INFN CA
Certificate Policy and Certification Practice Statement

Version 2.4

November, 1 2015

This document is available from **http://security.fi.infn.it/CA/CPS/**

Contents

1. Introduction

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 passphrase, 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.

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

Issuing Certification Authority (Issuing CA)
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 identification and authentication of certificate subjects, but that does 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.

Robot
A personal credential which can perform automated tasks on behalf of the user.

Set of provisions
A collection of practice and/or policy statements, spanning a range of standard topics, for use in expressing a certificate policy definition or CPS and employing the approach described in this framework.

1.1 Overview

This document — structured according to RFC 2527 [RFC2527] — describes the set of rules and procedures followed by INFN CA, the top level Certification Authority for the *Istituto Nazionale di Fisica Nucleare* (INFN, http://www.infn.it/).

1.2 Identification

Document title:
INFN CA Certificate Policy and Certification Practice Statement

Document version:
2.4

Document date:
November, 1, 2015

Object Identifier assigned:
1.3.6.1.4.1.1043.10.1.8

This document is available from: **http://security.fi.infn.it/CA/CPS**

1.3 Community and Applicability

1.3.1 Certification Authorities

The INFN CA is a self-signed root certification authority. It doesn't issue certificates to subordinate CA's.

1.3.2 Registration Authorities

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

RA's must perform their tasks in accordance with this CP/CPS.

1.3.3 End Entities

INFN CA issues certificates for:

- INFN employees and fellows;
- people involved in research activities in collaboration with INFN employees;
- digital processing entities, capable of performing cryptographic operations, owned by INFN or used for activities in which INFN is involved;
- services on digital processing entities, owned by INFN or used for activities in which INFN is involved;
- parties not affiliated with INFN, when they have a bona fide need to possess a certificate issued by the INFN CA, as established by the PMA.

1.3.4 Applicability

Certificates issued can be used for:

- e-mail signing and encryption (S/MIME);
- client authentication (SSL/TSL and GSI);
- server authentication and encryption of communications (SSL/TSL and GSI);
- generation of proxy certificates, as specified in RFC3820 [RFC3820];
- object-signing.

1.4 Contact Details

1.4.1 Specification Administration Organization

The INFN CA is managed by the Istituto Nazionale di Fisica Nucleare (INFN).

This document is managed by the INFN CA manager (see Section 1.4.2).

1.4.2 Contact person

The primary contact and CA manager is

Roberto Cecchini
INFN, Sezione di Firenze
Via G. Sansone 1
I 50019 Sesto Fiorentino

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

1.4.3 Person Determining CPS Suitability for the Policy

See Section 1.4.2.

2. General Provisions

2.1 Obligations

2.1.1 CA Obligations

INFN CA will operate a Certification Authority service in accordance with all provisions of this CP and associated CPS.

In particular it will:

- issue certificates based on the requests from entitled subscribers, validated by a Registration Authority;
- notify the subscriber of the issuing of the certificate;
- publish the issued certificates;
- accept revocation requests according to the procedures outlined in this document;
- issue and publish Certificate Revocation Lists (CRL's).

2.1.2 RA Obligations

INFN CA delegates the tasks of identification and authorization of certificate subjects to **Registration Authorities**.

A Registration Authority must:

- authenticate the entity which makes the certification request in accordance 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;
- for host or service certificate verify that the requester is the system administrator of the resource or has been authorized by him;
- for robots certificates verify that the requester has satisfied the requirements
- accept revocation requests, according to the procedures outlined in this document, and immediately notify the INFN CA;
- provide information to the subscriber on how to properly maintain a certificate and the corresponding private key;
- record and archive all certificate requests, all revocation requests and notifications of certificate issuance.

2.1.3 Subscriber Obligations

Subscribers must:

- adhere to the procedures published in this document;
- use the certificates for the permitted purposes only;
- generate a key pair using a trustworthy method;
- for host or service certificates apply only if they are the system administrators or have been authorized by him;
- for robot certificates use a secure key token to protect the private key;
- 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 suitable pass phrase of at least 12 characters;
  - not storing it in a network shared file system (e.g. in an AFS or NFS directory);
- notify immediately the INFN CA or the RA 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.

