

ESnet SSL CA service
Certificate Policy
And
Certification Practice Statement
Version 1.0

June 30, 2004

Table of Contents

- Table of Contents.....2
- 1 Introduction.....3
 - 1.1 Overview3
 - 1.1.1 General Definitions4
 - 1.2 Identification5
 - 1.3 Community and Applicability.....5
 - 1.3.1 Certification Authorities.....5
 - 1.3.2 Registration Authority5
 - 1.3.3 End Entities.....6
 - 1.3.4 Applicability6
 - 1.4 Contact Details.....6
- 2 General Provisions.....6
 - 2.1 Obligations6
 - 2.1.1 CA and RA Obligations.....6
 - 2.1.2 Subscriber Obligations.....7
 - 2.1.3 Relying Party Obligations7
 - 2.1.4 Repository Obligations.....7
 - 2.2 Liability.....8
 - 2.3 Financial Responsibility.....8
 - 2.4 Interpretation and Enforcement8
 - 2.4.1 Governing Law.....8
 - 2.5 Fees8
 - 2.6 Publication and Repositories8
 - 2.6.1 Publication of CA information8
 - 2.6.2 Frequency of Publication8
 - 2.6.3 Access Controls.....8
 - 2.6.4 Repositories.....9
 - 2.7 Compliance audit9
 - 2.8 Confidentiality.....9
 - 2.9 Intellectual Property Rights9
- 3 Identification and Authentication9
 - 3.1 Initial Registration.....9
 - 3.1.1 Types of names9
 - 3.1.2 Name Meanings9
 - 3.1.3 Uniqueness of names.....9
 - 3.1.4 Method to Prove Possession of Private Key.....9
 - 3.1.5 Authentication of Individual Identity10
 - 3.2 Revocation Request.....10
- 4 Operational Requirements10
 - 4.1 Certificate Application10
 - 4.2 Certificate Issuance.....10
 - 4.3 Certificate Acceptance.....10
 - 4.4 Certificate Suspension and Revocation10
 - 4.4.1 Circumstances for Revocation10
 - 4.4.2 Who Can Request Revocation.....10
 - 4.4.3 Procedure for Revocation Request10
 - 4.4.4 Circumstances for Suspension.....10
 - 4.4.5 CRL Issuance Frequency.....11
 - 4.4.6 Online Revocation/status checking availability11
 - 4.5 Security Audit Procedures11

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	11
4.9	CA Termination	11
5	Physical, Procedural and Personnel Security Controls	11
5.1	Physical Security Controls	11
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	12
6.1.3	Public Key Delivery to Certificate Issuer	12
6.1.4	CA Public Key Delivery to Users	12
6.1.5	Key Sizes	12
6.1.6	Key usage Purposes	12
6.2	Private Key Protection	12
6.2.1	Private Key (n out of m) Multi person control	13
6.2.2	Private Key Escrow	13
6.2.3	Private Key Archival and Backup	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
6.6	Network Security Controls	13
7	Certificate and CRL Profiles	13
7.1	Certificate Profile	13
7.1.1	Version number	14
7.1.2	Certificate Extensions	14
7.1.3	Name Forms	14
7.1.4	Certificate Policy Object Identifier	14
7.1.5	Usage of Policy Constraints Extensions	14
7.1.6	Policy qualifier syntax and semantics	14
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

1 Introduction

1.1 Overview

This document describes the set of rules and procedures established by the ESnet Policy management Authority for the operations of the ESnet SSL CA service. ESnet operates the ESnet Public Key infrastructure under the authority of the ESnet PMA.

ESnet will operate the ESnet SSL CA and maintain it in the ESnet data center located at Lawrence Berkeley National Laboratory, Berkeley, California.

This document will include both the Certificate Policy and the Certification Practice Statement for the ESnet SSL CA. The ESnet SSL certificate authority is a subordinate of the ESnet root CA.

It is the intent of the ESnet SSL CA to issue host or website certificates for use by DOE or its partner's sites.

The ESnet SSL CA is using a Certificate Authority based on Iplanet Certificate Management System running on a Solaris platform. This configuration directly influences the architecture supported.

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.

Grid Admin

this is a special roll supported by the ESnet SSL CA. A person assigned this roll must be certified by an ESnet RA. This roll has the ability to submit a CSR and approve it.

Host Certificates

these certificates are used by host to establish an SSL session with a remote client. There by providing a certified host identity to its clients.

Person Certificate

A certificate used for authentication to establish a Grid Person Identity. It will represent an individual person. This is also known as a long term certificate. No personal certificates will be issued by this service.

