INFN CA
Certificate Policy and Certification Practice Statement

Version 0.3 (DRAFT)

March 2001

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

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

More details can be found at **http://security.fi.infn.it/CA/CPS/**

Contents

1. Introduction

1.1 Overview

This document is a **draft**, structured according to RFC 2527 [RFC2527]

This document describes the set of rules used by INFN CA, the top level Certification Authority for the *Istituto Nazionale di Fisica Nucleare* (INFN, http://www.infn.it/).

1.1.1 General Definitions

The document makes use of 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
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.

Official INFN e-mail address
An e-mail address of the form: [**name.**]**surname@city**`.infn.it` (e.g. `Paolo.Rossi@fi.infn.it` or `bianchi@fi.infn.it`).

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.

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.

1.2 Identification

Document title:
INFN CA Certificate Policy and Certification Practice Statement

Document version:
0.2

Document date:
February 2001.

1.3 Community and Applicability

1.3.1 Certification Authorities

No stipulation.

1.3.2 Registration Authorities

INFN CA manages the functions of its Registration Authority.

1.3.3 End Entities

INFN CA issues certificates for:

- INFN employees;
- INFN fellows;
- Servers owned by INFN or used for activities in which INFN is involved.

1.3.4 Applicability

Certificates issued are of the following types:

- **personal**: for e-mail signing and encryption (S/MIME);
- **server**: for server certification and encryption of communications (SSL/TSL);
- object-signing.

1.4 Contact Details

INFN CA is managed by the *INFN Security Group* (http://security.fi.infn.it/).

Contact person for questions related to this document or the INFN CA in general:

Roberto Cecchini
INFN CA
c/o INFN, Sezione di Firenze
L.go E. Fermi 2
I 50125 Firenze

phone: +39 0552307696
fax: +39 055229330
e-mail: infn-ca@fi.infn.it

2. General Provisions

2.1 Obligations

2.1.1 CA and RA Obligations

INFN CA will:

- accept certification requests from entitled entities;
- authenticate entities according to the procedures outlined in this document;
- issue certificates based on the requests from authenticated entities;
- notify the subscriber of the issuing of the certificate;
- publish the issued certificates;
- accept revocation requests according to the procedures outlined in this document;
- authenticate entities requesting the revocation of a certificate;
- issue a Certificate Revocation List (CRL);
- publish the CRL issued.

2.1.2 Subscriber Obligations

Subscribers must:

- read and adhere to the procedures published in this document;
- generate a key pair using a trustworthy method;
- take reasonable precautions to prevent any loss, disclosure or unauthorized use of the private key associated with the certificate, including:
  - selecting a passphrase of at minimum 8 characters
  - protecting the passphrase from others
- authorize the treatment and conservation of personal data;
- notify immediately INFN CA in case of private key lost or compromised.

2.1.3 Relying Party Obligations

Relaying parties must:

- read the procedures published in this document;
- verify the CRL before validating a certificate;
- use the certificates for the permitted uses only.

2.1.4 Repository Obligations

INFN CA will publish on its web server (http://security.fi.infn.it/CA) certificates and CRLs as soon as issued.

2.2 Liability

INFN CA only guarantees to control the identity of the subjects requesting a certificate according to the practices described in this document. No other liability, implicit or explicit, is accepted.

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. It doesn't warrant its procedures and it will take no responsibility for problems arising from its operation, or for the use made of the certificates it provides.

INFN CA denies any financial or any other kind of responsibilities for damages or impairments resulting from its operation.

2.3 Financial Responsibility

No financial responsibility is accepted.

2.4 Interpretation and Enforcement

2.4.1 Governing Law

Interpretation of this policy is according to Italian laws.

2.5 Fees

No fees are charged.

2.6 Publication and Repositories

2.6.1 Publication of CA information

INFN CA operates a secure online repository that contains:

- INFN CA's certificate;
- certificates issued;
- a Certificate Revocation List;
- a copy of this policy
- other relevant information.

2.6.2 Frequency of Publication

Certificates will be published as soon as issued.

CRLs will be published as soon as issued and at least every month.

2.6.3 Access Controls

The online repository is available on a substantially 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 and issued certificates and CRLs.

In the future, INFN CA may impose access controls on issued certificates, their status information and CRLs at its discretion, subject to agreement between the CA, relying parties and subscribers.

2.6.4 Repositories

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

2.7 Compliance Audit

No stipulation.

2.8 Confidentiality

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

Information included in issued certificates and CRLs is **not** considered confidential.

INFN CA doesn't collect any kind of confidential information.

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

2.9 Intellectual Property Rights

Parts of this document are inspired by [EuroPKI], [TrustID] , [NCSA] and [FBCA].

