscribers' full name, organization and e-mail address. This information is included in the issued certificates. No other subscribers' information is collected.

Under no circumstances will the NorduGrid CA have access to the private keys of any subscriber to whom it issues a certificate.

2.8.1 Types of information to be kept confidential

The NorduGrid CA does not collect any confidential information.

2.8.2 Types of information not considered confidential

The information in issued certificates and revocation list is not considered confidential.

2.8.3 Disclosure of certificate revocation/suspension information

No stipulation.

2.8.4 Release to law enforcement officials

No stipulation.

2.8.5 Release as part of civil discovery

No stipulation.

2.8.6 Disclosure upon owner's request

The NorduGrid CA does not collect any kind of confidential information.

2.8.7 Other information release circumstances

No stipulation.

2.9 Intellectual Property Rights

This document is heavily inspired by [1] and [2].

3 Identification and Authentication

3.1 Initial Registration

3.1.1 Types of names

Each entity has a clear and unique Distinguished Name in the certificate subject field, structured according to X.501 and encoded in ASCII.

Any name under this CP/CPS will start with "O=Grid, O=NorduGrid". The remaining part is dependent on the type of entity:

Natural Person:

The subject name must contain the affiliation of the subscriber to his organization. This organisation must be one of the organizational end-entities detailed in section 1.3.3. The affiliation is included in the subject organizationalUnit with the value corresponding to the domain part of the FQDN of the organization

The full name of the entity must be included in the distinguished name after the OrganizationalUnit.

In cases of name clashes the subject name will have additional attributes after the name to make it unique.

Internetwork Entity:

Fully Qualified Domain Name as registered in the DNS. Normally the FQDN is prefixed with a network service name such as "host" or "ldap".

3.1.2 Need for names to be meaningful

The Subject Name must represent the subscriber in a way that is easily understandable for humans and must have a reasonable association with the authenticated name of the subscriber.

3.1.3 Rules for interpreting various name forms

See section 3.1.1

3.1.4 Uniqueness of names

The Distinguished Name must be unique for each subject certified by the NorduGrid CA. If the name presented by the subscriber is not unique, additional numbers or letters are appended to the common name to ensure uniqueness. Certificates must apply to unique individuals or resources. Users may not share certificates.

3.1.5 Name claim dispute resolution procedure

Name claim disputes are settled at the sole discretion of the CA administrator.

3.1.6 Recognition, authentication and role of trademarks

No stipulation.

3.1.7 Method to prove possession of private key

The NorduGrid Certification Authority verifies the possession of the private key relating to certificates requests by out-of-band, non-technical means at the time of authentication. Such verification may take the form of a directly posed question to requester.

3.1.8 Authentication of organization identity

The NorduGrid Certification Authority verifies the authenticity of the organization by checking that the organization is either

- known to peers as part of the Nordic academia network;
- checking organisation contact information;
- that the organisation in involved in research or education, by personal contact with either its peers or its (former) students.

3.1.9 Authentication of individual identity

3.2 Routine Rekey

Rekeying of certificates of persons before the expiration can be requested by sending an email signed with the private key. No other checks are performed.

Rekeying of expired certificates or Digital Processing Entities certificates follows the same rules as an initial registration.

3.3 Rekey after Revocation

Rekey after revocation follows the same rules as an initial registration.

3.4 Revocation Request

Certificate revocation requests must be sent by either a signed e-mail or communicated over other secure channel.

4 Operational Requirements

4.1 Certificate Application

Procedures are different if the subject is a person or a Digital Processing Entity. In every case the subject has to generate his own key pair. Minimum key length is 1024 bits. The maximum validity period is 1 year.

The NorduGrid Certification Authority will reject certificate applications that are not legitimate; in case a valid electronic mail address is supplied as part of the request, the NorduGrid Certification Authority may notify such applicant of this rejection. Obvious nonsense requests may be discarded without notification.