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

INFN CA will make available on its web server and its LDAP server the certificates and CRL's, as soon as issued.

2.2 Liability

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

2.2.1 CA Liability

The INFN 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.

2.2.2 RA Liability

It is RA's responsibility to authenticate the subscribers according to the procedure described in this document and to inform the CA if circumstances for revocation are satisfied.

2.3 Financial Responsibility

The INFN 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 PMA and the sponsoring organization pursuant to the agreement between the two entities.

2.4 Interpretation and Enforcement

2.4.1 Governing Law

Interpretation of this CP and CPS is according to Italian law.

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.

Before termination of its operations, the INFN CA will notify its subscribers and Registration Authorities. All issued certificates will be revoked before the time of termination.

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

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 refund will be given at any time.

2.6 Publication and Repositories

2.6.1 Publication of CA Information

The INFN CA operates an on-line repository at the address specified below that contains:

- the INFN CA's certificate;
- issued certificates;
- the Certificate Revocation List;
- a copy of this document and all previous versions;
- other relevant information.

2.6.2 Frequency of Publication

Certificates will be published as soon as issued.

CRL's will be 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.

2.6.3 Access Controls

The on-line repository is maintained on a best effort basis, available on 24 hours per day, 7 days per week basis, subject to reasonable scheduled maintenance.

INFN CA doesn't impose any access control on its Policy, its certificate, issued certificates and CRL's.

2.6.4 Repositories

Repository of certificates and CRLs is at **http://security.fi.infn.it/CA/**.

2.7 Compliance Audit

2.7.1 Frequency of Entity Compliance Audit

The INFN CA management will carry, once per year, a self-assessment to verify the compliance of its operating procedures to this CP/CPS.

INFN CA will accept no more than an external compliance audit per year and its entire cost must be borne by the requester.

2.7.2 Identity/Qualifications of Auditor

No stipulation.

2.7.3 Auditor's Relationship to Audited Party

The audit can be requested by qualified relying parties, e.g. by a policy management authority which INFN CA recognizes. INFN CA may require evidence of the chosen auditor qualifications. INFN CA may impose confidentiality restrictions upon the auditor.

2.7.4 Topics Covered by Audit

The audit will verify the compliance of the CA operating procedures with the current CP/CPS.

2.7.5 Actions Taken as a Result of Deficiency

The CA manager will announce the steps, with a timetable, that will be taken to remedy the deficiencies found.

2.7.6 Communication of Results

The CA manager will publish the results and the proposed remedies. The quantity of details will be decided according to security and confidentiality reasons.

2.8 Confidentiality

INFN CA collects subscribers' full name, organization, e-mail address, details of the document presented for identification (type, number, date of issuance) and "Fiscal Code", in accordance with the Italian Personal Data Protection Law.

Under no circumstances INFN CA will 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

Data collected during the authorization process and not published in the certificate is considered confidential.

2.8.2 Types of Information Not Considered Confidential

Information included in the issued certificates and CRL's is not considered confidential.

2.8.3 Disclosure of Certificate Revocation/Suspension Information

When a certificate is revoked, a reason code may be included in the CRL entry for the action. This reason code is not considered confidential.

Other details concerning the revocation will not be disclosed unless required by a legal authority of competent jurisdiction.

2.8.4 Release to Law Enforcement Officials

See Section 2.4.1.

2.8.5 Release as Part of Civil Discovery

See Section 2.4.1.

2.8.6 Disclosure Upon Owner's Request

Disclosure upon owner's request will be done according to the Italian Personal Data Protection Law.

2.8.7 Other Information Release Circumstances

No other circumstances for release of personal information apart those in the above paragraphs.

2.9 Intellectual Property Rights

This document follows the template specified by RFC 2527 [RFC2527].

Parts of this document are inspired or copied by other CP and CPS: [TrustID] , [NCSA], [HEPKI], [FBCA] and in particular [UkeS] and [DGri].

3. Identification and Authentication

3.1 Initial Registration

3.1.1 Types of Names

The subject name is of the X.500 name type, all its parts are encoded as *PrintableString*s.

