NERSC Online CA – Short Lived Credential Service.

Certification Policy and Certificate Practice Statement – v1.0

Shreyas Cholia
National Energy Research Scientific Computing Center,
Lawrence Berkeley National Laboratory
2008-09-16

NERSC Online CA Certification Policy and Certificate Practice Statement – v1.0

1 Introduction

This document is a combined certification policy and certificate practice statement. It describes the set of procedures followed by the NERSC Online Certification Authority, and outlines the responsibilities of the involved parties. The NERSC Online CA operates as an X.509 Public Key Short Lived Credential Service (SLCS) Certification Authority and issues short-lived credentials (maximum validity period of 1 million seconds) to end-entities.

This document is based on the framework and structure outlined in the Internet Engineering Task Force's RFC 3647. This document establishes compliance of the policies and practices of the NERSC Online CA with the current minimum requirements of the International Grid Trust Federation (IGTF) SLCS CA profile, maintained by the TAGPMA.

1.1 Overview

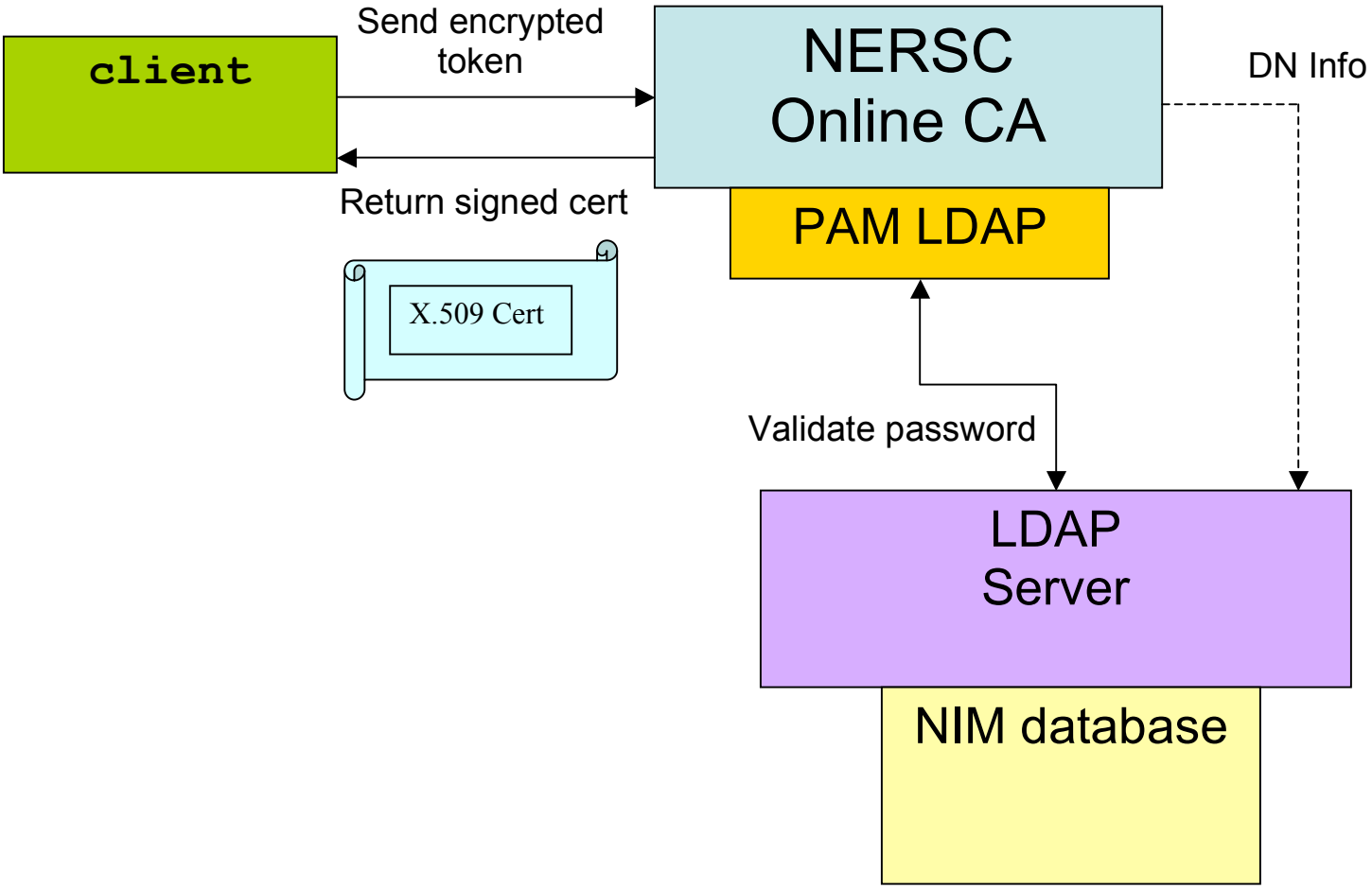
The National Energy Research Scientific Computing Center (NERSC) is the flagship scientific computing facility of the United States Department of Energy and is located at Lawrence Berkeley National Laboratory. The mission of the center is to accelerate scientific discovery through computing. Grid computing is an important aspect of this mission, and allows researchers to access distributed resources, both at NERSC and at collaborating grid sites through the use of grid services and X.509 grid certificates.

