INFN CA Certificate Policy and Certification Practice Statement

Version 2.0

December 2003

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

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
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.

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:
2.0

Document date:
December 2003

Object Identifier assigned:
1.3.6.1.4.1.1043.10.1.3

1.3 Community and Applicability

1.3.1 Certification Authorities

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

1.3.2 Registration Authorities

INFN CA deletages identification and authorization of certificate subjects to trusted indivuals (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 End Entities

INFN CA issues certificates for:

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

1.3.4 Applicability

Certificates issued can be used for:

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

1.4 Contact Details

1.4.1 Specification Administration Organization

The Policy Management Authority (PMA) for this CP is the *INFN Security Group* (http://security.fi.infn.it/).

1.4.2 Contact person

The primary contact for this PMA is

Roberto Cecchini
INFN CA
c/o INFN, Sezione di Firenze
Via 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

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

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.

Its obligations include:

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

2.1.2 RA Obligations

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

Their obligations include:

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

2.1.3 Subscriber Obligations

Subscribers must:

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

2.1.4 Relying Party Obligations

Relaying parties must:

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

2.1.5 Repository Obligations

INFN CA will make available online on its web server and its Lightweight Directory Access Protocol (LDAP) server the certificates and CRLs, as soon as issued.

2.2 Liability

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

In particular 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.

2.2.1 CA Liability

Cf. section 2.2.

2.2.2 RA Liability

Cf. section 2.2.

2.3 Financial Responsibility

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

Interpretation of this CP and CPS is the responsibility of the PMA identified in section 1.4.1 above.

2.4.1 Governing Law

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

2.4.2 Severability, Survival, Merger, Notice

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

2.4.3 Dispute Resolution Procedures

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

2.5 Fees

No fees are charged.

2.5.1 Certificate Issuance or Renewal Fees

No stipulation

2.5.2 Certificate Access Fees

No stipulation

2.5.3 Revocation or Status Information Access Fees

No stipulation

2.5.4 Fees for Other Services such as Policy Information

No stipulation

2.5.5 Refund Policy

No stipulation

2.6 Publication and Repositories

2.6.1 Publication of CA Information

INFN CA operates a secure online repository that contains:

- INFN CA's certificate;
- Issued certificates;
- the 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 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 online repository is available on a 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 CRLs.

2.6.4 Repositories

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

2.7 Compliance Audit

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

2.7.1 Frequency of Entity Compliance Audit

No stipulation.

2.7.2 Identity/Qualifications of Auditor

No stipulation.

2.7.3 Auditor's Relationship to Audited Party

No stipulation.

2.7.4 Topics Covered by Audit

No stipulation.

2.7.5 Actions Taken as a Result of Deficiency

No stipulation.

2.7.6 Communication of Results

No stipulation.

2.8 Confidentiality

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*.

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

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

2.8.2 Types of Information Not Considered Confidential

Information included in issued certificates and CRLs 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

Cfr section 8.3.

2.8.5 Release as Part of Civil Discovery

Cf. section 8.3

2.8.6 Disclosure Upon Owner's Request

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

2.8.7 Other Information Release Circumstances

No stipulation.

2.9 Intellectual Property Rights

Parts of this document are inspired by [EuroPKI], [TrustID] , [NCSA] , [HEPKI] 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:

- **Natural Person:**
  f*ull name* of the subject and his/her e-mail address;
- **Digital Processing Entity:**
  Fully Qualified Domain Name as registered in the DNS and the e-mail address of the person in charge.

3.1.2 Need for Names to Be Meaningful

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

3.1.3 Rules for Interpreting Various Name Forms

Cfr. 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.

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

3.1.5 Name Claim Dispute Resolution Procedure

The PMA 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

The request of a 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 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, csr generation, and submission stages. No proof of possession of private key test is made in these cases.

Renewal function employ a proof of possession of private key.

3.1.8 Authentication of Organization Identity

No stipulation.

3.1.9 Authentication of Individual Identity

- **Natural Person**: the subscriber is authenticated *personally* by the RA using a valid photo ID document.
- **Digital Processing Entity:** the requestor 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 verifying the correctness of the request.