The *CommonName* has one of the following forms:

- **Natural Person:**
  name and surname of the subscriber;
- **Digital Processing Entity:**
  the entity fully qualified domain name;
  Service:
  the service name, a '**/**' and the server fully qualified domain (e.g. '**gridftp/server.domain.name**');
- **Robot**
  the string '**Robot:** ', a brief description of its function, a '-' and the full name of the subscriber (e.g.: '**Robot: function – subscriber name**')

3.1.2 Need for Names To Be Meaningful

The *CommonName* 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. It may contain additional text to disambiguate between different users or to allow the same user to have more than one certificate.

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 INFN CA. If the name presented by the subscriber is not unique, additional numbers or letters are appended to the common name to ensure uniqueness (see Section 3.1.2).

INFN CA will ensure that each issued DN is unique and that it will never be assigned to more than one entity for the whole life of the CA.

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

3.1.5 Name Claim Dispute Resolution Procedure

The CA manager will resolve this kind of disputes.

3.1.6 Recognition, Authentication and Role of Trademarks

No stipulation.

3.1.7 Method to Prove Possession of Private Key

A request of a personal certificate is initiated by a key generation tag or control which the user's web browser reads on the CA's user registration web page. Key and 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 in requests originating in web browser functions.

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

Rekeying employs a proof of possession of private key.

3.1.8 Authentication of Organization Identity

Authentication of Organization Identity is part of the procedure for the appointment of an RA (see Section 1.3.2), and only the Organizations for which an RA has been appointed appear the certificates.

3.1.9 Authentication of Individual Identity

- **Natural Person**: the subscriber is authenticated *de visu* by the RA using a valid photo ID document. The RA will communicate to the CA in a secure on-line transaction: name and surname of the requester, the details of his ID document and his "Fiscal Code".
- **Digital Processing Entity** and **Service:** the requester must send the request to the RA by a signed e-mail. The RA verifies the correctness of the request and sends it – including the requester's signature – to the CA by a signed e-mail.
- **Robot**: as for a Natural Person. In addition the certificate request must be generated in the RA's presence using a secure hardware token, as described in Section 6.2.1.

3.2 Routine Re-key

Re-key of certificates of natural persons and Robots before the expiration, *and providing that the last identification in accordance to Section 3.1.9 is not older than 5 years*, can be requested by an on-line procedure, which checks the validity of the subject's certificate. The certificate is issued after the approval by the pertinent RA.

In all the other cases re-keying follows the same rules as an initial registration.

3.3 Re-key After Revocation

Re-key after revocation follows the same rules as an initial registration.

3.4 Revocation Request

Certificate revocation requests must be sent by **signed** e-mail by the owner of the certificate, by the appropriate Registration Authority or by any other entity presenting proof of knowledge of a circumstance for revocation.

4. Operational Requirements

4.1 Certificate Application

Procedures are different if the subject is a natural person or a digital processing entity. In every case the subject has to generate his own key pair.

Minimum key length is 1024 bits.

- **Natural person**.
  Before submitting the request the user must be authenticated by an RA. During the authentication a random authorization number is generated, communicated to the user and sent to the CA, together with the user's data (see Section 3.1.9). Before 48 hours from the authentication, the user must submit a certificate request via an on-line procedure, specifying the above authorization number. The request is considered valid if the information supplied by the user coincides with that received during the authentication.
- **Digital Processing Entity** and **Services**.
  Certificate requests are sent by e-mail to the appropriate RA and must be signed by a valid INFN CA certificate belonging to a natural person. The RA verifies the right of the requester to obtain the certificate and then forwards the request to the INFN CA by a signed e-mail. An e-mail with a request of confirmation is sent to the address specified by the requestor to check its validity. The certificate request is not valid until reception of the confirmation.
  A configuration file for OpenSSL is available from the CA web server.
- **Robot.**
  As for a natural person, with the difference that the user must generate the certificate request in presence of the RA, using a secure hardware token (see Section 6.2.1).

4.2 Certificate Issuance

INFN CA issues the certificate if, and only if, the authentication of the subject is successful.

If the subject is a natural person, a message is sent to his e-mail address with the download instructions. In the other cases, the certificate is sent *to the address specified in the request*.

If the authentication is unsuccessful, the certificate is not issued and e-mail with the reason is sent to the subject.

A copy of all correspondence is always sent to the RA.

4.3 Certificate Acceptance

No stipulation.

