

ESnet Root CA
Certificate Policy
And
Certification Practice Statement
Version 1.3

September 12, 2003

Table of Contents

Table of Contents.....	2
1 Introduction.....	4
1.1 Overview.....	4
1.1.1 General Definitions.....	4
1.2 Identification.....	6
1.3 Community and Applicability.....	6
1.3.1 Certification Authorities.....	6
1.3.2 Registration Authorities.....	6
1.3.3 End Entities.....	6
1.3.4 Applicability.....	6
1.4 Contact Details.....	6
2 General Provisions.....	6
2.1 Obligations.....	7
2.1.1 CA Obligations.....	7
2.1.2 Subordinate CA Obligations.....	7
2.1.3 Relying Party Obligations.....	7
2.1.4 Repository Obligations.....	7
2.2 Liability.....	8
2.3 Financial Responsibility.....	8
2.4 Interpretation and Enforcement.....	8
2.4.1 Governing Law.....	8
2.5 Fees.....	8
2.6 Publication and Repositories.....	8
2.6.1 Publication of CA information.....	8
2.6.2 Frequency of Publication.....	8
2.6.3 Access Controls.....	8
2.6.4 Repositories.....	8
2.7 Compliance audit.....	9
2.8 Confidentiality.....	9
2.9 Intellectual Property Rights.....	9
3 Identification and Authentication.....	9
3.1 Initial Registration.....	9
3.1.1 Types of names.....	9
3.1.2 Name Meanings.....	9
3.1.3 Uniqueness of names.....	9
3.1.4 Method to Prove Possession of Private Key.....	10
3.1.5 Authentication of Individual Identity.....	10
3.2 Routine Rekey.....	10
3.3 Rekey After Revocation.....	10
3.4 Revocation Request.....	10
4 Operational Requirements.....	10
4.1 Certificate Application.....	10
4.2 Certificate Issuance.....	10
4.3 Certificate Acceptance.....	10
4.4 Certificate Suspension and Revocation.....	10
4.4.1 Circumstances for Revocation.....	10
4.4.2 Who Can Request Revocation.....	10
4.4.3 Procedure for Revocation Request.....	11
4.4.4 Circumstances for Suspension.....	11
4.4.5 CRL Issuance Frequency.....	11

4.4.6	Online Revocation/status checking availability.....	11
4.4.7	Online Revocation checking requirements.....	11
4.4.8	Other forms of revocation advertisement available.....	11
4.5	Security Audit Procedures.....	11
4.6	Records Archival.....	11
4.6.1	Types of Event Recorded.....	11
4.6.2	Retention Period for Archives.....	11
4.7	Key Changeover.....	11
4.8	Compromise and Disaster Recovery.....	12
4.9	CA Termination.....	12
5	Physical, Procedural and Personnel Security Controls.....	12
5.1	Physical Security Controls.....	12
5.2	Procedural Controls.....	12
5.3	Personnel Security Controls.....	12
6	Technical Security Controls.....	12
6.1	Key Pair Generation and Installation.....	12
6.1.1	Key Pair Generation.....	12
6.1.2	Private Key Delivery to Entity.....	13
6.1.3	Public Key Delivery to Certificate Issuer.....	13
6.1.4	CA Public Key Delivery to Users.....	13
6.1.5	Key Sizes.....	13
6.1.6	Public Key Parameters Generation.....	13
6.1.7	Parameter Quality Checking.....	13
6.1.8	Hardware/Software Key Generation.....	13
6.1.9	Key usage Purposes.....	13
6.2	Private Key Protection.....	13
6.3	Other Aspects of Key Pair Management.....	13
6.4	Activation Data.....	13
6.5	Computer Security Controls.....	13
6.5.1	Specific Computer Security Technical Requirements.....	13
6.5.2	Computer Security Rating.....	14
6.6	Life-Cycle Security Controls.....	14
6.7	Network Security Controls.....	14
6.8	Cryptographic Module Engineering Controls.....	14
7	Certificate and CRL Profiles.....	14
7.1	Certificate Profile.....	14
7.1.1	Version number.....	14
7.1.2	Certificate Extensions.....	14
7.1.3	Algorithm Object identifiers.....	14
7.1.4	Name Forms.....	14
7.1.5	Name Constraints.....	14
7.1.6	Certificate Policy Object Identifier.....	14
7.1.7	Usage of Policy Constraints Extensions.....	15
7.1.8	Policy qualifier syntax and semantics.....	15
7.2	CRL Profile.....	15
7.2.1	Version.....	15
7.2.2	CRL and CRL Entry Extensions.....	15
8	Specification Administration.....	15
8.1	Specification Change Procedures.....	15
8.2	Publication and Notification Procedures.....	15
8.3	CPS Approval Procedures.....	15
	Bibliography.....	15
	List of Changes.....	16