3.2 Routine Rekey

Rekey of certificates of natural persons before the expiration can be requested by an online procedure, which checks the validity of the subject's certificate. The certificate is issued after the approval by the pertinent RA.

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

3.3 Rekey After Revocation

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

3.4 Revocation Request

Certificate revocation requests must be sent by **signed** e-mail.

4. Operational Requirements

4.1 Certificate Application

Procedures are different if the subject is a person or a Digital Processing Entity. **In every case the subject has to generate his own key pair.**

Minimum key length is 1024 bits.

- **Natural person**.
  Before submitting the request the user must be authenticated by an RA. During the authentication a random number is generated, which is comunicated to the user and to the CA (by secure means) together with the user's affiliation, name and e-mail address. The certificate request is then submitted by the user via an online procedure, which requires the same data specified during the authentication, including the authorization number.The request is considered valid if the information supplied by the user coincides with that received at the end of the authentication phase
- **Digital Processing Entity**.
  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 requestor to obtain the certificate and then forwards the request to the INFN CA by a a signed e-mail.
  A configuration file for OpenSLL/SSLeay is available from the INFN CA web server.
  If the e-mail address specified in the request doesn't belong to the person who signed it, 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 natural person, a message is sent to his 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.

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

4.4.2 Who Can Request Revocation

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

4.4.3 Procedure for Revocation Request

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

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

4.4.4 Revocation Request Grace Period

There is no revocation grace period.

4.4.5 Circumstances for Suspension

There is no provision for certificate suspension.

4.4.6 Who Can Request Suspension

Not applicable.

4.4.7 Procedure for Suspension Request

Not applicable.

4.4.8 Limits on Suspension Period

Not applicable.

4.4.9 CRL Issuance Frequency

CRLs are issued after every certificate revocation or at least every month.

4.4.10 CRL Checking Requirements

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

4.4.11 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

Netscape Revocation URL.

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 Audited

The following events are audited:

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

4.5.2 Frequency of Processing Log

Audit logs will be reviewed at least weekly.

4.5.3 Retention Period for Audit Logs

Minimum retention period is three years.

4.5.4 Protection of Audit Log

Only authorized people have access to the logs.

4.5.5 Audit Log Backup Procedures

Logs are copied monthly to removable media and encrypted with a passphrase of suitable length.

4.5.6 Audit Collection System (Internal vs. External)

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

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

The following events are recorded and archived

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

4.6.2 Retention Period for Archives

Minimum retention period is three years.

4.6.3 Protection of Archive

Archives are backed up on removable media, which are stored in a room with restricted access.

4.6.4 Archive Backup Procedures

See Section 4.6.3

4.6.5 Requirements for Time-stamping of Records

No stipulation.

4.6.6 Archive Collection System (Internal or External)

See Section 4.6.3

4.6.7 Procedures to Obtain and Verify Archive Information

No stipulation.

4.7 Key Changeover

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

4.8 Compromise and Disaster Recovery

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

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

4.8.2 Entity Public Key is Revoked

See Section 4.8.3.

4.8.3 Entity Key is Compromised

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

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

4.8.4 Secure Facility After a Natural or Other Type of Disaster

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

4.9 CA Termination

Before INFN CA terminates its services, it will:

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

5. Physical, Procedural and Personnel Security Controls

5.1 Physical Security Controls

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

5.1.1 Site Location and Construction

The CA is housed in the Physics Department in the Campus at Sesto Fiorentino.

5.1.2 Physical Access

No unauthorized access to the hardware is permitted and all removable media is stored in secure containers.

5.1.3 Power and Air Conditioning

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

5.1.4 Water Exposures

The building is 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 encrypted form in a safe.

5.1.7 Waste Disposal

No stipulation.

5.1.8 Off-site Backup

No stipulation.

5.2 Procedural Controls

5.2.1 Trusted Roles

No stipulation.

5.2.2 Number of Persons Required per Task

No stipulation.

5.2.3 Identification and Authentication for Each Role

No stipulation.

5.3 Personnel Security Controls

Trained persons, well aware of the necessary security requirements, do CA management.

5.3.1 Background, Qualifications, Experience, and Clearance Requirements

No stipulation.