4.4 Certificate Suspension and Revocation

4.4.1 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 violated his obligations.

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

4.4.2 Who Can Request Revocation

A certificate revocation can be requested by the holder of the certificate to be revoked or by any other entity presenting proof of knowledge of a circumstance for revocation (see Section 3.4).

4.4.3 Procedure for Revocation Request

The entity requesting the revocation must authenticate itself properly. CA Operators will decide on the matter.

4.4.4 Revocation Request Grace Period

The revocation for a compromise of the private key must be requested immediately, within one working day for the other circumstances.

4.4.5 Circumstances for Suspension

INFN CA doesn't offer suspension services.

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 immediately after every certificate revocation or at least every week.

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 (see Section 2.1.4).

4.4.11 Online Revocation/Status Checking Availability

OCSP is not supported.

4.4.12 Online Revocation Checking Requirements

No stipulation.

4.4.13 Other Forms of Revocation Advertisement 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 events are recorded:

- authentications of natural person;
- certification requests;
- issued certificates;
- revocation requests;
- issued CRL's;
- all correspondence sent and received by the INFN CA;
- reboot, login and logout on the signing machine.

4.5.2 Frequency of Processing Log

No stipulation.

4.5.3 Retention Period for Audit Logs

The minimum retention period is three years.

4.5.4 Protection of Audit Log

Only authorized persons have access to the logs.

4.5.5 Audit Log Backup Procedures

Logs of the signing machine are copied weekly to a removable media and kept in a safe.

Information kept on the on-line repository is copied daily to a NAS server.

4.5.6 Audit Collection System (Internal vs. External)

The audit record collection process is done under the control of the CA operators.

4.5.7 Notification to Event-causing Subject

The subject who caused an audit event to occur is not notified of the audit action.

4.5.8 Vulnerability Assessments

No stipulation.

4.6 Records Archival

4.6.1 Types of Event Recorded

See Section 4.5.1.

4.6.2 Retention Period for Archives

See Section 4.5.3.

4.6.3 Protection of Archive

See Section 4.5.4

4.6.4 Archive Backup Procedures

See Section 4.5.5.

4.6.5 Requirements for Time-stamping of Records

No stipulation.

4.6.6 Archive Collection System (Internal or External)

See Section 4.5.6.

4.6.7 Procedures to Obtain and Verify Archive Information

No stipulation.

4.7 Key Changeover

A new CA self-signed certificate is generated at least one year before the expiry of the old one. 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 by the associated private key also have expired.
The CA certificate will have a validity period of ten 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 it will be replaced as soon as possible using the backup copies available on-site and off-site.

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 CA's;
2. terminate the certificates and CRL distribution services for certificates and CRL's 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 re-certify, following the initial identification procedures defined in Section 4.1.

4.8.4 Secure Facility After a Natural or Other Type of Disaster

Backup copies are kept in an off-site location, so it should be possible to restart CA operations.

4.9 CA Termination

At least 60 days before INFN CA terminates its services, it will:

1. inform subscribers (by electronic messages) and cross-certifying CA's;
2. make widely available information of its termination;

3. stop issuing certificates and CRL's.

The CA manager will be responsible for the archival of records as per Section 4.6.

5. Physical, Procedural and Personnel Security Controls

5.1 Physical Security Controls

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

5.1.1 Site Location and Construction

The CA is housed in the Physics Department in the 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 manager and CA operators only.

The on-line repository is located in a computer room whose access is restricted to authorized people only: CA and Computing Service personnel only.

5.1.3 Power and Air Conditioning

The building has an air conditioning system and the on-line repository is connected to an UPS system.

5.1.4 Water Exposures

The building is at the first floor of the building and in a zone not subject to floods.

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

Critical files are backed up at an off-site location.

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:
- controls private key generation for robot certificates

5.2.2 Number of Persons Required per Task

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

5.2.3 Identification and Authentication for Each Role

No stipulation.

5.3 Personnel Security Controls

5.3.1 Background, Qualifications, Experience, and Clearance Requirements

CA management is done by trained persons, well aware of the necessary security requirements.

RA must be familiar with their tasks and be aware of the security implications of their activities. Periodical instruction seminars are kept by CA personnel.

