Belnet
BEgrid
Certification

Belnet BEgrid Certification Authority

Version 1.0

October 2003

Table of Contents

I INTRODUCTION

This Certification Policy and Practice Statement (CP/CPS) is written according to the framework laid out by RFC 2527. It describes the set of rules and procedures adhered to by the *Belnet BEgrid Certification Authority*, operated by Belnet, the Belgian Research Network, as a courtesy service to the BEgrid community.
This document is a draft, currently at version 1.0. Upon completion, the document is to be referred to as *the Belnet BEgrid certification*.

1.1 Overview

The Belnet BEgrid certification is a statement of practices, which the BEgrid CA employs in issuing public-key certificates.
A public-key certificate (hereinafter "certificate") binds a public-key value to a set of information that identifies the entity (such as person, organisation, account, or site) associated with use of the corresponding private key (this entity is known as the "subject" of the certificate). A certificate is used by a "certificate user" or "relying party" that needs to use, and rely upon the accuracy of, the public key distributed via that certificate. A certificate user is typically an entity that is verifying a digital signature from the certificate's subject or an entity sending encrypted data to the subject.
The degree to which a certificate user can trust the binding embodied in a certificate depends on several factors. These factors include the practices followed by the certification authority (CA) in authenticating the subject; the CA's operating policy, procedures, and security controls; the subject's obligations (for example, in protecting the private key); and the stated undertakings and legal obligations of the CA (for example, warranties and limitations on liability).

1.2 Identification

This document is named the Belnet Begrid certification. The currently valid version of the text is available from http://grid.belnet.be/policy/.
The current version is **draft 2~~1~~.0**, dated November ~~October~~ 1~~6~~5, 2003.

1.3 Community and Applicability

1.3.1 Certification authorities

The only entities that issue certificates of the Belnet BEgrid Certification Authority are persons, which means that no automated issuing is allowed. These persons are formally assigned staff members responsible for for the operational service of the Belnet BEgrid Certification Authority. The current list of persons comprising the operational staff of the Belnet BEgrid Certification Authority is published in an on-line accessible repository. The location of this list is stated as part of the CPS in section 1.4.
The assigned staff operate the CA functions on a best-effort basis only. They cannot be held liable for any damages resulting from the operation or non-operation of the Belnet BEgrid Certification Authority.
~~No~~ ~~S~~subordinate certification authorities will be allowed under this policy. The subordinate certification authorities will be recognised by the Director and Technical

Director of Belnet. Distributed validation will be implemented using a network of subordinate certification authorities and trusted registration authorities (RA's).

1.3.2 Subordinate Certification Authorities

An institution can be recognised by Belnet as a subordinate Certification Authority. The same rules for issuing certificates apply as those used for issuing certificates by the Belnet BEgrid CA. The subordinate CA's are required to sign a document declaring their understanding of and adherence to this CP/CPS.

~~1.3.2~~1.3.3 Registration authorities

Individuals or groups of individuals can be recognised by the Belnet BEgrid Certification Authority to act as trusted intermediaries in the identity verification process between subscriber and certification authority. Such trusted intermediaries are formally assigned by the CA and their identities and contact details published in an on-line accessible repository, the location of which is stated in section 1.4.
The RA's are required to sign a document declaring their understanding of and adherence to this CP/CPS.

~~1.3.3~~1.3.4 End entities

Certificates can be issued to natural persons and to computer entities. The entities that are eligible for certification by the Belnet BEgrid Certification Authority are all Belnet users and the entities associated with BEgrid.

~~1.3.4~~1.3.5 Applicability

The certificates issued by the Belnet BEgrid Certification Authority may not be used for financial transactions. Other than that, these certificates may be used for any application that are used on BEgrid..

1.4 Contact Details

1.4.1 Specification administration organisation

The Belnet BEgrid Certification Authority is administered by Belnet, the Belgian Research Network, by XXX. It is operated by the support team of Belnet. The contact person for this CP/CPS is:
XXX, Belnet
Rue de la science 4, Wetenschapsstraat
B-1050 Brussels
Tel.: +32 27903333
e-mail: ca@belnet.be.