Comment: No person certs? Sounds reasonable, do we want to limit this?

Policy Management Authority (PMA)

For the ESnet PKI this is a committee composed of ESnet staff and invited members.

Policy Qualifier

The 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.

Security Incident

An incident that has the potential of private key loss or compromise, regardless of if the compromise or loss was successful. Such incidents include but are not limited to user credential compromise, privilege escalation on systems known to contain private keys, accidental exposure of private keys to unauthorized third parties or loss of a private key.

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.

1.2 Identification

Document title:

ESnet SSL CA Certificate Policy and Certification Practice Statement

Document version:

1.0

Document date:

June 30, 2004.

OID: [ESnet].ERmember.DOEGrids.Security.CP

1.2.840.113612.3.7. ~~XX~~

Comment: Need new OID

1.3 Community and Applicability**1.3.1 Certification Authorities**

ESnet will manage and operate the ESnet SSL CA. The on-line CA and its Registration Manager is located in ESnet data center. The following is a list of the PKI components:

Component	Location	Function
Root CA	Offline, ESnet Data Center vault	Signs subordinate CAs
ESnet SSL CA	ESnet Data Center	Signs host or website certificates

Comment: Does this class of CA need a repository? LDAP

1.3.2 Registration Authority

The ESnet SSL CA will use RA from around the DOE community to authorize the appointment of local Grid Administrators. These Grid Administrators will request and approve certificates for hosts under their jurisdiction. They will not request certificates for hosts not under their direct administration.

1.3.3 End Entities

ESnet SSL CA will issue long term host identity certificates for DOE sites and their partners. These certificates are for the use of Hosts and not for individuals or Grid type of services.

1.3.4 Applicability

See section 1.1.1 for definition of certificate types.

Host certificates will be issued by the ESnet SSL CA. These certificate allow a web server to identify itself to its clients.

Personal certificates will not be issued by the ESnet SSL CA.

Grid service certificates will not be issued by the ESnet SSL CA.

1.4 Contact Details

ESnet SSL CA is operated by **ESnet** and managed by a Policy Management Authority. The members of the PMA consist of ESnet staff.

Name	Email	Affiliation
Tony J. Genovese	Tony@es.net	ESnet
Mike Helm	Helm@es.net	ESnet
Dhivakaran Muruganatham	Dhiva@es.net	ESnet
John Webster	Webster@es.net	ESnet
Roberto Morelli	Morelli@es.net	ESnet

Contact person for questions related to this document is the chairman of the PMA. The PMA chairman and his/her contact information:

~~XXXXX~~

Contact information regarding other communications with the ESnet SSL CA, including security incidents, is maintained at www.es.net/CA

The following email addresses and phone numbers can be used to request information or report a problem (Security, access or service failures)

Purpose	Email	Phone
Report a problem	Trouble@es.net	+1 800 333 7638 +1 510 486 7600
Information request	info@es.ent	

2 General Provisions

2.1 Obligations

2.1.1 CA and RA Obligations

ESnet SSL CA will:

- Accept certification requests from entitled entities;
- Notify the RA of certification request and accept authentication results from the RA.
- 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.
- Keep audit logs of the certificate issuance process
- Notify the RA of security incidents that have been reported and coordinate incident response between it and the RA.
- Publish contact information for the CA.

Comment: Do we need this?

An ESnet SSL RA will:

- Accept authentication requests from the ESnet SSL CA;
- Authenticate entity making the certification request according to procedures outlined in this document;
- Notify the ESnet SSL CA when authentication is completed for a certification or revocation request;
- Accept revocation requests according to the procedures outlined in this document;
- Notify the ESnet SSL CA of all revocation requests;
- Authenticate entity making revocation request according to procedures outlined in this document.
- Notify CA of security incidents. Notification should be made as soon as possible, ideally within 12 hours of initial knowledge of incident.
- Publish contact information for the RA
- Notify the CA whenever the contact information for the RA changes.

2.1.2 Subscriber Obligations

Subscribers must:

- Read and adhere to the procedures published in this document;
- Provide correct system/host information and authorize the publication of the certificate;
- Notify ESnet PMA immediately of any security incidents. Notification shall occur within the first 12 hours of initial knowledge of incident.

Comment: Relates to directory.

2.1.3 Relying Party Obligations

Relying parties must:

- Read the procedures published in this document;
- Use the certificates for the permitted uses only.
- Notify ESnet PMA of any security incidents. Notification shall occur within the first 12 hours of initial knowledge of incident.

