GARR Certification Authority Certificate Policy and Certification Practice Statement

Version 1.0

November 2006

The PDF version of this document has been signed with following PGP key:

```
pub   1024R/5BA9D271 1997-11-25
fingerprint = B3 A2 C9 CC 02 50 37 CB 79 BF 6C 00 EB F7 0A BE
uid   Roberto Cecchini <ROberto.Cecchini@fi.infn.it>
```

More info at **http://ca.garr.it/**

Contents

1 Introduction

1.1 Overview

This document — structured according to RFC 3647 [RFC3647] — describes the set of rules and procedures followed by GARR CA, the top level Certification Authority for the *GARR Consortium*.

1.2 Document name and identification

Document title:
GARR CA Certificate Policy and Certification Practice Statement
Document version:
1.0
Document date:
November 2006
Object Identifier assigned:
1.3.6.1.4.1.26238.10.1.1

1.3 PKI participants

1.3.1 Certification Authorities

GARR CA doesn't issue certificates to subordinate Certification Authorities.

1.3.2 Registration Authorities

GARR CA delegates identification and authorization of certificate subjects to trusted individuals (Registration Authorities). These intermediaries are formally nominated by the Director of the Structure in which they operate and their identities are published in an on-line repository.

1.3.3 Subscribers

GARR CA issues certificates for:

- GARR employees and fellows;
- persons belonging to the GARR constituency;
- digital processing entities, capable of performing cryptographic operations, registered in the GARR network;
- parties not affiliated with GARR, when those parties have a bona fide need to possess a certificate issued by the CA, as established by the PMA.

1.3.4 Relying parties

Relying parties may or may not be subscribers.

1.3.5 Other participants

No stipulation.

1.4 Certificate usage

1.4.1 Appropriate certificate uses

Certificates can be used for:

- e-mail signing and encryption;
- server certification and encryption of communications.

1.4.2 Prohibited certificate uses

Certificates cannot be used for uses not stated in this document.

1.5 Policy administration

1.5.1 Organization administering the document

The Policy Management Authority (PMA) for this CP and CPS is the Direction of the GARR Consortium.

1.5.2 Contact person

The primary contact is

Roberto Cecchini
GARR CA
c/o INFN, Sezione di Firenze
Via G. Sansone 1
I 50019 Sesto Fiorentino

phone: +39 0554572113
e-mail: garr-ca@garr.it

1.5.3 Person Determining CPS Suitability for the Policy

The PMA above is responsible for reviewing and approving the CPS that is to be associated with this CP.

1.5.4 CPS approval procedures

No stipulation.

1.6 Definitions and acronyms

This document uses the following terms.

Activation data
Data values, other than keys, that are required to operate cryptographic modules and that need to be protected (e.g., a PIN, a pass phrase, or a manually-held key share).

Certificate Policy (CP)
A named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements. For example, a particular certificate policy might indicate applicability of a type of certificate to the authentication of electronic data interchange transactions for the trading of goods within a given price range.

Certificate Renewal
The issuance of a new certificate to the subscriber without changing the subscriber or other participant's public key or any other information in the certificate.

Certificate Re-key
The issuance of a new certificate to the subscriber with the same DN, but different serial number and a new key pair.

Certificate Signing Request (CSR)
A message sent from an applicant to a certificate authority in order to apply for a digital identity certificate.

Certification Practice Statement (CPS)
A statement of the practices, which a certification authority employs in issuing certificates.

Issuing Certification Authority
In the context of a particular certificate, the issuing CA is the CA that issued the certificate.

Policy Management Authority (PMA)
The Authority responsible for the maintenance of the CP and CPS.

Policy Qualifier
Policy-dependent information that accompanies a certificate policy identifier in an X.509 certificate.

Registration Authority (RA)
An entity that is responsible for one or more of the following functions: the identification and authentication of certificate applicants, the approval or rejection of certificate applications, initiating certificate revocations or suspensions under certain circumstances, processing subscriber requests to revoke or suspend their certificates, and approving or rejecting requests by subscribers to renew or re-key their certificates. RAs, however, do not sign or issue certificates (i.e., an RA is delegated certain tasks on behalf of a CA).

Relying Party
A recipient of a certificate who acts in reliance on that certificate and/or digital signatures verified using that certificate.