1.4.1.1 Online repositories

general web address http://grid.belnet.be/certificate
policy documents http://grid;belnet.be/policy/
certificate repository
http://grid.belnet.be/certificate/rep+
~~ldap://grid.belnet.be/o=Belnet~~

certificate revocation list http://grid.belnet.be/certificates/cacrl.pem
root certificate http://grid.belnet.be/certificate/cacert.pem

1.4.2 Contact person

The Belnet BEgrid Certification Authority is operated (as meant by section 1.3.1) by:

- XXX, phone

The Registration Authorities for the Belnet BEgrid Certification Authority are:

- XXX

1.4.3 Person determining CPS suitability for the policy

Not applicable.

II GENERAL PROVISIONS

2.1 Obligations

2.1.1 CA obligations

The Belnet BEgrid Certification Authority will develop and maintain this document to reflect in detail the practices and procedures by which the CA will operate. The Belnet BEgrid Certification Authority ensures that all aspects of the CA services, operations and infrastructure related to the certificates issued under this policy are performed in accordance with the requirements of this policy. The Belnet BEgrid Certification Authority will generate and suitably protect the private key used for signing certificates under this policy.

The Belnet BEgrid Certification Authority will accept requests for certification by all entities eligible for certification under this policy, as detailed in section 1.1.3. The CA will authenticate these entities according to the procedures outlined in this document and issue signed certificates based on these requests if and only if the requirements detailed in this document are satisfied. The subscriber will be notified of the issuing of the certificate by electronic mail, sent to the address where the request originated or the address contained in the certificate request.

In special cases, an alternate e-mail address communicated to the CA operator by out-of-band means can be used. Such a case will be explicitly noted in the audit trail associated with the request.

The certificates issued by the Belnet BEgrid Certification Authority under this policy will contain a reference to the policy object identifier as part of the "certificatePolicies" certificate extension. A reference to an on-line repository containing the CP/CPS will be part of the comments-extension of the certificate.

All certificates issued by the Belnet BEgrid Certification Authority will be published in a publicly-accessible on-line repository.

The Belnet BEgrid Certification Authority will accept revocation requests according to the procedures outlined in this document. Entities requesting revocation will be authenticated by the CA or its assigned RA.
The Belnet BEgrid Certification Authority will issue a Certificate Revocation List. This CRL will be published in a publicly-available on-line repository.

By issuing a certificate that references this policy, the CA certifies to the subscriber and to all qualified relying parties who reasonably and in good faith rely on the information contained in the certificate during its operational period, that the CA has issued and will manage the certificate in accordance with this policy, as stated in the certificate extensions. Also, the CA certifies that there are no misrepresentations of fact in the certificate known to the CA, and the CA has taken reasonable steps to verify any additional information in the certificate. Also, the certificate meets all material requirements of this CP/CPS. No other liability, either expressed or implied,

is accepted with regard to the certificates issued by the Belnet BEgrid Certification Authority.

The Belnet BEgrid Certification Authority will retain a repository of the information pertaining to the certificates issued. This repository is intended to:

- establish an authentication binding between the request and the identity of the subscriber. This binding includes the affiliation of the subscriber with the organisation mentioned in the certificate subject.
- provide a means to contact the subscriber about expiration or revocation of the subscriber's certificate.
-

This repository is not available externally in an automated way. Access to this repository is restricted to CA operational staff and to assigned internal or external auditors of the CA. The repository will not hold more information than:

- Name of subscriber
- affiliation of subscriber to the level of detail as stated in the certificate
- electronic mail addresses of subscriber
- telephone numbers and call logs related to the authentication verification procedure
- physical addresses and or location of subscriber at the time of identity verification
- serial numbers of identity card shown during the verification process
- the name(s) of the RA or RA's involved in the verification process

The information contained in this repository will not be made available to any party but the CA operations staff and the internal or external auditors as part of their assigned duty.
The Belnet BEgrid Certification Authority also operates an on-line public repository of all certificates issued. This repository will contain no data about the subscriber, except for such data as contained within the certificate. In particular, no sensitive private data, no data concerning the identification procedure and no specific address information will be maintained in this repository. Professional affiliation is not to be considered sensitive private data.