2.1.4 Repository Obligations

ESnet PKI will provide access to ESnet SSL CA information, as outlined in section 2.6.1, on its web site. The following pages deal with individual items from 2.6.1:

CA information: www.es.net/CA |

Certificates: Browser access: ~~XXXX~~

LDAP access: ~~XXXX~~

CRL information: ~~XXXX~~

CP/CPS: ~~XXXX~~

Comment: New or use the existing one?

Comment: Are we going to do this? Is this needed?

2.2 Liability

No liability, implicit or explicit, is accepted.

ESnet PKI 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 ESnet SSL Certificates. All costs for operation are covered directly or indirectly by DOE.

2.6 Publication and Repositories

2.6.1 Publication of CA information

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

ESnet SSL CA's certificate;

Certificates issued by the PKI;

A Certificate Revocation List;

A copy of this policy

Other information deemed relevant to the ESnet SSL CA.

Comment: Use of repository here is different from the Certificate Repository.

Comment: Another issue related to directory.

2.6.2 Frequency of Publication

- Certificates will be published to the ESnet SSL CA repository as soon as issued.
- CRLs will be published as soon as issued or refreshed once every month if there are no changes.
- All ESnet SSL CA documents will be published to the project website as they are updated.

2.6.3 Access Controls

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

ESnet SSL CA does not impose any access control on its Policy, its signing Certificate and issued certificates, and its CRLs. In the future, ESnet SSL 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 can be found in the service's LDAP directory: **XXXX** or on its website www.doe grids.org:

CA certificate:

www.es.net/CA

CRLs:

www.es.net/CA

CP/CPS:

www.es.net/CA

2.7 Compliance audit

The ESnet SSL CAI is not audited by an outside party. The CA operation may be reviewed by any potential relying organization if approved by the PMA.

2.8 Confidentiality

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

ESnet PKI does not collect any kind of confidential information.

ESnet PKI does have access to or generate the private keys such as those used in host certificates.

2.9 Intellectual Property Rights

TBD. This work is based on the efforts and experience of the DOEGrids PKI.

3 Identification and Authentication

3.1 Initial Registration

3.1.1 Types of names

Names will be consistent with the name requirements specified in RFC2459. See section 7.1.4 for more details.

3.1.2 Name Meanings

The value of the CN component of the DN has no semantic significance. It should contain the FQDN for the host being certified.

3.1.3 Uniqueness of names

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

3.1.4 Method to Prove Possession of Private Key

No stipulation. This service only issues Host certificates. The private key management for host is dependent on local site policies.

3.1.5 Authentication of Individual Identity

This service does not issue individual identity certificates. The host certificates that are issued are issued to and for individuals that have administrative responsibility for the host being certified.

3.2 Revocation Request

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

4 Operational Requirements

4.1 Certificate Application

Certificate signing requests (CSRs) are generated by the host administrator by an online procedure. The CSR is sent to the ESnet SSL CA for issuance.

4.2 Certificate Issuance

ESnet SSL CA issues the certificate if, and only if, an RA has validated the identity of the requestor. It is assumed the RA will delegate or act as the site Grid admin for requesting and approving host certificates.

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 host's private key is lost or suspected to be compromised;
- The information in the host's certificate is suspected to be inaccurate;
- The host no longer needs the certificate;
- The subscriber violated his/her obligations.

4.4.2 Who Can Request Revocation

A request to revoke an End Entity Certificate can be done by the following entities if they can present reasonable evidence that the private key has been compromised or that the subscriber's data is in error:

- The Holder or owner of the Certificate.
- The site RA that validated the original Certificate request
- The ESnet SSL CA managers.

4.4.3 Procedure for Revocation Request

The entity requesting the revocation must authenticate itself to the ESnet SSL CA or the ESnet PKI staff, which must use the same procedures used for the authentication of identity of a person.

4.4.4 Circumstances for Suspension

The ESnet PKI does not support Certificate Suspension.

4.4.5 CRL Issuance Frequency

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

4.4.6 Online Revocation/status checking availability

An online Status checking facility will be provided.

Comment: Should we do this?

4.5 Security Audit Procedures

Security Auditing of the ESnet PKI 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 on the PMA mailing list;

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

4.9 CA Termination

Before ESnet SSL CA terminates its services, it will:

1. Inform subscribers and subordinate RAs;
2. Make widely available information of its termination;
3. Stop issuing certificates and CRLs.
4. Destroy its private key's and all copies.