Subscriber
A subject of a certificate who is issued a certificate.

2 Publication and Repository Responsibilities

2.1 Repositories

Repository of certificates, CRL and other relevant information is at **http://ca.garr.it/**.

2.2 Publication of Certification Information

GARR CA operates an on-line repository that contains:

- the GARR CA certificate;
- issued certificates;
- the Certificate Revocation List;
- this policy and its previous versions;
- other relevant information.

2.3 Time or Frequency of Publication

Certificates are published as soon as issued.

CRLs are published as soon as issued and at least every week..

Changes to this CP and CPS will be published as soon as they are approved. Previous versions will remain available on-line.

2.4 Access Controls on Repositories

The on-line repository is available on 24/7, subject to reasonable scheduled maintenance.

GARR CA doesn't impose any access control on its policy, its certificate, issued certificates and CRLs.

A valid personal certificate is necessary to submit a request of the following type:

- a re-key of the same certificate;

- a server certificate.

RAs must authenticate using valid certificates to be able to access the RA interface on the CA web server.

3 Identification and Authentication

3.1 Naming

3.1.1 Types of Names

The **Subject Name** is of the X.500 name type. It has one of the following forms:

- **Natural Person:**
  full name and surname of the subscriber.
- **Server:**
  fully qualified domain name.

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, make use of the allowed characters only and must have a reasonable association with the real name of the subscriber.

3.1.3 Anonymity or Pseudonymity of Subscribers

Not allowed.

3.1.4 Rules for Interpreting Various Name Forms

Common Name (CNs) must be encoded as **PrintableString** ([RFC1778]). The maximum length is 64 characters.

The character set allowed for a Common Name in personal certificates is: space (blank), decimal digits, lower and upper case US ASCII letters, apostrophe, and hyphen.

3.1.5 Uniqueness of Names

The Distinguished Name must be unique for each subject certified by GARR CA. If the name presented by the subscriber is not unique (differences in spaces are not considered significant), the CA will ask a new submission with some variation to ensure uniqueness (e. g. by additional numbers or letters).

A DN cannot be reused unless for re-keying.

Certificates must apply to unique individuals or resources. Subscribers must not share certificates.

3.1.6 Recognition, Authentication and Role of Trademarks

The PMA will resolve this kind of disputes.

3.2 Initial Identity Validation

3.2.1 Method to Prove Possession of Private Key

The request of a personal certificate is initiated by a key generation tag or control which the individual's web browser reads on the CA's user registration web page. Key generation, certificate signing request generation and submission are tied together in a single SSL session, and there is a reasonable presumption of possession of private key.

Keys generated by other means (such as **OpenSSL** [SSL]), have separate key generation, certificate signing request generation and submission stages. No test for proof of possession of the private key is made in these cases.

Re-keying employs a proof of possession of private key.

3.2.2 Authentication of Organization Identity

No stipulation.

3.2.3 Authentication of Individual Identity

- **Natural Person**: the subscriber is authenticated *in a face-to-face meeting* by the RA using a valid photo ID document. During the meeting the RA gives him an unique identifier which the subscriber must specify in the certificate request.
- **Servers**: the requester must send the request to the RA by a signed e-mail, confirming that he is responsible for the resource in question. The RA sends the request to the CA after the appropriate checks.

3.2.4 Non-Verified Subscriber Information

No stipulation.

3.2.5 Validation of Authority

- **Natural Person:**
  the RA verifies the right of the subject to obtain a certificate.
- **Server**:
  the RA verifies that the requester has administrative rights on the entity.

3.2.6 Criteria for Interoperation

No stipulation.

3.3 Identification and Authentication for Re-key Requests

3.3.1 Identification and Authentication for Routine Re-key

Re-key of certificates of natural persons before the expiration can be done by an on-line procedure, which checks the validity of the subject's certificate and asks for the approval by the competent RA.

Re-key of server certificates follows the same rules as the request of a new certificate.

3.3.2 Identification and Authentication for Re-key After Revocation

Re-key after revocation follows the same rules as the request of a new certificate.

3.4 Identification and Authentication for Revocation Request

Certificate revocation requests must be sent by **signed** e-mail by the owner of the certificate, or, if not possible, by the appropriate Registration Authority.

Revocation requests by third parties will be subject to appropriate checks by the CA personnel.