2.1.2 Subordinate CA obligations

The subordinate CA's have the same obligations as those mentioned in 2.1.1. The subordinate CA's cannot further delegate the certification authority. They can recognise RA's that have to follow this CP/CPS. The subordinate CA informs the Belnet BEgrid CA of any RA's that it recognizes.

~~2.1.2~~2.1.3RA obligations

A Registration Authority shall validate requests for certification. The authentication of the identity of the subject shall be in accordance with chapter 3 of this CP/CPS. An RA shall validate the connection between the public key contained in the request and the identity of the requester.
An RA shall verify to a reasonable extent that the private key pertaining to the certification request is in the possession of the requesting entity. This verification may be out-of-band and may rely on non-technical means.
An RA shall confirm any such validation versus the CA via a reliable and trusted

mechanism. This may be either via personal contact between the RA and the CA (by phone or in person), or via cryptographically non-repudiatable and integrity protected electronic means.
Entities that act as RA for the Belnet BEgrid Certification Authority have no notification obligations when certificates are issued, revoked or suspended.

~~2.1.3~~2.1.4 Subscriber obligations

Subscribers to the Belnet BEgrid Certification Authority have the obligation to ensure that the data represented in the certification request is accurate. The subscriber will generate a key pair in a trustworthy manner, and has the obligation to protect the private key against disclosure or unintended usage. Specifically, it should be stored only in encrypted form. The pass phrase protecting the private key should be strong and at least 8 characters in length. The encrypted private key may be stored on a publicly accessible medium. The certificate must only be used for purposes consistent with this policy.
The subscriber must instruct the CA to revoke the certificate promptly upon any actual or suspected loss, disclosure or other compromise of the subscribers private key.
By making a certificate request to the Belnet BEgrid Certification Authority, the subscriber or potential subscriber accepts the registration of such data in all the repositories described in section 2.1.1. The subscriber is allowed to correct or complete the data retained in these repositories by contacting the CA operator stated in section 1.4, in accordance with the Belgain Personal Data Protection Act. Request to remove data from this repository will result in immediate and irreversible revocation of the certificate(s) pertaining to the subscriber.

~~2.1.4~~2.1.5 Relying party obligations

Qualified relying parties are expected to rely on certificates that reference this Policy and Practice Statement as appropriate authentication of the subscriber if:

- The relying party is familiar with this CP/CPS before drawing any conclusion on trust of a certificate issued by the Belnet BEgrid Certification Authority,
- The reliance is reasonable and in good faith, in light of all the circumstances known to the relying party at the time of the reliance,
- The purpose for which the certificate was used was appropriate under this CP/CPS,
- The relying party accepts all limitations on the liability of the Belnet BEgrid Certification Authority, as detailed in section 2.2,
- The relying party checked the status of the certificate prior to every reliance. Specifically, they have to check whether the validity period has expired and if the certificate has been included in the most recent Certificate Revocation List issues by the Belnet BEgrid Certification Authority,
- The relying party has checked the authenticity of the Belnet BEgrid Certification Authority root certificate before using it.

~~2.1.5~~2.1.6 Repository obligations

The Belnet BEgrid Certification Authority will maintain an on-line accessible repository of valid certificates, and of the Certificate Revocation List (CRL). The

Belnet BEgrid Certification Authority will not publish pending certification requests. Issued certificates are published within one hour after issuing. Revoked certificates are published within one hour after revocation by including them in a Certificate Revocation List.
The contact addresses for the online repositories are stated in section 1.4.
The repository is operated at a best-effort basis, where the intended availability is continuous.