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

In case of unauthorized actions by a CA or RA operator, the CA manager may revoke the privileges concerned.

5.3.7 Contracting Personnel Requirements

No stipulation.

5.3.8 Documentation Supplied to Personnel

The CA manager will supply the CA and RA operators with a copy of this document.

The CA operator has access to the on-line documentation of the CA procedures on the INFN CA internal wiki.

6. Technical Security Controls

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

Keys for the INFN 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 own key pair.

6.1.2 Private Key Delivery to Entity

No delivery of private keys is allowed. INFN CA doesn't generate private keys for its subjects.

6.1.3 Public Key Delivery to Certificate Issuer

Entities' public keys are delivered to the CA in a secure and trustworthy manner: by on-line SSL transaction for personal and robot certificates, by signed e-mail for server and service certificates.

6.1.4 CA Public Key Delivery to Users

CA certificate is available from its web site and from TACAR repository.

6.1.5 Key Sizes

Minimum key length is 1024.

The CA key is of 2048 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

If the key pair is associated to a robot certificate, it must be kept in a secure hardware token, and must be generated in it. In the other cases, key may be generated as software tokens.

6.1.9 Key Usage Purposes

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

The INFN CA private key is the only one that can be used for signing Certificates and CRL's.

The Certificate *keyUsage* field is used in accordance with RFC3280 [RFC3280].

6.2 Private Key Protection

CA private key is kept on removable media and kept in a safe.

Subscribers must adequately protect the private keys of the certificates issued to them. The required level of protection depends on the type of certificate:

- **personal**: the key must be stored in encrypted form with a sufficiently strong pass phrase, with appropriate file system protections and not in a network shared file system; alternatively the key may be stored in an hardware token as described in Section 6.2.1;
- **host or service**: the key may be stored in unencrypted form, with appropriate file system protections and not in a shared file system; alternatively the key may be stored in an hardware token as described in Section 6.2.1;
- **robot**: the key must be generated and stored in an hardware token as described in Section 6.2.1.

6.2.1 Standards for Cryptographic Module

A secure hardware token must comply with the requirements of at least FIPS 140-1 level 2, FIPS 140-2 level 2 or equivalent.

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

Private keys pertaining to personal certificate must not be under multi-person control.

CA private key is not under multi-person control.

6.2.3 Private Key Escrow

Private keys must not be escrowed.

6.2.4 Private Key Backup

INFN CA private key is kept, encrypted, in multiple copies and in different locations, on removable media.

6.2.5 Private Key Archival

Backup copies can be used as an archival service.

6.2.6 Private Key Entry into Cryptographic Module

Apart for robot certificates, private keys may be uploaded into an hardware token.

6.2.7 Method of Activating Private Key

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

6.2.8 Method of Deactivating Private Key

The pass phrase of the CA private key is kept only in the memory of the signing machine, which is powered off at the end of each signing session.

6.2.9 Method of Destroying Private Key

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

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

INFN CA certificate has a validity of ten years. Subscribers' certificates have a validity of at most one year.

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

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

6.4.2 Activation Data Protection

The pass phrase of the CA private key is kept in a sealed envelope kept in an off-site safe.

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 a suitably configured firewall.

The machine used for signing certificates isn’t connected to any kind of networks.

6.5.2 Computer Security Rating

No stipulation.

6.6 Life-Cycle Security Controls

6.6.1 System Development Controls

INFN CA uses public domain 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:

X.509 v3.

7.1.2 Certificate extensions

Subscriber certificates contain the following extensions (not critical, unless explicitly stated):

Basic Constraints (CRITICAL)
CA:FALSE

Key Usage (CRITICAL)
Digital Signature, Key Encipherment, Data Encipherment

ExtendedKeyUsage
people: *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)*
object-signing: *1.3.6.1.5.5.7.3.3 (Signing of downloadable executable code)*
digital processing entity: *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), msSGC,nsSGC*
service: *serverAuth,clientAuth,msSGC,nsSGC*
robot:: none

Certificate Authority Key Identifier
Directory Address: `C=IT,O=INFN,CN=INFN Certification Authority`
Serial Number: `B3:26:02:C6:7D:49:26:27`