4 Certificate Life-Cycle Operational Requirements

4.1 Certificate Application

4.1.1 Who Can Submit a Certificate Application

- **Personal certificate**: the application must be submitted by the subject.

- **Server certificate**: the application must be submitted by a person with the appropriate administrative rights on it.

In every case the requester must generate his own key pair.

4.1.2 Enrollment Process and Responsibilities

- **Natural person**.
  The key pair is generated by the web browser on the subject's machine during the submission process. The same web browser must be used to download the certificate from the CA web site.
- **Server.**
  The certificate request is generated by the requester. The request is then sent, by signed e-mail, to the competent RA for approval and forwarding to the CA.

4.2 Certificate Application Processing

4.2.1 Performing Identification and Authentication Functions

- **Natural person**
  - **New request**
    Before submitting the request the user must be authenticated *in a face-to-face* meeting using a valid photo ID document by the competent RA. During the authentication a random number is generated by the system and communicated to the user by the RA and to the CA (by secure means, together with the user's affiliation, name and e-mail address). The certificate request must then be submitted by the user via an on-line procedure which requires the same data specified during the authentication, including the authorization number.
  - **Re-keying request**
    If the certificate is still valid, the user can request the re-keying via an on-line procedure which verifies the validity of his certificate. A request for approval is sent to the competent RA.
    If the certificate is no longer valid, the procedure is the same as for a new request.
- **Server.**
  Certificate requests must be sent by e-mail to the competent RA and **must be signed by a valid GARR CA certificate belonging to the requester.** The RA verifies the right of the requester to obtain the certificate and then forwards the request to the GARR CA by a **signed e-mail**.
  An e-mail with a request of confirmation is sent to the e-mail address specified in the certificate request.

4.2.2 Approval or Rejection of Certificate Applications

- **Natural person**
  - **New request**
    The certificate application is approved if the information supplied by the subject is identical to that received by the CA during the authentication phase (see 4.2.1).
  - **Re-keying request for a valid certificate**
    The competent RA receives by e-mail a notification of the re-keying request, verifies the user's right to the re-keying and sends a signed e-mail to the CA indicating its conclusions. The application is approved only if the RA gives his consent explicitly.
- **Server.**
  The certificate application is approved if the CA can verify the correctness of the signatures in the application and a confirmation of the validity of the e-mail address specified in the application is received.

4.2.3 Time to Process Certificate Applications

The maximum time of the Certificate Application Process is **2 working days**. If, after that time the process is not completed, the Certificate Application is canceled and all the involved parties are notified by the CA.

4.3 Certificate Issuance

4.3.1 CA Actions During Certificate Issuance

CA operative procedures use **OpenSSL** [SSL] and S/MIME implementations in Thunderbird/Mozilla to validate the signatures of the relevant e-mail messages.

RA access to the authentication procedure is controlled by the SSL module of the Apache CA web server.

4.3.2 Notification to Subscribers by the CA of Issuance of Certificate

If the subject is a natural person, a message is sent to his e-mail address with the instructions on how to download it from the GARR CA web server. In the other cases, the certificate is sent by e-mail to the address specified in the request and to the competent RA.

4.4 Certificate Acceptance

4.4.1 Conduct Constituting Certificate Acceptance

No stipulation.

4.4.2 Publication of the Certificate by the CA

GARR CA will make available on-line on its web server the certificate, as soon as issued.

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

The competent RA receives a notification of the issuance of personal certificates and a copy of the server certificates.

4.5 Key Pair and Certificate Usage

4.5.1 Subscriber Private Key and Certificate Usage

Subscribers must:

- read and adhere to the procedures published in this document;
- generate a key pair using a trustworthy method;
- for personal certificates, choose a unique DN (see 3.1.5) and supply a valid personal email address;
- for server certificates, apply for certificates only for resources for which they are responsible and use an email address in the request which satisfies the requirement that mail sent to that address will reach the subscriber;
- authorize the processing and conservation of personal data, as required under the DL 30 giugno 2003, n. 196;
- requesting revocation if the subscriber is no longer entitled to a certificate, or if information in the certificate becomes wrong or inaccurate;
- provide to the RA the information required to validate the request. This information may depend on the type of request;
- take reasonable precautions to prevent any loss, disclosure or unauthorized use of the private key associated with the certificate; in particular, for natural person certificates:

- selecting a good passphrase **of at least 12 characters**;
- **not storing the private key in a location accessible from the network** (e.g. in an AFS or NFS directory);
- notify immediately GARR CA in case of loss or compromise of the private key.