3. Identification and Authentication

3.1 Initial Registration

3.1.1 Types of names

The subject name is of the X.500 name type. It has one of the following forms:

- **Person**.
  F*ull name* of the subject and his/her *official INFN e-mail address*.
- **Server**.
  Server DNS name and the e-mail address of the person in charge of the machine.

3.1.2 Name Meanings

The Subject Name in a certificate must have a reasonable association with the authenticated name of the subscriber.

3.1.3 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.

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

3.1.4 Method to Prove Possession of Private Key

No stipulation.

3.1.5 Authentication of Organization Identity

No stipulation.

3.1.6 Authentication of Individual Identity

Procedures differ if the subject is a person or a server.

- **Person** (listed in the official INFN Phonebook).
  INFN CA staff calls the subject by phone and check if the request was from him/her.
  The authentication procedure fails after five days of unsuccessful attempts.

- **Person** (not listed in the official INFN Phonebook).
  The request **must** be accompanied by an e-mail to **infn-ca@fi.infn.it**, **signed by a valid INFN CA certificate**, certifying the identity of the subject.
- **Server**.
  Requests **must** be signed with a valid personal INFN CA certificate.

3.2 Routine Rekey

Rekeying of certificates of persons **before their expiration** can requested by an online procedure, which checks the validity of the subject's certificate. No other checks are performed.

Rekeying of expired certificates or server certificates follows the same rules as an initial registration.

3.3 Rekey After Revocation

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

3.4 Revocation Request

Certificate revocation requests must be sent by e-mail, **signed by a valid INFN CA certificate**, to **infn-ca@fi.infn.it**. If this isn't possible, INFN CA staff checks with the same procedure used for the authentication of identity of a person.

4. Operational Requirements

4.1 Certificate Application

Procedures are different if the subject is a person or a server. **In every case the subject has to generate his/her own key pair.**

Minimum key length is 512 bits, recommended length is 1024 bits.

- **Person**.
  Certificate requests are submitted by an online procedure, using a Netscape or Internet Explorer browser.
  Access to the procedure is restricted to nodes belonging to **infn.it** domain.
- **Server**.
  Certificate requests are sent by e-mail to **infn-ca@fi.infn.it** and **must be signed by a valid INFN CA certificate**.
  A configuration file for OpenSLL/SSLeay is available from the INFN CA web server. *Non conforming requests aren't accepted.*
  If the e-mail address in the request doesn't belong to a person that owns a valid INFN-CA certificate, an e-mail with a request of confirmation is sent to that address (to check if it is valid). The certificate application is not valid until reception of the confirmation.

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 person, a message is sent to his/her official INFN e-mail address with the instructions on how to download it from the INFN CA web server. In the other case the certificate itself 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.

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 no longer needs the certificate to access Relaying Parties' resources;
- the subscriber violated his/her obligations.

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 the private key compromise or of the variation of subscriber's data.

4.4.3 Procedure for Revocation Request

The entity requesting the revocation must authenticate itself in one of the following ways:

- sending an e-mail, signed by a valid INFN CA certificate, to **infn-ca@fi.infn.it**;
- in the other cases, INFN CA staff checks with the same procedure used for the authentication of identity of a person.

4.4.4 Circumstances for Suspension

No stipulation.

4.4.5 Who Can Request Suspension

No stipulation.

4.4.6 Procedure for Suspension Request

No stipulation.

4.4.7 Limits on Suspension Period

No stipulation.

4.4.8 CRL Issuance Frequency

CRLs are issued after every certificate revocation or every month.

4.4.9 Online revocation/status checking availability

An online procedure for status checking is available.

4.4.10 Online revocation checking requirements

No stipulation.

4.4.11 Other forms of revocation advertisement available

No stipulation.

4.5 Security Audit Procedures

4.5.1 Types of Event Audited

The following events are audited:

- certification requests;
- issued certificates;
- issued CRLs;

4.5.2 Retention period for Audit Logs

Minimum retention period is three years.

4.6 Records Archival

4.6.1 Types of Event Recorded

The following events are recorded and archived

- certification requests;
- issued certificates;
- issued CRLs;
- all e-mail messages sent to INFN CA;
- all e-mail messages sent by INFN CA.

4.6.2 Retention Period for Archives

Minimum retention period is three years.

4.7 Key Changeover

No stipulation.

4.8 Compromise and Disaster Recovery

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

1) inform subscribers and cross-certifying CAs;

2) terminate the certificates and CRL distribution services for certificates and CRLs issued using the compromised key.

4.9 CA Termination

Before INFN CA terminates its services, it will:

1) inform subscribers and cross-certifying CAs;

2) make widely available information of its termination;

3) stop issuing certificates and CRLs.