5.3.2 Background check procedures

No stipulation.

5.3.3 Training Requirements

No stipulation.

5.3.4 Retrainig Frequency and Requirements

No stipulation.

5.3.5 Job Rotation Frequency and Sequence

No stipulation.

5.3.6 Sanctions for Unauthorized Actions

No stipulation.

5.3.7 Contracting Personnel Requirements

No stipulation.

5.3.8 Documentation Supplied to Personnel

No stipulation.

6. Technical Security Controls

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

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

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 delivery of private keys is allowed: see Section 6.1.1

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 online transaction from a secure web server for personal certificates and by signed e-mail for server certificates.

6.1.4 CA Public Key Delivery to Users

CA certificate is available from its public repositories.

6.1.5 Key Sizes

Keys of length inferior to 1024 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

Key generation is performed in software.

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 [RFC3280]

6.2 Private Key Protection

6.2.1 Standards for Cryptographic Module

No stipulation.

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

No stipulation.

6.2.3 Private Key Escrow

CA private keys are not escrowed.

6.2.4 Private Key Backup

INFN CA private key is kept, encrypted, in multiple copies and in different locations, on CD-ROMs.

6.2.5 Private Key Archival

Backup copies can be used as an archival service.

6.2.6 Private Key Entry into Cryptographic Module

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

6.2.7 Method of Activating Private Key

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

6.2.8 Method of Deactivating Private Key

No stipulation.

6.2.9 Method of Destroying Private Key

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

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 five years and will expire on 18 September 2007.

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

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

6.4.2 Activation Data Protection

Passphrase 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 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.

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

Software is periodically checked for tampering using strong cryptographic techniques.

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

Basic Constraints (CRITICAL)
not a CA.

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

Subject Key Identifier

Certificate Authority Key Identifier
Directory Address: `C=IT,O=INFN,CN=INFN Certification Authority`
Serial Number: `00`

Subject Alternative Name
people: subject's e-mail address
object-signing: requestor's e-mail address
digital processing entity: FQDN and requestor's e-mail address

Issuer Alternative Name
e-mail address of the CA

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

Certificate Policies
see Section 1.2

Netscape Cert Type
SSL Client Certificate, Email

Netscape Comment
`Issued under INFN CA CP and CPS v` *X.X*`,`
`http://security.fi.infn.it/CA/CPS/`

Netscape Base Url
`http://security.fi.infn.it/`

Netscape Revocation Url
`cgi-bin/check-rev.pl?`

Netscape Renewal Url
`cgi-bin/check-renew.pl?`

Netscape CA Policy Url
`http://security.fi.infn.it/CA/policy.html`

7.1.3 Algorithm Object Identifiers:

Subject Public Key Algorithm: RSA Encryption (1.2.840.113549.1.1)

Certificate Signature Algorithm: MD5 With RSA Encryption (1.2.840.113549.1.1.4)

7.1.4 Name forms:

Issuer: **`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`**;

localityName:
the Structure where the RA is appointed;

commonName:
people: name and surname;
object-signing: name and surname of the requestor;
digital processing entity: a Fully Qualified Domain Name as registered in the DNS.

7.1.5 Name Constraints

No stipulation.

7.1.6 Certificate Policy Object Identifier

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 (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. Relevant changes will be made as widely available as possible.

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 15

[FBCA] - X.509 Certificate Policy For The Federal Bridge Certification Authority (FBCA), Version 1.0, 18 December 1999 15

[HEPKI] HEPKI Campus Certificate Policy**,** Ottobre 2001 15

[NCSA] - National Computational Science Alliance, Certificate Policy, Version 0.9.1, June 30, 1999 15

[OpenSSL] - http://www.openssl.org/ 17

[RFC3280] - R. Housley, W. Polk, W. Ford and D. Solo, Internet X.509 Public Key Infrastructure Certificate and CRL Profile, RFC 3280 23

[RFC2527] - S. Chokani and W. Ford, Internet X.509 Infrastructure Certificate Policy and Certification Practices Framework, RFC 2527, March 199 9

[TrustID] - TrustID Certificate Policy http://www.digsigtrust.com/certificates/policy/tsindex.html 15

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