2.2 Liability

2.2.1 CA liability

The Belnet BEgrid Certification Authority will not give any guarantees about the security or suitability of the service; it is provided on a best-effort basis only. The Belnet personnel is not to be held liable for any damages, including but not limited to lost profit, list savings and incidental or consequential damages. The Belnet BEgrid Certification Authority is not to be held legally responsible for problems arise out of its operation, or for problems relating to the use or misuse of the certificates it issues. It is explicitly prohibited to use the certificates issued by the Belnet BEgrid Certification Authority under this policy for any kind of financial transactions or for any kind of trade.

2.2.2 RA liability

See section 2.2.1.

2.3 Financial responsibility

No financial responsibility is accepted by the Belnet BEgrid Certification Authority.

2.4 Interpretation and Enforcement

2.4.1 Governing law

Interpretation of this policy is according to the Belgian Law.

2.4.2 Severability, survival, merger, notice

In the evennet that the CA ceases operation, all subscribers, RA'as and relying partners will be promptly notified of the termination.
All certificates issued by the CA that reference tis certificate policy will be revoked no later than the time of termination.

2.4.3 Dispute resolution procedures

In case of a dispute based on the contents of this CPS, the Director of Belnet will be the sole person responsible for resolution of the problem. The complainer cannot take legal action against Belnet.

2.5 Fees

No fees are charged for any service provided by the Belnet BEgrid Certification

Authority.

2.5.1 Certificate issuance or renewal fees

No fees are charged.

2.5.2 Certificate access fees

No fees are charged..

2.5.3 Revocation or status information access fees

No fees are charged.

2.5.4 Fees for other services such as policy information

No fees are charged.

2.5.5 Refund policy

No fees are charged.

2.6 Publication and Repository

2.6.1 Publication of CA information

The Belnet BEgrid Certification Authority operates an on-line repository, that contains:

- the CA certificate for its signing key,
- all certificates issued under this CP/CPS,
- a Certificate Revocation List (CRL), signed by the CA,
- all past and current versions of the CP/CPS.

2.6.2 Frequency of publication

CRLs will be published as soon as issued and al least every 30 days.

2.6.3 Access controls

The Belnet BEgrid Certification Authority imposes no access control on this CP/CPS and on the CRL. There is no access control on the publication of issued certificates, although the Belnet BEgrid Certification Authority reserves the right to impose such access controls when needed for reasons of proper system maintenance and to prevent abuse of the data contained in the certificates.

2.6.4 Repositories

An on-line repository will be maintained at the location specified in section 1.4.

2.7 Compliance audit

No stipulation.

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

2.8 Confidentiality

The Belnet BEgrid Certification Authority collects personal data about subscribers. This data collection is subject to the Belgian Personal Data Protection Act. The subscriber acknowledges that such data is being collected by the CA and permits storage of any such data in the secure repository intended in section 2.1.2 according to the stipulations made therein.

2.8.1 Types of information to be kept confidential

Any data part of the verification audit trail, and any data collected during the validation process is considered confidential.

2.8.2 Types of information not considered confidential

Any data contained in the subscribers certificate and any data contained in CRL's is not considered confidential.

2.8.3 Disclosure of certificate revocation/suspension information

The CA may disclose the time of revocation of a certificate but will not disclose the reason for revocation. The CA may disclose revocation statistics.

2.8.4 Release to law enforcement officials

The Belnet BEgrid Certification Authority will not disclose certificate or certificate related information to any third party, above that what is part of the certificate, except when ordered by a judge.
The Belnet BEgrid Certification Authority will take care that no information will be available except for what is required for authentication validation purposes required under this CP/CPS. Any unneeded information will be securely and completely destroyed.

2.8.5 Release as part of civil discovery

No stipulation.

2.8.6 Disclosure upon owner's request

No information will be disclosed unless requested by the subscriber in a hand-signed request and upon presentation of proper proof of identity.