Failure to comply to these obligations is sufficient cause for the revocation of the certificate.

4.5.2 Relying Party Public Key and Certificate Usage

Relying parties must:

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

4.6 Certificate Renewal

Not allowed.

4.7 Certificate Re-Key

4.7.1 Circumstances for Certificate Re-Key

Re-key of a certificate is allowed for a revoked certificate, an expired certificate and a valid certificate, but not before 30 days from its expiration.

4.7.2 Who May Request Certification of a New Public Key

Re-key of a personal certificate can be required only by the subscriber.

Re-key of a certificate for a server can be required by a different requester.

4.7.3 Processing Certificate Re-Keying Requests

See 4.2.

4.7.4 Notification of New Certificate Issuance to Subscribers

See 4.3.2

4.7.5 Conduct Constituting Acceptance of a Re-Keyed Certificate

No stipulation

4.7.6 Publication of the Re-Keyed Certificate by the CA

See 4.4.2

4.7.7 Notification of the Certificate Issuance by the CA to Other Entities

See 4.4.3

4.8 Certificate Modification

No certificate modification is supported. If the information in the certificate is no longer valid, it must be revoked and re-issued.

4.9 Certificate Suspension and Revocation

4.9.1 Circumstances for Revocation

A certificate will be revoked when the information it contains is suspected to be incorrect or compromised. This includes situations where:

- the subscriber's private key is lost or suspected to be compromised;
- the information in the subscriber's certificate is suspected to be inaccurate;
- the subscriber no longer needs the certificate to access relaying parties' resources;
- the subscriber violated his obligations.

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

4.9.2 Who Can Request Revocation

A certificate revocation can be requested by the holder of the certificate, the competent RA or by any other entity presenting proof of knowledge of a circumstance for revocation.

4.9.3 Procedure for Revocation Request

The revocation request is accepted in the following circumstances:

- the request is signed by the same certificate whose revocation is requested;
- the request is signed by the competent RA;
- the request is from a properly authenticated entity.

4.9.4 Revocation Request Grace Period

The revocation request must be immediate in case of key compromise, within one working day in all the other circumstances.

4.9.5 Time Within Which CA Must Process the Revocation Request

The CA will process the revocation request within one working day.

4.9.6 Revocation Checking Requirements for Relying Parties

Relying parties must check the revocation status of a certificate before its validation.

4.9.7 CRL Issuance Frequency

CRLs are issued immediately after each revocation and at least weekly.

4.9.8 Maximum Latency for CRLs

The posting of the CRL to the repository is within minutes from its generation.

4.9.9 On-Line Revocation/Status Checking Availability

GARR CA provides an on-line consultation of the issued certificates.

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

Suspension is not supported.

4.9.14 Who Can Request Suspension

No stipulation.

4.9.15 Procedure for Suspension Request

No stipulation.

4.9.16 Limits on Suspension Period

No stipulation.

4.10 Certificate Status Services

Non supported

4.11 End of Subscription

If the subscriber wants to end his subscription, he must request a revocation of his certificate.

No procedure is necessary if the certificate is expired.

4.12 Key Escrow and Recovery

Not supported.

5 Facility, Management, and Operational Controls

5.1 Physical Controls

5.1.1 Site Location and Construction

The CA is housed in the detached GARR Offices located in the University of Florence Campus at Sesto Fiorentino.

5.1.2 Physical Access

The signing machine and all removable media are stored in safes whose combinations are known to the CA personnel only.

The repository is managed by servers hosted in rooms where access is monitored and restricted to authorized people.

5.1.3 Power and Air Conditioning

The building has an air conditioning system and the servers are connected to an UPS system.

5.1.4 Water Exposures

The building is in a zone not subject to floods and the computer room is at an upper level.

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 whose combination is known to CA personnel only.

5.1.7 Waste Disposal

No stipulation.

5.1.8 Off-site Backup

No stipulation.

5.2 Procedural Controls

5.2.1 Trusted Roles

CA Manager

- appointed by the GARR Consortium;
- supervises CA operation;
- manages the CP/CPS.