In order to facilitate the ease of use and widespread deployment of grid certificates among its users, NERSC has created an online Certification Authority based on the SLCS authentication profile. The NERSC Online CA is based on the NCSA MyProxy software and issues short-lived end entity X.509 credentials to its users. The NERSC Online CA is integrated with a local identity management system known as the NERSC Information Management system (NIM). NIM provides the information database and supports an LDAP based authentication service for all NERSC users.

The NERSC Online CA serves as a catch-all CA for the NERSC user community. The NERSC user community consists of a diverse set of users from several different home institutions that use NERSC resources for their scientific computing needs. NERSC Users are researchers that are funded by the U.S. Department of Energy (DOE), or must be engaged in research that falls within the mission of the DOE Office of Science. NERSC users are awarded use of NERSC resources through an accounts and allocations process.

The NERSC accounts and allocations process establishes the initial identity of the user, which results in the creation of a NERSC account with a unique user identifier or UID.

Users are assigned a distinguished name, based on a combination of their full names and this UID. To obtain credentials, NERSC users run the MyProxy client software on the host where their credentials are to be stored. The software generates the subscriber's private key locally, authenticates the user using their NIM-LDAP password, issues a signed certificate request to the CA, and, if the request is approved, receives a signed certificate from the CA. The NERSC Online CA looks up the full name and UID of the user in the NIM LDAP database, that corresponds to the user's authenticated identity, then issues a certificate with the appropriate distinguished name.



Further policy and implementation details are provided throughout the document.

1.2 DOCUMENT NAME AND IDENTIFICATION

Title: NERSC Online CA Certificate Policy and Certification Practice Statement.
Version: Version 1.0.
Date: March 4, 2008
Approved: Waiting for TAGPMA Review
Expiration: This document is valid until further notice.
ASN.1 OID: The following unique Object Identifier (OID) identifies this CP/CPS:
1.2.840.113613.1.5.1.0

The following table describes the meaning of the OID:

1.2.840	iso(1) member-body(2) us(840)
113613	nersc(113613)
5	NERSC Online CA
1	CP/CPS
1.0	major(1), minor(0) CP/CPS version number

1.3 PKI Participants

The NERSC Online CA is operated by authorized NERSC staff, and issues short-lived end entity certificates for valid NERSC users. These certificates are expected to be used to securely access NERSC resources, as well as grid resources across the world.

1.3.1 Certification authorities

This policy is valid for the NERSC CA. The NERSC Online CA will only sign end entity certificates, and will follow the CP/CPS, as approved by the TAGPMA under the SLCS profile. The NERSC Online CA does not issue certificates to subordinate CAs.