2.8.7 Other information release circumstances

The CA recognises no circumstances for release of perdonal information other than those decribed in 2.8.3, 2.8.4, 2.8.5 and 2.8.6.

2.9 Intellectual Property Rights

This document is formatted according to RFC 2527 by Chokhani and Ford (ISOC 1999), and inspired by the DutchGrid and NIKHEF X.509 Certfication Authority CP/PS Version 2.1, the Grid-Ireleand CP/PS and the UK z_Svience Certification Authority CP/PS.

III IDENTIFICATION AND AUTHENTICATION

This chapter describes the procedures used to identify and authenticate certificate requesters to a RA or CA before certificate issuance. It also describes how parties requesting re-keying or revocation are authenticated. This chapter also details naming practices.

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.
Any name under this CP/CPS will start with "`O=Belnet`". Thereafter, the subscribers class, defined as either "users", "hosts" or "servers", shall be attached in the form "`O=class`". The "users" class shall contain only certificates for subscribers that are natural persons. The "hosts" class shall contain only certificates for subscribing entities that are automated systems, applications or services. The private key for "hosts" certificates may be stored in an unencrypted form. The "servers" class shall contain only certificates for subscribers that are automated systems, applications or services. The private key for such entities must be stored in proper encrypted form only.

3.1.2 Need for names to be meaningful

The subject and issuer names contained in a certificate must be meaningful and have a reasonable association with the authenticated names of the end-entities. The name used for the organisation may be a commonly recognised colloquial name. The name used for a natural person must map on the full name of such person given at birth. No name associated with an assumed identity, re-assigned identity or alias can be used.

3.1.3 Rules for interpreting various name forms

No stipulation.

3.1.4 Uniqueness of names

The Belnet BEgrid Certification Authority will assert to a reasonable level that the subject name is globally unique. At least, any name shall be unique within the ensemble of certificates issued by the Belnet BEgrid Certification Authority.

3.1.5 Name claim dispute resolution procedure

No stipulation.

3.1.6 Recognition, authentication and role of trademarks

No stipulation.

3.1.7 Method to prove possession of private key

No stipulation.

3.1.8 Authentication of organisation identity

The Belnet BEgrid Certification Authority authenticates organisations by checking: that it is a Belnet customer.

3.1.9 Authentication of individual identity

Certificates issued by the CA bind a subject name to an identified entity that is in possession of the private key pertaining to that certificate. This binding will be authenticated by the CA or its assigned RA's. In case the entity is a natural person, this authentication will be based on suitable identification documents or firm personal acquaintance by the CA or RA, testified to in writing by such RA.
In case the entity to be certified is a machine or software component, the requester (a natural person) shall prove to the satisfaction of the CA and RA that the binding will be to the service or system defined in the subject and that the requester is adequately authorised.
For subscribers, the CA shall ensure that the applicants identity is verified in accordance with this CP/CPS. In addition, the CA and RA shall record the process followed for issuance of each certificate. This record shall include:

- The identity of the person performing the identification,
- a signed declaration by that person that he has verified the identity of the subscriber as required by this policy,
- either the type and unique number of the proof of identity presented by subscriber, or a written statement by the verified that he has firm personal acquaintance with the subscriber,
- a declaration of identity, signed by a handwritten signature of the certificate applicant; this declaration requirement is waived if the RA or CA has firm personal acquaintance with the applicant and the applicant is not identified in-person.

For authentication identification, the applicant must appear in-person before the RA or CA and show at least one of either a passport or a European Identity Card. The RA or CA will meet the holder in-person and compare the photographs and will register the number of the identity piece. The RA and CA will make sure that the subject name of the certificate is non-null. In case of a natural person, the subject name must be conforming to the full name shown of the identity piece.
The affiliation of application with the organisation mentioned in the request is performed by checking public databases maintained by such organisation, or by written statement by such organisation testifying said affiliation to the RA or CA. When phone identity verification is used in the authorization process, the phone number used must be within the number range or ranges assigned to the organisation.
Machines and object are authorised by contacting the natural person responsible for such machine or object. This responsible will be authorised in accordance with the stipulation made in this section.
The certificate is send to the subscriber at the electronic mail address provided within or as part of the request. On request of the subscriber, the certificate may be delivered by other suitable means.
Since no private keys are generated by the CA, these need not be delivered to the

subscriber.