1 Introduction

1.1 Overview

This document is structured according to RFC 2527 [RFC2527]. Not all sections of RFC 2527 are used. Sections that are not included have a default value of "No stipulation".

This document describes the set of rules and procedures established by ESnet for the operations of the ESnet Root CA service. ESnet and the data center housing the ESnet Root CA server are located at Lawrence Berkeley National Laboratory, Berkeley, California.

This document will include both the Certificate Policy and the Certification Practice Statement for the ESnet Root CA. The general architecture is a single certificate authority. The certificate authority is a stand-alone self signed CA.

It is the intent of the ESnet Root CA to sign only subordinate CAs.

1.1.1 General Definitions

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).

Certification Authority (CA)

The entity / system that issues X.509 identity certificates (places a subject name and public key in a document and then digitally signs that document using the private key of the CA)

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.

Community RM

One or more RMs that serve multiple, low request rate, sites / Virtual Organizations.

Host Certificate

A Certificate for server certification and encryption of communications (SSL/TSL). It will represent a single machine. Host Certificates are used internally by the PKI service and are not issued to other sites/VOs

Person Certificate

A certificate used for authentication to establish a Grid Person Identity. It will represent an individual person.

Policy Management Authority (PMA)

For the DOEGrids PKI this is a committee composed of the CA managers and representatives from the site/VO Registration Authorities. The PMA has direct responsibility for the CP/CPS and oversight of ESnet operations of the PKI.

Policy Qualifier

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

Point of Contact

The member of a site/VO RA that has been chosen to handle all communications about policy matters with the DOE GRIDS PMA.

Private RM

RMs that serve high certificate request rate sites / Virtual Organizations, and that are operated by the site/VO.

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).

Registration Agent (RAg) or “Agent”

RAg is the entity that interacts with the RM in order to cause the CA to issue certificates.

Registration Manager (RM)

The RM is a front-end Web server for the CA that provides a Web user interface for CA subscribers and agents. The RM forwards certificate-signing requests to the actual CA (DOE GRIDS) to issue X.509 certificates.

Relying Party

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

Service Certificate

A certificate for a particular service running on a host. It will represent a single service on a single host.

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.

Subscriber

Or sometimes called End Entity is the person who applied for and was issued a certificate.

Virtual Organization (VO)

An organization that has been created to represent a particular research or development effort independent of the physical sites that the Scientist or Engineers work at. (i.e. PPDG, FNC, EDG, etc).

1.2 Identification

Document title:
ESnet Root CA Certificate Policy and Certification Practice Statement

Document version:
1.3

Document date:
September 12, 2003

OID: 1.2.840.113612.4.3 #d1b603c3 ESnet root

1.3 Community and Applicability

1.3.1 Certification Authorities

ESnet will manage and operate the ESnet Root CA. This CA is never on a computer network. When not in use to sign certificates or CRL's, the CA is offline, with components stored in a highly secured location. Access to CA services is by console only. All data transferred to or from the CA host will be done by removable media. The private key of the CA will be managed by a FIPS 140 level 3 compliant device.

1.3.2 Registration Authorities

The ESnet PKI security officers will act as the Root CA RAs and process all subordinate CA signing requests.

1.3.3 End Entities

This CA issues a few service and administrator certificates for its own internal use. No end entity certificates for use by the public are issued.

1.3.4 Applicability

See section 1.1.1 for definition of certificate types.