Subject Alternative Name
people: *subject's e-mail address*
object-signing: *subject's e-mail address*
digital processing entity: *one or more FQDN and one e-mail address*
service: *server FQDN and one e-mail address*
robot: *subject's e-mail address*

CRL Distribution Points
`URL=http://security.fi.infn.it/CA/INFN-CA-2015.crl`

Certificate Policies
one or more OID's, one referring to this CP/CPS

The CA certificate contains the following extensions (not critical, unless explicitly stated):

Basic Constraints (CRITICAL)
CA:TRUE

Key Usage (CRITICAL)
Certificate Sign, CRL Sign

7.1.3 Algorithm Object Identifiers

Subject Public Key Algorithm: RSA Encryption (1.2.840.113549.1.1)
Certificate Signature Algorithm: SHA256 With RSA Encryption

7.1.4 Name forms

Subject certificates:

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

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

countryName: `IT`

organizationName: `INFN`

organizationalUnitName:
people: `Personal Certificate`
object-signing: `Objsign`
digital processing entity: `Host`
service: `Service`
robot: `Robot`

localityName:
the Structure where the RA is appointed;

commonName:
people: requester's full name;
object-signing: requester's full name;
digital processing entity: a Fully Qualified Domain Name
service: the service name, '/', a Fully Qualified Domain Name
robot: '`Robot:` ', *robot's function*, '-', *requester's full name*

CA certificate:

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

Subject: `C=IT,O=INFN,CN=INFN Certification Authority`

7.1.5 Name Constraints

No stipulation.

7.1.6 Certificate Policy Object Identifier

Certificates contain in the Certificate Policy extension one or more OID's, one of them referring to this document (see Section 1.2).

7.1.7 Usage of Policy Constraints Extensions

No stipulation.

7.1.8 Policy Qualifier Syntax and Semantics

The qualifier is a pointer to this document, in the form of an URL.

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

8. Specification Administration

8.1 Specification Change Procedures

Relevant CPS changes will be announced to the RA, published on the CA web site and submitted to the EuGridPMA.

Minor changes will only be announced on the CA web site.

8.2 Publication and Notification Procedures

The policy and all previous versions are available at **http://security.fi.infn.it/CA/CPS**.

8.3 CPS Approval Procedures

The CA manager approves the CP/CPS.

Bibliography

[FBCA] *X.509 Certificate Policy For The Federal Bridge Certification Authority (FBCA)*, Version 1.0, 18 December 1999.

[HEPKI] David Wasley, *HEPKI Model Campus Certificate Policy***,** October 2002.

[NCSA] National Computational Science Alliance, *Certificate Policy, Version 0.9.1*, June 30, 1999**.**

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

[RFC2527] S. Chokani and W. Ford, *Internet X.509 Infrastructure Certificate Policy and Certification Practices Framework*, RFC 2527.

[**TrustID]** *TrustID Certificate Policy,* Version 1.2, June 2005.

[UKeS] *UK e-Science Certification Authority Certificate Policy and Certification Practices Statement*, Version 1.4, November 2007.

[DGri] *DutchGrid and NIKHEF medium-security X.509 Certification Authority Certification Policy and Practice Statement*, Version 3.0, April 2007.

List of changes

VERSION	DATE	CHANGES
0.1	February 2001	Initial Release
0.2	February 2001	Better compliance to RFC2527
0.3	March 2001	Better clarification of **Name Forms** (**7.1.4**)
1.0	December 2001	Better compliance to RFC2527 Specification of the document OID
1.1	January 2003	New root certificate Eliminated the paragraph on possible future access restrictions (2.6.3)
2.0	December 2003	Proper RA are required for identity checking and authorization
2.1	March 2004	Certificates can be issued for services
2.2	November 2006	New INFN CA root certificate: • Netscape revocation URL eliminated (4.4.13) • CA cert validity changed to ten years (4.7) • Netscape extensions eliminated (7.1.2) • New issuer: **C=IT, O=INFN, CN=INFN CA** (7.7.14)
2.3	February, 12 2008	More detailed descriptions of CA operation Robot certificates.

VERSION	DATE	CHANGES
2.3.1	February, 28 2008	The challenge email for server or service certificates is always sent (4.1)
2.4	November, 1 2015	New Root certificate