3.2 Routine Re-key

The CA will allow routine re-keying before expiration of the subscribers current certificate. The re-key request must be accompanied by a request based on a new key pair. Recertification of the existing public key is not allowed.
Re-key authentication may be be the procedure detailed in section 3.1.9, or by signing the re-key request with a current, valid private key, provided that the last identification according to 3.1.9 is not longer ago than 10 years.

3.3 Re-key after Revocation

A revoked key will not be re-certified. The authentication of a new certificate request follows the rules specified in section 3.1.

3.4 Revocation Request

A revocation request needs to be authenticated, unless the Belnet BEgrid Certification Authority can independently verify that a key compromise has happened. Authentication can be by the procedure described in section 3.1, or via a digitally singed message with a non-expired and non previously revoked certificate issued under this policy, regardless of the CP/CPS version.

IV OPERATIONAL REQUIREMENTS

4.1 Certificate Application

The Belnet BEgrid 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 Belnet BEgrid Certification Authority may notify such applicant of this rejection. Obvious nonsense requests will be discarded without notification.
Applicants must generate their own key pair; the Belnet BEgrid Certification Authority will never generate a key pair for an applicant. The Belnet BEgrid Certification Authority does not accept secret key escrow responsibilities and will reject requests that contain a private key.
The minimum key length for all applications is at least 1024 bits. The maximum validity period for a certificate is related to the key length, such that keys with a length of 1024 bits are signed for a period of at most 1 year, and keys with a length of 2048 bits are signed for a period of at most 5 years. The default validity period is 1 year.
Certificate application is by submitting a PEM-formatted certificate request by electronic mail to `ca@belnet.be`, or by any other secure on-line procedure provided by the Belnet BEgrid 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 Belnet BEgrid 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.

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 1.1.3),

- the subscribers data is suspected to be inaccurate,
- the associated private key has been compromised or misused,
- the associated private key is suspected to have been compromised or misused,
- the subscriber is known to have violated his obligations with regard to the Belnet BEgrid Certification Authority.

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 event proof of knowledge of the private key compromise or change of subscriber's data.

4.4.3 Procedure for revocation request

The Belnet BEgrid Certification Authority will handle request for revocation that reaches it by any means, authenticated or unauthenticated. If the Belnet BEgrid Certification Authority can independently verify that a certificate has been compromised or misused, Belnet BEgrid Certification Authority will revoke the certificate. In all other cases, the request for revocation will be authenticated as detailed in section 3.3.

4.4.4 Revocation request grace period

No stipulation.

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 (if applicable)

No stipulation.

4.4.10 CRL checking requirements

No stipulation.

4.4.11 On-line revocation/status checking availability

Not applicable.

4.4.12 On-line revocation checking requirements

Not applicable.

4.4.13 Other forms of revocation advertisements available

No stipulation.

4.4.14 Checking requirements for other forms of revocation advertisements

Not applicable.

4.4.15 Special requirements re key compromise

No stipulation.

4.5 Security Audit Procedures

No stipulation.

4.5.1 Types of event recorded

No stipulation

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

No stipulation.

4.5.5 Audit log backup procedures

No stipulation.

4.5.6 Audit collection system (internal vs external)

No stipulation.

4.5.7 Notification to event-causing subject

No stipulation.

4.5.8 Vulnerability assessments

No stipulation.