5. Physical, Procedural and Personnel Security Controls

5.1 Physical Security Controls

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

5.2 Procedural Controls

No stipulation.

5.3 Personnel Security Controls

No stipulation.

6. Technical Security Controls

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

Each entity must generate its key pair. *INFN CA doesn't generate private keys for its subjects.*

6.1.2 Private Key Delivery to Entity

No stipulation.

6.1.3 Public Key Delivery to Certificate Issuer

Entities' public keys are delivered to the issuing CA in a secure and trustworthy manner: by SSL for personal certificates and by signed e-mail for server certificates.

6.1.4 CA Public Key Delivery to Users

CA certificate is delivered by an online transaction from a secure web server.

6.1.5 Key Sizes

Keys of length inferior to 512 bits are not accepted, recommended length is 1024 bits.

6.1.6 Public Key Parameters Generation

No stipulation.

6.1.7 Parameter Quality Checking

No stipulation.

6.1.8 Hardware/Software Key Generation

No stipulation.

6.1.9 Key Usage Purposes

Keys may be used for authentication, non-repudiation, data encipherment, message integrity and session key establishment.

INFN 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 [RFC2459]

6.2 Private Key Protection

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

No stipulation.

6.2.2 Private Key Escrow

No stipulation.

6.2.3 Private key Archival and Backup

INFN CA private key is kept, encrypted, in multiple copies and in different locations, on CD-ROMs. For emergencies, the passphrase is in a sealed envelope kept in a safe.

6.3 Other Aspects of Key Pair Management

INFN CA certificate has a validity of three years.

6.4 Activation Data

INFN CA private key is protected by a passphrase.

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 and applicable 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.

6.5.2 Computer Security Rating

No stipulation.

6.6 Life-Cycle Security Controls

No stipulation.

6.7 Network Security Controls

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

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

Basic Constraints (CRITICAL)
not a CA.

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

Subject Key Identifier

Authority Key Identifier

Subject Alternative Name
Subject's e-mail address

Issuer Alternative Name

CRL Distribution Points

Certificate Policies

Netscape Cert Type

Netscape Comment

Netscape Base Url

Netscape Revocation Url

Netscape Renewal Url

Netscape CA Policy Url

7.1.3 Algorithm object identifiers:

No stipulation.

7.1.4 Name forms:

Issuer: `C=IT, O=INFN, OU=Authority, CN=INFN CA (2)`

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

countryName:
"`IT`"

organizationName:
"`INFN`" or the organization which owns the server;

organizationalUnitName:
"`Person`" (for personal certificates);

"`Object Signer`" (for object-signing certificates)
use (for server certificates);

localityName:
the city/laboratory where the subject resides;

commonName:
name and surname (personal and object–signing certificates) or DNS name (server certificates) and e-mail address of the subject (personal and object-signing certificates) or of the manager (server certificates).

7.1.5 Name Constraints

No stipulation.

7.1.6 Certificate Policy Object Identifier

No stipulation.

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.

7.2 CRL Profile

7.2.1 Version

X.509 v1.

Version 1 is required for compatibility with Netscape Communicator.

7.2.2 CRL and CRL Entry Extensions

No stipulation

8. Specification Administration

8.1 Specification Change Procedures

Users will not be warned in advance of changes to INFN CA's policy and CPS.

8.2 Publication and Notification Procedures

The policy is available at http://security.fi.infn.it/CA/policy.html.

8.3 CPS Approval Procedures

No stipulation.

Bibliography

[EuroPKI] - EuroPKI Certificate Policy, Version 1.1 (Draft 4), October 2000 11

[FBCA] - X.509 Certificate Policy For The Federal Bridge Certification Authority (FBCA), Version 1.0, 18 December 1999 11

[NCSA] - National Computational Science Alliance, Certificate Policy, Version 0.9.1, June 30, 1999 11

[OpenSSL] - http://www.openssl.org/ 12

[RFC2459] - R. Housley, W. Ford, W. Polk and D. Solo, Internet X.509 Public Key Infrastructure Certificate and CRL Profile, RFC 2459, January 1999 16

[RFC2527] - S. Chokani and W. Ford, Internet X.509 Infrastructure Certificate Policy and Certification Practices Framework, RFC 2527, March 1999 7

[TrustID] - TrustID Certificate Policy http://www.digsigtrust.com/certificates/policy/tsindex.html 11

List of changes

VERSION	DATE	CHANGES
0.1	February 2001	Initial Release
0.2	February 2001	Better compliance to RFC 2527
0.3	March 2001	Better clarification of **Name Forms** (**7.1.4**)