Certificate application is by submitting a PEM-formatted certificate request by electronic mail to ca@nbi.dk, or by any other secure on-line procedure provided by the NorduGrid Certification Authority. In case the requester is a natural person requesting his or her own certificate, the procedures detailed in section 3.1 apply. In case the entity is a machine or object, the certificate request may be signed by a valid certificate pertinent to the authorised administrator or responsible for the object of machine. Otherwise, such administrator or responsible will be authenticated using the procedures detailed in section 3.1.

4.2 Certificate Issuance

On receipt of a certificate request that qualified according to this CP/CPS, the CA or RA will carefully check the compliance and validity of any documents presented by the subscribers. After successful authentication, the NorduGrid Certification Authority will issue a certificate. Such issuance will be notified to the subscriber at the electronic mail address specified as part of the request. On request of the subscriber, another means of communication may be selected. If the communication fails permanently, the certificate may be revoked without further notice. No confirmation of receipt of electronic mail notification is done.

A request for certification is normally handled within one week, however during Danish summer vacation periods, and during the period around Christmas and New Year in Denmark, the response period may be three weeks.

4.3 Certificate Acceptance

No stipulation.

4.4 Certificate Suspension and Revocation

4.4.1 Circumstances for revocation

A certificate will be rekoved when the information it contains is suspected to be incorrect or when the secret key pertaining to the certificate is compromised or suspected to be compromised. This includes situation where:

- the subscribers data as represented in the certificate have changed (name changed, machine or object decommissioned, organisation dissolved or no longer eligible under the criteria detailed in section 1.3.3),
- the subscribers data is suspected to be inaccurate,
- the associated private key has been lost, compromised or misused,
- the associated private key is suspected to have been lost, compromised or misused,
- the subscriber is known to have violated his obligations with regard to the NorduGrid Certification Authority.

In addition, a subscriber may always request the revocation of his certificate directly.

4.4.2 Who can request revocation

A certificate revocation can be requested by the holder of the certificate or by the CA or RA that issued or was part of the issuance of the certificate. Also, any person currently responsible for a certified machine or object can request revocation.

Other entities may request revocation, presenting proof of knowledge of the private key compromise or change of subscriber's data.

4.4.3 Procedure for revocation request

The NorduGrid Certification Authority will handle request for revocation that reach it by any means, authenticated or unauthenticated. If the NorduGrid Certification Authority can independently verify that a certificate has been lost, compromised or misused, the NorduGrid Certification Authority will revoke the certificate.

4.4.4 Revocation request grace period

The NorduGrid Certification Authority has a maximum response time of three days (excluding weekends and public holidays in Denmark, and excluding the period between Christmas and New Year in Denmark) for recovations; it will however handle revocation requests with priority as soon as the request is recognised as such.

4.4.5 Circumstances for suspension

No stipulation.

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

CRL's are issued within one hour after every certificate revocation, and at least seven days before expiration of the last-issued CRL. The maximum validity period of a CRL is 30 days.

4.4.10 CRL checking requirements

A relying party must verify a certificate against the most recent CRL issued, in order to validate the use of the certificate.

4.4.11 On-line revocation/status checking availability

OCSP is not supported.

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 eventsw are audited:

- all boots of the ca operation machine,
- any interactive logins on this system,

4.5.2 Frequency of processing log

No stipulation.

4.5.3 Retention period for audit log

The minimum retention period is three years.

4.5.4 Protection of audit log

Audit logs are copied periodically, but at least once every month to removable media.

4.5.5 Audit log backup procedures

See section 4.5.4

4.5.6 Audit collection system (internal vs external)

No stipulation.

4.5.7 Notification to event-causing subject

Entities that cause an audit event are not explicitly notified of the audit action.

4.5.8 Vulnerability assessments

No stipulation.

4.6 Records Archival

4.6.1 Types of event recorded

The following events are recorded in either digital or paper-based archives:

- certificate requests
- issued certificates
- all electronic mail sent to the NorduGrid CA
- all electronic mail sent by the NorduGrid CA

4.6.2 Retention period for archive

The minimum retention period is 3 years.