CA Operator

- appointed by the CA manager;
- verifies the requests;
- signs the certificates;
- publishes the certificates and CRL on the repository;
- makes periodical backups.

System Administrator

- performs periodical integrity checks on the software;
- keeps the system software updated;
- periodically verifies the backups.

System developer

- maintains and develops the software necessary for CA operation;
- maintains the ticketing system.

RA

- appointed by the Authority responsible for the Structure;
- verifies the user's identity and rights to the certificate requests;
- approves the re-key requests;
- submits to the CA the requests for server certificates.

5.2.2 Number of Persons Required per Task

One person for CA manager, System Administrator, System developer, at least two persons for CA Operator.

5.2.3 Identification and Authentication for Each Role

No stipulation.

5.2.4 Roles Requiring Separation of Duties

No stipulation

5.3 Personnel Controls

5.3.1 Background, Qualifications, Experience, and Clearance Requirements

CA personnel must be composed by trained persons and well aware of the necessary security requirements.

5.3.2 Background check procedures

No stipulation.

5.3.3 Training Requirements

GARR CA personnel is trained in:

- basic PKI Concepts;
- use and operation of the PKI software;
- the relevant CP/CPS;
- computer security.

5.3.4 Retraining Frequency and Requirements

Training in the use and operation of the PKI software and ticketing system will be provided whenever the software is updated.

Any changes in CP/CPS will be communicated to the CA personnel as soon as possible.

5.3.5 Job Rotation Frequency and Sequence

No stipulation.

5.3.6 Sanctions for Unauthorized Actions

In case of unauthorized action the CA manager will revoke the pertinent privileges.

5.3.7 Independent Contractor Requirements

No independent contractor are used.

5.3.8 Documentation Supplied to Personnel

GARR CA personnel is supplied with the following documentation:

- this CP/CPS;
- documentation of the ticketing system;
- documentation of the CA software;
- documentation of the operating procedures.

5.4 Audit Logging Procedures

5.4.1 Types of Events Recorded

The following events are recorded:

- certification requests;
- issued certificates;
- requests for revocation;
- issued CRLs;
- login/logout/reboot of the signing machine.

5.4.2 Frequency of Processing Log

Logs are archived weekly.

5.4.3 Retention Period for Audit Log

The minimum retention period is 3 years.

5.4.4 Protection of Audit Log

Audit logs can be modified by the system administrator only.

Copies are kept on non rewritable media locked in a safe.

5.4.5 Audit Log Backup Procedures

Logs are archived weekly by a CA Operator on write-once media. The media is kept locked in a safe.

5.4.6 Audit Collection System (Internal vs. External)

The system is internal.

5.4.7 Notification to Event-Causing Subject

No stipulation.

5.4.8 Vulnerability Assessments

Audit files are periodically scanned to identify potential attempts to breach the security of the system.

5.5 Records Archival

5.5.1 Types of Records Archived

All the events listed in 5.4.1 are archived.

5.5.2 Retention Period for Archive

Minimum retention period is 3 years.

5.5.3 Protection of Archive

Archives are kept on write-once media and are accessible only from CA personnel.

5.5.4 Archive Backup Procedures

Archives are copied weekly by a CA Operator on write-once media. The media is kept locked in a safe.

5.5.5 Requirements for Time-Stamping of Records

No stipulation.

5.5.6 Archive Collection System (Internal or External)

Archiving system is internal.

5.5.7 Procedures to Obtain and Verify Archive Information

No stipulation.

5.6 Key Changeover

The CA will generate a new CA self-signed certificate one year before the expiry of the CA certificate. In the last year the CA's old certificate will be available for validation purposes and CRL signing only: new certificates will be signed with the new key.

5.7 Compromise and Disaster Recovery

5.7.1 Incident and Compromise Handling Procedures

CA systems are continuously monitored for intrusion signs. As soon as a successful intrusion will be ascertained, the CA manager will be informed.

5.7.2 Computing Resources, Software, and/or Data Are Corrupted

If the private key is not compromised, computing resources will be rebuilt from the last good backup.

5.7.3 Entity Private Key Compromise Procedures

If the CA's private key is compromised, the CA will:

- inform the Registration Authorities, Subscribers and Relying Parties of which the CA is aware;
- terminate the certificates and CRL distribution services for certificates and CRLs issued using the compromised key;
- issue a new CA self-signed certificate and set up a new repository and distribution service.