4.6 Records Archival

4.6.1 Types of event recorded

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

- certification requests,
- issued certificates, where a paper-log is maintained including an audit trail containing: the CA operator, check marks for subject name validity, organisation affiliation, acceptable DN form, and key length; contact information about any in-person or by-phone validation procedures, including date and time of any such interactions; Serial numbers and types of identity documents (when applicable); certificate serial number; certificate validity in days; method and address of certification notification; signature of CA operator; any details regarding the verification attempt(s),
- issued CRL's,
- all electronic mail sent to the Belnet BEgrid Certification Authority,
- all electronic mail sent by the Belnet BEgrid Certification Authority,
- all signed agreements with other parties.

4.6.2 Retention period for archive

The minimum retention period is three years.

4.6.3 Protection of archive

No stipulation.

4.6.4 Archive backup procedures

No stipulation.

4.6.5 Requirements for time-stamping of records

No stipulation.

4.6.6 Archive collection system (internal or external)

No stipulation.

4.6.7 Procedures to obtain and verify archive information

No stipulation.

4.7 Key changeover

A new public key of the Belnet BEgrid Certification Authority is posted in the on-line repository mentioned in section 1.4. In addition, signed electronic mail is sent to relevant relying parties, in particular the mailing list `dg-eur-ca@services.cnrs.fr`.

4.8 Compromise and Disaster Recovery

If the private key of the Belnet BEgrid Certification Authority is compromised or

suspected to be compromised, the Belnet BEgrid Certification Authority will

- inform subscribers, relevant relying parties and all cross-certifying CAs,
- terminate the certificate and CRL distribution for the certificates or CRL's issued using the compromised private key.

If a RA's private key is compromised or suspected to be compromised, the RA shall inform the Belnet BEgrid Certification Authority and request revocation of the RA's certificate.
If an entities private key is compromised or suspected to be compromised, the entity or its administrator or responsible must request revocation of the certificate and inform any relevant relying parties.

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

All resources used for the CA follow the Belnet Policies and Procedures.

4.8.2 Entity public key is revoked

No stipulation.

4.8.3 Entity key is compromised

No stipulation.

4.8.4 Secure facility after a natural or other type of disaster

No stipulation.

4.9 CA Termination

Termination of the Belnet BEgrid Certification Authority occurs when all service associated with the Belnet BEgrid Certification Authority is terminated permanently. In this case, the CA will:

- inform all subscribers, cross-certifying CA's, and all relying parties with which the CA has established relations,
- make publicly available information of its termination,
- stop distributing certificates and CRL's.

V PHYSICAL, PROCEDURAL, AND PERSONNEL SECURITY CONTROLS

5.1 Physical Controls

5.1.1 Site location and construction

The CA machine is located in the technical room of Belnet..

5.1.2 Physical access

The technical room of Belnet is only accessible by authorized persons.

5.1.3 Power and air conditioning

No stipulation.

5.1.4 Water exposures

No stipulation.

5.1.5 Fire prevention and protection

No stipulation.

5.1.6 Media storage

No stipulation.

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

No stipulation.

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 unauthorised actions

No stipulation.

5.3.7 Contracting personnel requirements

No stipulation.

5.3.8 Documentation supplied to personnel

No stipulation.

VI TECHNICAL SECURITY CONTROLS

6.1 Key Pair Generation and Installation

6.1.1 Key pair generation

Each entity must generate its key pair. The Belnet BEgrid CA does not generate private keys for its users.

6.1.2 Private key delivery to entity

Not applicable.

6.1.3 Public key delivery to certificate issuer

The entity must submit a certificate request with the public key according to the procedures detailed in section 4.1.

6.1.4 CA public key delivery to users

The certificate will be delivered according to the procedures detailed in section 4.2.

6.1.5 Key sizes

Keys submitted for certification must be at least 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

No stipulation.

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

Keys may be used for authentication, non-repudiation, data encryption, message integrity and session key establishment.
The CA's private key is the only key that can be used for signing certificates and CRLs.
The certificateKeyUsage field is in accordance with RFC3280.

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

Not applicable.

6.2.3 Private key escrow

The Belnet BEgrid Certification Authority keys are not given in escrow. The Belnet BEgrid Certification Authority is also not available for accepting escrow copies of keys of other parties.