Subordinate CA certificates are the only certificates that will be generated by the CA. The subordinate CA certificates are used to establish a PKI. .

1.4 Contact Details

The ESnet Root CA is operated by **ESnet** and managed by ESnet.

Contact person for questions related to this document is:

Tony J. Genovese
One Cyclotron Road, B50A 3131
Berkeley, CA 94706
phone: +1 800 333 7638
e-mail: ESnet-Root-CA-1@es.net

2 General Provisions

2.1 Obligations

2.1.1 CA Obligations

ESnet Root CA will:

- Accept certification requests from entitled entities;
- Issue certificates based on the requests from authenticated entities;
- 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.
- Keep audit logs of the certificate issuance process

2.1.2 Subordinate CA Obligations

The Subordinate CA must:

- Have a valid CP/CPS
- Promise to follow its CPS, and promptly update its CPS document when policies change
- Publish a name and contact information of the party responsible for this subordinate CA
- Maintain a web site and corresponding URL where information about this subordinate CA may be found by the general public
- Provide reasonable proof of right to use trademarked or well-known organizational names or domain identifiers in its subject name

2.1.3 Relying Party Obligations

Relying parties must:

- Read the procedures published in this document;
- Must read and comply with provisions of subordinate CA's CP/CPS.

Relying parties must not:

- Assume any attributes or policies based solely on the subordinate CA being signed by the ESnet Root CA.

Relying parties may:

- The relying party should check that the Subordinate CA certificate is not on the ESnet root CRL.

2.1.4 Repository Obligations

ESnet will provide access to ESnet Root CA information, as outlined in section 2.6.1, on its web site or other participating web sites. The ESnet Root Repository can be found at: www.ES.Net/CA

The following pages deal with individual items from 2.6.1:

ESnet root CA information: http://www.es.net/CA/md5_fingerprint.htm

CRL information PEM:

<http://www.es.net/CA/ESnet%20Root%20CA%201/ESnet%20Root%20CA%201.pem>

CP/CPS: <http://www.es.net/CA/d1b603c3/Certificate%20Policy.pdf>

2.2 Liability

ESnet Root CA only signs subordinate CA certificates according to the practices described in this document. No liability, implicit or explicit, is accepted.

ESnet and its agents make no guarantee about the security or suitability of a subordinate CA that is signed by the ESnet Root CA. The ESnet certification service is run with a reasonable level of security, but it is provided on a *best effort only* basis. It does not 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.

ESnet denies any financial or any other kind of responsibility 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

This policy is subordinate to all applicable U.S. government laws, as well as Department of Energy (DOE) orders.

2.5 Fees

No fees are charged for Certificates issued by this service. All costs for operation are covered directly or indirectly by DOE.

2.6 Publication and Repositories

2.6.1 Publication of CA information

ESnet Root CA will operate a secure online repository that contains:

- Esnet Root CA's certificate;
- Certificates issued by the PKI;
- A Certificate Revocation List;
- A copy of this policy
- Other information deemed relevant to the ESnet Root CA service.

2.6.2 Frequency of Publication

- Certificates will be published to the ESnet Root CA repository as soon as issued.
- CRLs will be published as soon as issued or refreshed once every six months if there are no changes.

2.6.3 Access Controls

The online repository is available on a substantially 24/7 basis, subject to reasonable scheduled maintenance.

The ESnet Root Ca service does not impose any access control on its Policy, its signing Certificate and issued certificates, and its CRLs.

2.6.4 Repositories

Repository of certificates and CRLs can be found at: www.ES.Net/CA.

2.7 Compliance audit

The ESnet Root CA service is not currently audited by an outside party. The CA operation may be reviewed by any cross certifying organization or potential relying organization if approved by the PMA.

2.8 Confidentiality

The ESnet Root CA service collects information about the subordinate CA.

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

The ESnet Root CA service does not collect any kind of confidential information.

The ESnet Root CA service does not have access to or generate the private keys of a subordinate CA key pair. These key pairs are generated and managed by the requesting CA and are the sole responsibility of the subordinate CA.

2.9 Intellectual Property Rights

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

3 Identification and Authentication

3.1 Initial Registration

3.1.1 Types of names

Names will be consistent with the name requirements specified in RFC3280. See section 7.1.4 for more details.