5.7.4 Business Continuity Capabilities After a Disaster

New facilities will be set up using the backup copies kept off-site.

5.8 CA or RA Termination

Before the GARR CA terminates its services, it will:

- inform the Registration Authorities, Subscribers and Relying Parties of which the CA is aware;
- make information of its termination widely available;
- stop issuing certificates.

An advance notice of at least 60 days will be given in the case of scheduled termination.

The CA Manager at the time of termination shall be responsible for the subsequent archival of all records.

6 Technical Security Controls

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

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

RAs and other subjects must generate their own key pair: in software (e.g. via the **OpenSSL** package) or in hardware.

*I*n every case GARR CA doesn't generate private keys for its subjects.

6.1.2 Private Key Delivery to Subscribers

No delivery of private keys is allowed: see Section 6.1.1

6.1.3 Public Key Delivery to Certificate Issuer

Subjects' public keys are delivered to the issuing CA in a secure and trustworthy manner: by an on-line transaction from a secure web server for personal certificates, via the HTTPS protocol, and by signed e-mail for server certificates.

6.1.4 CA Public Key Delivery to Relying Parties

CA certificate is available from its public repository.

6.1.5 Key Sizes

Minimum and recommended key length is 1024 bits.

Maximum key length is 2048 bits.

6.1.6 Public Key Parameters Generation and Quality Checking

No stipulation.

6.1.7 Key Usage Purposes (as per X.509 v3Key Usage Field)

Keys may be used for authentication, data encryption, message integrity and session key establishment.

GARR CA private key is the only key that can be used for signing certificates and CRLs.

The Certificate key Usage field must be used in accordance with [RFC3280].

6.2 Private Key Protection and Cryptographic Module Engineering Control

6.2.1 Cryptographic Module Standards and Controls

No stipulation.

6.2.2 Private Key (n out of m) Multi-person Control

Multi-person control not allowed

6.2.3 Private Key Escrow

Private key escrow not allowed

6.2.4 Private Key Backup

GARR CA private key is kept, encrypted, in multiple copies and in different locations, on write-once media.

6.2.5 Private Key Archival

Backup copies can be used as an archival service.

6.2.6 Private Key Transfer Into or From a Cryptographic Module

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

6.2.7 Private Key Storage on Cryptographic Module

No stipulation.

6.2.8 Method of Activating Private Key

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

6.2.9 Method of Deactivating Private Key

Cryptographic modules which have been activated will not be left unattended. They will be deactivated after use, e.g. via logout procedure.

6.2.10 Method of Destroying Private Key

Private key backup copies will be disposed by physical destruction of the media.

6.2.11 Cryptographic Module Rating

No stipulation.

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 Certificate Operational Periods and Key Pair Usage Periods

GARR CA certificate has a validity of **ten** (10) years and will expire on **25 October 2016**.

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

The length of the pass phrase is at least of 15 characters.

6.4.2 Activation Data Protection

Pass phrase isn't 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

CA servers include the following functionalities:

- operating systems are maintained at a high level of security by applying all recommended security patches;
- monitoring is done to detect unauthorized software changes;
- services are reduced to the bare minimum;
- machines are protected by suitably configured firewalls.

The machine used for signing certificates is never connected to any kind of network.

6.5.2 Computer Security Rating

No stipulation.

6.6 Life-Cycle Security Controls

6.6.1 System Development Controls

GARR CA uses public domain software and in house developed only.

6.6.2 Security Management Controls

Software is periodically checked for tampering using strong cryptographic techniques.

6.6.3 Life Cycle Security Controls

No stipulation.

6.7 Network Security Controls

See Section 6.5.1.

6.8 Time-Stamping

No stipulation.

7 Certificate, CRL and OCSP Profiles

7.1 Certificate Profile

7.1.1 Version Number:

X.509 v3.