6.2.4 Private key backup

The private keys of the Belnet BEgrid Certification Authority are backup up on encrypted removable magnetic media, stored in a securely controlled environment.

6.2.5 Private key archival

Backup copies made are never destroyed and may be used as an archival service.

6.2.6 Private key entry into cryptographic module

The private key of the Belnet BEgrid Certification Authority is stored in encrypted form only, and protected by a pass phrase of at least 15 characters.

6.2.7 Method of activating private key

The activation of the CA private key is by providing the pass phrase, which is at least 15 characters long.

6.2.8 Method of deactivating private key

No stipulation.

6.2.9 Method of destroying private key

No stipulation.

6.3 Other Aspects of Key Pair Management

6.3.1 Public key archival

The CA archives all issued certificates.

6.3.2 Usage periods for the public and private keys

Subscribers' certificates have a validity period of one year. The CA certificate has a validity period of five years.

6.4 Activation Data

6.4.1 Activation data generation and installation

All pass phrases used by the CA have a length of at least 15 characters, and are suitably strong according to current best practice.

6.4.2 Activation data protection

All pass phrases are known to all current staff members of the CA. Change of staff will imply change of pass phrases.

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 machine used for signing is maintained at a appropriate level of security by applying relevant security patches. It is not connected to any kind of network, and unauthorised physical access is prohibited.
The systems used by the CA to hold on-line repositories are maintained at a high level of security by applying all recommended and applicable security patches. The machine(s) are protected by a suitable firewall.

6.5.2 Computer security rating

No stipulation.

6.6 Life Cycle Technical Controls

6.6.1 System development controls

No stipulation.

6.6.2 Security management controls

No stipulation.

6.6.3 Life cycle security ratings

No stipulation.

6.7 Network Security Controls

Certificates are issued on a machine not connected to any kind of data network.

6.8 Cryptographic Module Engineering Controls

No stipulation.

VII CERTIFICATE AND CRL PROFILES

7.1 Certificate Profile

7.1.1 Version number(s)

The Belnet BEgrid Certification Authority will issue X.509 certificates at version 3.

7.1.2 Certificate extensions ~~??????~~

The following extensions will be set appropriately in entity certificates:

- **basicConstraints** (critical) Not a CA.
- **keyUsage** digitalSignature, nonRepudiation, keyEncypherment, dataEncypherment.
- **subjectKeyIdentifier** hash
- **authorityKeyIdentifier** keyid, issuer:always
- **subjectAltName** e-mail address, when requested by subscriber
- **cRLDistributionPoints** URI
- **nsCaPolicyURL** URL
- **certificatePolicies** OID 1.3.6.1.4.1.10434.4.2.1.2.0
- **nsComment** a descriptive string with reference to the CP/CPS
- **nsCertType** server, client, email

7.1.3 Algorithm object identifiers

No stipulation.

7.1.4 Name forms

See section 3.1.2.

7.1.5 Name constraints

See section 3.1.2.

7.1.6 Certificate policy Object Identifier

No stipulation.

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

The qualifier is a URL~~l~~ pointing to this document.

7.2 CRL Profile

7.2.1 Version number(s)

The Belnet BEgrid Certification Authority will issue version 1 CRLs.

7.2.2 CRL and CRL entry extensions

No stipulation.

VIII SPECIFICATION ADMINISTRATION

8.1 Specification change procedures

Minor editorial changes to this document can be made without announcement to subscribers, relying parties of cross-certifying CA's. Substantial changes in policy or changes in the technical security controls will be notified to all relevant relying parties, all cross-certifying CA's and to the public on-line repositories. ~~It will also be announced on the DataGrid CA mailing list.~~

8.2 Publication and notification policies

This policy and any older versions are available from the on-line repository mentioned in section 1.4.

8.3 CPS approval procedures

No stipulation.

IX VERSIONS

9.1 Change log

- **version 1.0** drafted October 2003
- **Version 2.0 drafted November 2003**