5 Physical, Procedural and Personnel Security Controls

5.1 Physical Security Controls

The ESnet SSL CA 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. The servers are maintained in access controlled secure racks. All access to the servers is limited to ESnet PKI Security officer and system support staff of ESnet. All servers are Sun Solaris systems. Security on these systems 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.

The ESnet SSL CA server is located behind a Cisco Pix Firewall. The entire server farm will be monitored by the Bro intrusion detection system.

5.2 Procedural Controls

No Stipulations.

5.3 Personnel Security Controls

All access to the servers and applications that comprise the ESnet SSL CA is limited to ESnet PKI 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

The administrator (Grid Admin) for a host being certified must generate its own key pair. ESnet SSL CA does not generate private keys.

6.1.2 Private Key Delivery to Entity

The ESnet SSL CA service never has access to the End Entity private key.

6.1.3 Public Key Delivery to Certificate Issuer

Entities' public keys are delivered to the issuing CA in a secure and trustworthy manner (e.g. SSL/TLS).

6.1.4 CA Public Key Delivery to Users

CA certificate is delivered by an online transaction from a secure web server or by other out of band secure process.

6.1.5 Key Sizes

Keys of length less than 1024 bits will not be signed.

6.1.6 Key usage Purposes

ESnet SSL CA certificates are only warranted for authentication of the named host..

The ESnet SSL CA signing key is the only key that will be used for signing CRLS and Certificates for hosts.

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

Not supported.

6.2.2 Private Key Escrow

Not supported.

6.2.3 Private Key Archival and Backup

There is no support for Private Key Archival and Backup for End Entity Certificates.

ESnet SSL CA signing private key is managed by an nCipher FIPS-140 compliant hardware and software system.

This private key is stored in 3DES encrypted form on the hard disk of the server, and is backed up by conventional server backup services and by other means. The private key is never available in plain text form (that is, in a usable form) to the server operating system or any back up service. The private key is managed by a set of smart cards.

The keys for these smart cards, and the 3DES key used to encrypt the signing private key, are generated by the nCipher nShield FIPS 140 device (key generation is based on a hardware random number generator). Access to these keys is only available through a set of administrator smart cards. Several copies of cards have been created and stored in secure locations.

6.3 Other Aspects of Key Pair Management

ESnet SSL CA certificate has a validity of **five** years.

6.4 Activation Data

ESnet SSL CA signing key is protected by a 3DES key. This key is known only to a set of operator smart cards (the OCS), which are unlocked by pass-phrases individually assigned to each card.

6.5 Computer Security Controls

6.5.1 Specific Computer Security Technical Requirements

CA servers include the following:

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;

6.6 Network Security Controls

ESnet will maintain an Online CA for issuing Certificates authorized by the ESnet SSL RA.

The ESnet SSL CA servers are located behind a Cisco Pix Firewall. The entire server farm will be monitored by the Bro intrusion detection system [Bro].

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

Comment: We had this discussion once, but do we need non-repudiation? And what is key Encipherment 😊

Comment: Do we want the admin's email here?

7.1.3 Name Forms

The X.509 character set is case insensitive. But in some situations software being used to interpret these fields does interpret the name forms as case sensitive. To insure proper operation, relying parties must make sure the case used in Globus map files match the case of issued certificates. Until uniform interpretation of case is deployed it is strongly recommended that we follow the case conventions that are used in the examples below.

Issuer: DC=ES; DC=net; CN=ESnet SSL ca;

Or: O= ES.net; CN=ESnet SSL ca

The subject name of the End Entity will be a valid Distinguished Name (DN). These DNs will consist of the following Relative DNs (RDN):

- OU=Host; O= Site name
- OU=Host; DC= site domain component one; DC=domain component two
- Other valid DN components can be added to meet the site's requirements.

The Common Name (CN) components of the DNs are defined as follows for Host certificates:

A fully qualified domain name as registered in DNS or its 4 octet IP address, optionally prefixed with "host/".

CN= mail2.es.net; OU=hosts; O=ES.net

CN= mail2.es.net; OU=hosts; DC= ES; DC=net

Comment: We don't need this for the general community do we?

Comment: Need OID from ESnet

7.1.4 Certificate Policy Object Identifier

OID: [ESnet].ERmember.DOEScienceGrid.Security.CP

1.2.840.113612.3.6. **X.X**

7.1.5 Usage of Policy Constraints Extensions

No stipulated.

7.1.6 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 ESnet SSL CA's policy and CPS.

8.2 Publication and Notification Procedures

The policy is available at: www.es.net/CA

8.3 CPS Approval Procedures

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