7.1.2 Certificate extensions

Basic Constraints

root certificate: **critical**, CA:TRUE

end-entity certificate: **critical**, CA:FALSE

Key Usage

root certificate: **critical**, CertSign, CRLSign

end-entity certificate: **critical**, Digital Signature, Key Encipherment, Data Encipherment

Extended Key Usage

natural person: 1.3.6.1.5.5.7.3.2 (TLS WWW client authentication), 1.3.6.1.5.5.7.3.4 (E-mail protection)

server: 1.3.6.1.5.5.7.3.1 (TLS WWW server authentication), 1.3.6.1.5.5.7.3.2 (TLS WWW client authentication), 1.3.6.1.4.1.311.10.3.3 (Microsoft Server Gated Crypto), 2.16.840.1.113730.4.1 (Nestcape Server Gated Crypto)

Subject Key Identifier

Unique identifier of the subject key according to RFC 2459 [RFC2459].

Certificate Authority Key Identifier

Directory Address: **`C=IT,O=GARR,CN=GARR Certification Authority`**

Serial Number: **`00`**

Unique identifier of the issuer key according to RFC 2459 [RFC2459].

Subject Alternative Name

natural person: subject's e-mail address

server: FQDN of the server and requester's e-mail address

CRL Distribution Points

URL=http://ca.garr.it/crl.der

Certificate Policies

see Section 1.2

7.1.3 Algorithm Object Identifiers:

Subject Public Key Algorithm: RSA Encryption (1.2.840.113549.1.1)

Certificate Signature Algorithm: SHA-1 With RSA Encryption (1.2.840.113549.1.1.5)

7.1.4 Name forms:

Issuer: `C=IT, O=GARR, CN=GARR Certification Authority`

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

countryName: `IT`

organizationName: `GARR`

organizationalUnitName:

A name which identifies unambiguously the organization hosting the RA which approved the subject's request

commonName:

natural person: name and surname;

server: a fully qualified domain name as registered in the DNS;

7.1.5 Name Constraints

No stipulation.

7.1.6 Certificate Policy Object Identifier

The OID of the relevant CP/CPS without any qualifiers.

7.1.7 Usage of Policy Constraints Extensions

No stipulation.

7.1.8 Policy Qualifier Syntax and Semantics

Not allowed.

7.1.9 Processing Semantics for the Critical Certificate Policy Extension

No stipulation.

7.2 CRL Profile

7.2.1 Version

X.509 v1.

7.2.2 CRL and CRL Entry Extensions

No stipulation

7.3 OCSP Profile

No stipulation

8 Compliance Audit and Other Assessment

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

8.1 Frequency and Circumstances of Assessment

No Stipulation.

8.2 Identity/Qualifications of Assessors

No stipulation.

8.3 Assessor's Relationship to Assessed Entity

No stipulation.

8.4 Topics Covered by Assessment

No stipulation.

8.5 Actions Taken as a Result of Deficiency

No stipulation.

8.6 Communications of Results

No stipulation.

9 Other Business and Legal Matters

9.1 Fees

No fees are charged.

9.2 Financial Responsibility

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

9.3 Confidentiality of Business Information

No stipulation.

9.3.1 Scope of Confidential Information

No stipulation.

9.3.2 Information not Within the Scope of Confidential Information

No stipulation.

9.3.3 Responsibility to Protect Confidential Information

No stipulation.

9.4 Privacy of Personal Information

GARR CA collects subscribers' full name, organization and e-mail address. This information is included in the issued certificates.

No other subscribers' information is collected.

9.4.1 Privacy Plan

The treatment of the user's personal data is done according to the current Italian legislation.

9.4.2 Information Treated as Private

No information is treated as private

9.4.3 Information not Deemed Private

All information collected by the CA is not deemed private.

9.4.4 Responsibility to Protect Private Information

No stipulation

9.4.5 Notice and Consent to Use Private Information

The user must give his consent to the treatment of his personal data.

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

No stipulation.

9.4.7 Other Information Disclosure Circumstances

No stipulation.

9.5 Intellectual Property Rights

The GARR CA does not claim any Intellectual Property Rights on issued certificates.

Parts of this document are inspired by or copied from [CER06], [DOE01], [EPK04], [FBC99], [INF06], [UKE06].

9.6 Representations and Warranties

9.6.1 CA Representations and Warranties

The GARR CA guarantees to issue certificates only to subscribers identified by requests received from RAs via secure channels.

The GARR CA will revoke a certificate only in response to an authenticated request from the Subscriber, or the RA which approved the subscriber's request, or if it has itself reasonable proof that circumstances for revocation are fulfilled.