3.1.2 Name Meanings

The ESnet root CA signs subordinate CA certificates. If these certificates contain names that might reasonably be assumed to be the trademark or well-known nickname of an organization, then the signing requestor must demonstrate that the requestor has a right to make use of this name, and must provide proof that the organization has delegated to ESnet the right to sign a certificate containing this name.

Example: Requestor asks for a certificate with the subject name

“CN=LBL Certificate Authority, OU=LBL Services, DC=LBL, DC=GOV”

Requestor must provide reasonable proof that this organization permits this use of its name. Reasonable proof is subject to negotiation with each site or organization.

ESnet prefers that organizations use domain component naming when appropriate (see example above, as well as the ESnet root CA subject name).

3.1.3 Uniqueness of names

The Distinguished Name must be unique for each subject name certified by the ESnet Root CA service.

3.1.4 Method to Prove Possession of Private Key

No stipulation.

3.1.5 Authentication of Individual Identity

The ESnet Root CA service does not issue End Entity certificates and does not verify individual identities.

3.2 Routine Rekey

No Stipulation

3.3 Rekey After Revocation

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

3.4 Revocation Request

See section 4.4.2 for details on who can request a certificate revocation.

4 Operational Requirements

4.1 Certificate Application

In every case the subordinate CA has to generate its own key pair. Certificate signing requests (CSRs) are submitted by a secure offline procedure. The CSR is sent to the ESnet Root CA service for validation.

4.2 Certificate Issuance

The ESnet Root CA service issues the certificate if, and only if, ESnet has validated the identity of the requestor and the associated CA. A valid CP/CPS must exist before a certificate is issued.

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 subordinate CA private key is lost or suspected to be compromised;
- The information in the subordinate CA certificate is suspected to be inaccurate;
- The subordinate CA no longer needs the certificate to generate EE certificates;
- The subscriber violated his/her own CP/CPS.

4.4.2 Who Can Request Revocation

A request to revoke a subordinate CA certificate can be done by the following entities if they can present reasonable evidence that the private key has been compromised or that the subordinate CA's data is in error: The Holder or owner of the Certificate.

- The RA for the subordinate CA
- The ESnet Root CA managers.
- Any other official entity that is a member of the subordinate CA organization.

The subordinate CA may revoke (or request revocation of) the subordinate CA's own certificate for any reason at any time.

4.4.3 Procedure for Revocation Request

The entity requesting the revocation must authenticate itself to the ESnet Root CA service.

4.4.4 Circumstances for Suspension

The ESnet Root CA does not support Certificate Suspension.

4.4.5 CRL Issuance Frequency

CRLs are issued after every certificate revocation or refreshed once every six months if there are no changes.

4.4.6 Online Revocation/status checking availability

An experimental OCSP service will be made available.

4.4.7 Online Revocation checking requirements

No stipulation.

4.4.8 Other forms of revocation advertisement available

No stipulation.

4.5 Security Audit Procedures

Security Auditing of the ESnet Root CA is not supported.

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 correspondence;

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 subordinate CAs;
2. Terminate the certificates and CRL distribution services for certificates and CRLs issued using the compromised key.

4.9 CA Termination

Before ESnet Root CA terminates its services, it will:

1. Inform subordinate CAs;
2. Make widely available information of its termination;
3. Stop issuing certificates and CRLs.
4. Destroy its private keys and all copies.

5 Physical, Procedural and Personnel Security Controls

5.1 Physical Security Controls

The ESnet Root CA is offline at all times and in a vault when not in use. It is located at Lawrence Berkeley National Laboratory (LBNL) in the ESnet Data Center. The ESnet Data center maintains a limited access procedure keyed to the LBNL badge system. All access to the server is limited to ESnet Security officer and system support staff of ESnet. The Root CA is run on a Sun Solaris system. Security on this system is maintained and configured to highest level provided for by Sun. All security patches will be applied as soon as they are released by Sun and verified by the ESnet support staff.

5.2 Procedural Controls

No Stipulations.