4.6.3 Protection of archive

The electronic part of the archive, that includes the electronic mail exchange, is part of the regular back-up procedure of the Niels Bohr Institute, implies daily tape backups. Access to the electronic mail archive is controlled by Unix-style permissions.

4.6.4 Archive backup procedures

See section 4.6.3

4.6.5 Requirements for time-stamping of records

No stipulation.

4.6.6 Archive collection system (internal or external)

See section 4.6.3

4.6.7 Procedures to obtain and verify archive information

No stipulation.

4.7 Key changeover

The CA's private signing key is changed periodically; from that time on, only the new key will be used for certificate signing purposes. The older, but still valid, certificate will be available to verify old signatures until all of the certificates signed using the associated private key also have expired. The CA's certificate will have a validity period of five years.

4.8 Compromise and Disaster Recovery

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

If CA equipment is damaged or rendered inoperative, but the CA private key is not destroyed, CA operation will be reestablished as quickly as possible. If the private key is destroyed the case will be treated as in section 4.8.3.

4.8.2 Entity public key is revoked

See section 4.8.3.

4.8.3 Entity key is compromised

If the CA's private key is – or suspected to be - compromised, the CA will:

1. inform subscribers (by electronic message) and cross-certifying CAs;
2. terminate the certificates and CRL distribution services for certificates and CRLs issued using the compromised key;
3. generate a new CA authority certificate (with a new key pair) and make it immediately available in the public repository;
4. all subjects will have to recertify, following the initial identification procedures defined in Section 4.1.

4.8.4 Secure facility after a natural or other type of disaster

In the case of a disaster whereby the CA installation is physically damaged and all copies of the CA signature key are destroyed as a result, the PMA will take whatever action it deems appropriate.

4.9 CA Termination

Before the NorduGrid CA terminates its services, it will:

1. inform subscribers (by electronic messages) and cross-certifying CAs;
2. make widely available information of its termination;
3. stop issuing certificates and CRLs.

5 Physical, procedural, and personnel security controls

5.1 Physical Controls

The CA operates in a controlled environment, where access is restricted to authorized people.

5.1.1 Site location and construction

The CA is housed in the High Energy Physics deparment at the Niels Bohr Institute. See address in section 1.4.2

5.1.2 Physical access

The CA is placed on a removable hard drive which is stored in a safe.

5.1.3 Power and air conditioning

No stipulation.

5.1.4 Water exposures

No stipulation.

5.1.5 Fire prevention and protection

The building has a fire alarm system.

5.1.6 Media storage

Backups are stored in a safe.

5.1.7 Waste disposal

No stipulation.

5.1.8 Off-site backup

No stipulation.

5.2 Procedural Controls

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 role

No stipulation.

5.3 Personnel Controls

5.3.1 Background, qualifications, experience, and clearance requirements

Trained personal, well aware of the security requirements, do CA management. The persons are usually staff at the Niels Bohr Institute or otherwise working there.

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

Keys for the NorduGrid CA are generated by CA staff on a dedicated machine, not connected to any kind of network. The software package is OpenSSL.

Each entity must generate its key pair. The NorduGrid CA does not generate private keys for its subjects.

6.1.2 Private key delivery to entity

No delivery of private keys is allowed: see Section 6.1.1.

6.1.3 Public key delivery to certificate issuer

The public keys are delivered to the issuing CA through emails.

6.1.4 CA public key delivery to users

The CA certificate is available from its public repositories.

6.1.5 Key sizes

Minimum key size is 1024 bits. The recommended length is 1024 bits.

6.1.6 Public key parameters generation

No stipulation.

6.1.7 Parameter quality checking

No stipulation.

6.1.8 Hardware/software key generation

Key generation is performed in software.

6.1.9 Key usage purposes

Keys may be used for digital signature, non repudiation and key encipherment.