The CA only guarantees to verify subscriber's identities according to procedures described in this document. In particular, certificates are guaranteed only to reasonably identify the subscriber (see sections 3.2 and 3.3).

9.6.2 RA Representations and Warranties

It is the RA's responsibility to authenticate the identity of subscribers requesting certificates, according to the practices described in this document.

It is the RA's responsibility to request revocation of a certificate if it is aware that circumstances for revocation are satisfied.

9.6.3 Subscribers Representations and Warranties

No stipulation.

9.6.4 Relying Party Representations and Warranties

No stipulation.

9.6.5 Representations and Warranties of Other Participants

No stipulation.

9.7 Disclaimers of Warranties

9.8 Limitations of Liability

The GARR CA does not warrant its procedures, nor takes responsibility for problems arising from its operation or the use made of the certificates it provides and gives no guarantees about the security or suitability of the service.

The CA does not accept any liability for financial loss, or loss arising from incidental damage or impairment, resulting from its operation. No other liability, implicit or explicit, is accepted.

9.9 Indemnities

GARR CA declines any payment of indemnities for damages arising from the use of its certificates.

9.10 Term and Termination

9.10.1 Term

This document will become effective after its publication on the GARR CA web site.

9.10.2 Termination

This document is effective until it is superseded by a newer version,

9.10.3 Effect of Termination and Survival

No stipulation.

9.11 Individual Notices and Communications with Participants

All communications between CA and RAs must happen in a secure way (e.g. by signed e-mail).

9.12 Amendments

9.12.1 Procedure for Amendment

Non trivial changes to this document must undergo the procedure described in section 1.5.

9.12.2 Notification Mechanism and Period

Planned changes will be advertised on the CA web site and sent to all the RAs at least 15 days in advance.

9.12.3 Circumstances Under Which OID Must Be Changed

Each non trivial change will require a change of the OID.

9.13 Dispute Resolution Provisions

No stipulation.

9.14 Governing Law

GARR CA operation is subject to the Italian laws.

9.15 Compliance with Applicable Law

No stipulation.

9.16 Miscellaneous Provisions

9.16.1 Entire Agreement

This document supersedes all prior and contemporaneous written or oral understandings relating to the same subject matter.

9.16.2 Assignment

No stipulation.

9.16.3 Severability

If a clause of this document should be declared invalid by a court or other tribunal, it will be replaced by a conforming one as soon as possible, but the remainder of the document will remain en force.

9.16.4 Enforcement (Attorney's Fees and Waiver of Rights)

No stipulation.

9.17 Other Provisions

No stipulation.

Bibliography

[CER06] *CERN Certification Authority Certificate Policy and Certificate Practice Statement,* Version 1.1 (2006).

[DOE01] *DOE Science Grid CA CP/CPS,* Version 1.1 (2001).

[EPK04] *EuroPKI Certificate Policy*, Version 1.1 (2004).

[FBC99] *X.509 Certificate Policy For The Federal Bridge Certification Authority* (FBCA), Version 1.0, (1999).

[INF06] *INFN CA CP/CPS*, version 2,2 http://security.fi.infn.it/CA/CPS/CPS-2.1.pdf (2006).

[UKE06] *UK e-Science Certification Authority Certificate Policy and Certification Practices Statement*, Version 1.3 (2006).

[SSL] http://www.openssl.org/.

[RFC1778] T. Howes, S. Kille, W. Yeoung, and C. Robbins, T*he String Representation of Standard Attribute Syntaxes,* RFC 1778 (1995).

[RFC2252] M. Wahl, A. Coulbeck, T. Howes, and S. Kille, *Lightweight Directory Access Protocol (v3): Attribute Syntax Definitions*, RFC 2252 (1997).

[RFC2459] R. Housley, W. Ford, W. Polk and D. Solo, *Internet X.509 Public Key Infrastructure Certificate and CRL Profile,* RFC 2459 (1999).

[RFC3280] - R. Housley, W. Polk, W. Ford and D. Solo, *Internet X.509 Public Key Infrastructure Certificate and CRL Profile*, RFC 3280

[RFC3647] - S. Chokani, W. Ford, R. Sabett, C. Merril and S. Wu, *Internet X.509 Infrastructure Certificate Policy and Certification Practices Framework*, RFC 3647 (2003).

List of changes

VERSION	DATE	CHANGES
1.0	November 2006	Initial Release