5.3 Personnel Security Controls

All access to the servers and applications that comprise the ESnet Root CA service is limited to ESnet Security officer and the ESnet system support staff.

6 Technical Security Controls

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

Each subordinate CA must generate its own key pair. ESnet Root CA service does not generate private keys.

6.1.2 Private Key Delivery to Entity

The ESnet Root CA service never has access to the subordinate CA private key.

6.1.3 Public Key Delivery to Certificate Issuer

Subordinate CA's public keys are delivered to the issuing CA offline in a secure and trustworthy manner. The procedures for CSR and certificate delivery are subject to negotiation with each requestor.

6.1.4 CA Public Key Delivery to Users

CA certificate is delivered by an out of band secure process.

6.1.5 Key Sizes

It is recommended that Keys of length less than 1024 bits not be signed, but if the organization has a use for shorter insecure keys the request will be reviewed.

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

The ESnet root CA private key will only be used to sign subordinate CAs.
The Certificate key Usage field must be used in accordance with [RFC3280]

6.2 Private Key Protection

The ESnet Root CA Private key is managed by a FIPS 140 Hardware Security module.

6.3 Other Aspects of Key Pair Management

The ESnet Root CA certificate has a validity of **10** years.

6.4 Activation Data

The ESnet Root CA private key is protected by a FIPS 140 compliant device. Access is controlled by smart cards. Access procedures are confidential.

6.5 Computer Security Controls

6.5.1 Specific Computer Security Technical Requirements

The server hosting the CA product is built from a vendor CD with reasonable provenance. No other services or software are loaded or operated on the CA server. The server will

receive occasional patches and other adjustments if the security risk warrants, in the judgement of ESnet staff.

6.5.2 Computer Security Rating

No stipulations.

6.6 Life-Cycle Security Controls

No stipulations.

6.7 Network Security Controls

The Root Certificate Authority will never be connected to a computer network under any circumstances.

6.8 Cryptographic Module Engineering Controls

No stipulations.

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)
CA.

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

7.1.3 Algorithm Object identifiers

No stipulations.

7.1.4 Name Forms

ESnet prefers that organizations use domain component naming.

7.1.5 Name Constraints

Not supported

7.1.6 Certificate Policy Object Identifier

OID: [ESnet].ESnet Root CA.CP

1.2.840.113612.4.3 #d1b603c3 ESnet root

7.1.7 Usage of Policy Constraints Extensions

No stipulated.

7.1.8 Policy qualifier syntax and semantics

Not supported.

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

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

It is expected that, over time, a set of standard policies profiles will emerge, and the ESnet CA will sign some CA's under some well-known policy profile. The ESnet CA may support multiple CP/CPS documents and policy OIDs. Additional policy OIDs will be referenced in this section (but the policies themselves will be described in separate documents).

8.2 Publication and Notification Procedures

The policy is available at: http://www.es.net/CA/d1b603c3/Certificate_policy.pdf

8.3 CPS Approval Procedures

The ESnet PKI PMA is responsible for the CP and CPS. All changes must be approved by the PMA.

Bibliography

[INFN CP] <http://security.fi.infn.it/CA/CPS/> INFN CA Policy and CPS.

[GridCP] <http://gridcp.es.net/> Global Grid Forum CP

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

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

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

[OpenSSL] - <http://www.openssl.org/>

[PAG] American Bar Associations PKI Assessment Guidelines ("PAG")
<http://www.abanet.org/scitech/ec/isc/pag/pag.html>

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

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

[RFC3280] - R. Housley & al, Internet X.509 Public Key Infrastructure
Certificate and Certificate Revocation List (CRL) Profile, RFC 3280,
April 2002 [replaces RFC 2459]

[TrustID] - TrustID Certificate Policy
<http://www.digistrust.com/certificates/policy/tsindex.html>

List of Changes

VERSION	DATE	CHANGES
1.0	January 15, 2003	Initial Release based on INFN CP/CPS
1.1	August 19, 2003	Updated publishing points and OIDs
1.2	August 25, 2003	Edits to allow various subordinate CAs and remove the RA appendix – does not apply to Root CA
1.3	September 12, 2003	Minor edits to clear up anachronisms