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

CA private keys are not escrowed.

6.2.4 Private key backup

The NorduGrid CA private key is kept, encrypted, in multiple copies and in different locations.

6.2.5 Private key archival

The backup copies can be used as an archival service.

6.2.6 Private key entry into cryptographic module

Private key is stored in encrypted form only and is protected by a passphrase of suitable length.

6.2.7 Method of activating private key

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

6.2.8 Method of deactivating private key

No stipulation.

6.2.9 Method of destroying private key

Private key backup copies will be disposed by physical destruction of the media or similar effective means.

6.3 Other Aspects of Key Pair Management

6.3.1 Public key archival

The public key is archived as part of the certificate archival.

6.3.2 Usage periods for the public and private keys

The NorduGrid CA certificate has a validity of five years and will expire on 22nd of May 2006.

6.4 Activation Data

6.4.1 Activation data generation and installation

The length of the passphrase is at least of 15 characters.

6.4.2 Activation data protection

Passphrase is not written on any kind of media.

6.4.3 Other aspects of activation data

No stipulation.

6.5 Computer Security Controls

6.5.1 Specific computer security technical requirements

The CA signing machine is not connected to any kind of network.

6.5.2 Computer security rating

No stipulation.

6.6 Life Cycle Technical Controls

6.6.1 System development controls

The NorduGrid CA uses open source software only.

6.6.2 Security management controls

No stipulation.

6.6.3 Life cycle security ratings

No stipulation.

6.7 Network Security Controls

See section 6.5.1

6.8 Cryptographic Module Engineering Controls

No stipulation.

7 Certificate and CRL Profiles

7.1 Certificate Profile

7.1.1 Version number(s)

The NorduGrid CA will issue X.509 certificates at version 3.

7.1.2 Certificate extensions

Basic Constraints:
CA:FALSE

Key Usage:
Digital Signature, Non Repudiation, Key Encipherment

Subject Key Identifier

Authority Key Identifier
DirName:/O=Grid/O=NorduGrid/CN=NorduGrid Certification Authority
serial:00

Subject Alternative Name
people: subjects e-mail address
hosts: none or FQDN.

Netscape Cert Type:
SSL Client, S/MIME

Netscape Comment:
OpenSSL Generated Certificate

7.1.3 Algorithm object identifiers

- Subject Public Key Algorithm: RSA Encryption (1.2.840.113549.1.1)
- Certificate Signature Algorithm: MD5 With RSA Encryption (1.2.840.113549.1.1.4)

7.1.4 Name forms

Issuer: O=Grid, O=NorduGrid, CN=NorduGrid Certification Authority

The Subject field contains a distinguished name of the entity with the following attributes:

OrganizationName:
"Grid"

OrganizationName:
"NorduGrid"

organizationalUnitName: people: Domain name of organization

hosts: none

commonName:

person: name and surname;

hosts a Fully Qualified Domain Name as registered in the DNS.

services service name "/" a Fully Qualified Domain Name as registered in the DNS.

7.1.5 Name constraints

See section 3.1.1

7.1.6 Certificate policy Object Identifier

This policy is identified with OID: 1.3.6.1.4.1.11604.1.1.1.1

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)

The NorduGrid CA will issue X.509 version 1 CRLs.

7.2.2 CRL and CRL entry extensions

No stipulation.

8 Specification Administration

8.1 Specification change procedures

Users will not be warned in advance of changes to the NorduGrid CA's policy and CPS. However, relevant changes will be made as widely available as possible.

8.2 Publication and notification policies

The policy is available through the NorduGrid web site: http://www.nordugrid.org/.

8.3 CPS approval procedures

No stipulation.

References

[1] INFN Certificate Policy and Certification Practice Statement - Version 2.0 - December 2003

[2] DutchGrid and NIKHEF Medium-security X.509 Certification Authority, Certification Policy and Practice Statement version 2.1

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