1.3.2 Registration authorities

The NERSC accounts and allocations staff serves as registration authorities for the NERSC Online CA. The NERSC RAs are responsible for vetting the identity of NERSC users, entering user information into the NIM database and creating accounts for these users in NIM and the LDAP database. The enrollment process is defined in Section 4.1.2. Distinguished names for users are automatically generated based on the user's full name and a unique, persistent identifier or UID established at account creation time.

The NERSC Online CA uses a secure, encrypted password authenticated by the NIM-LDAP database to establish identity subsequent to this. Short-lived certificates are issued upon successful authentication.

1.3.3 Subscribers

The NERSC Online CA issues and signs short lived end entity X.509 certificates for the NERSC user community. The NERSC Online CA only issues certificates to valid NERSC users. A valid NERSC user is one whose identity has been vetted by the NERSC accounts and allocations process, has an active record in the NIM database and has a signed NERSC Computer Policy Use form on file with NERSC.

The NERSC Online CA will not issue certificates to non-human or virtual entities, since a certificate generated by the CA must always contain information for a real person.

1.3.4 Relying parties

NERSC places no restrictions on who may accept certificates it issues. NERSC grid resources are expected to rely on certificates issued by this service, as are partner grid sites.

1.3.5 Other participants

No stipulation.

1.4 Certificate usage

1.4.1 Appropriate certificate uses

The goal of the NERSC online CA is to promote use of public-key certificates to identify users in many different applications. NERSC online CA end-entity certificate may be used for any application that is suitable for X.509 certificates, including but not limited to:

- Authentication of users
- Authentication and encryption of communications
- Authentication of signed e-mails
- Authentication of grid jobs and file transfers
- Authentication in web portals
- Authentication of signed objects
- SSL/TLS encryption for applications capable of making use of these technologies.

It is also expected that these certificates will be used in conjunction with authorization services that provide role-based access for a given identity.

Certificates may only be used or accepted for actions specified by the key usage extension in the certificate and that the individual identified by or responsible for the certificate keys is authorized to perform.

1.4.2 Prohibited certificate uses

Certificates issued by the NERSC Online CA must not be used for purposes that violate U.S. law or the law of the country in which the target end entity (i.e. application or

host, addressee of an e-mail) is located. Certificates can only be used to identify real NERSC users. Other uses of NERSC Online CA certificates that meet the above constraints are not prohibited, but may not be supported.

1.5 Policy administration

1.5.1 Organization administering the document

This policy is administered by the National Energy Research Scientific Computing Center (NERSC) at Lawrence Berkeley National Laboratory, 1 Cyclotron Road, Berkeley CA 94720 USA.

This policy is accredited by The Americas Grid Policy Management Authority (TAGPMA), a member of the International Grid Trust Federation (IGTF).

1.5.2 Contact person

The point of contact for this policy and other matters related to the NERSC Online CA is the NERSC TAGPMA representative.
Currently, the designated NERSC TAGPMA representative is:
Shreyas Cholia
Phone Number: +1 510-486-6552
Postal Address: 1 Cyclotron Road, MS 943-256, Berkeley, CA 94720 USA
Email: scholia@lbl.gov

Alternate or after-hours contact information:
NERSC Security Contact Email: security@nersc.gov
NERSC 24x7 Operations Phone Number: +1 800-666-3772 (or +1 510-486-8600)

1.5.3 Person determining CPS suitability for the policy

The NERSC TAGPMA representative, in conjunction with the NERSC Networking And Security Team is responsible for determining CPS suitability for the policy. As an accredited policy of the TAGPMA, all policy changes are subject to TAGPMA review and approval.

1.5.4 CPS approval procedures

This CP/CPS document will be approved by The Americas Grid Policy Management Authority (http://www.tagpma.org) under the SLCS CA profile of the International Grid Trust Federation (http://www.gridpma.org).

1.6 Definitions and acronyms

1.6.1 Definitions

The key words “MUST”, “MUST NOT”, “REQUIRED”, “SHALL”, “SHALL NOT”, “SHOULD”, “SHOULD NOT”, “RECOMMENDED”, “MAY”, and “OPTIONAL” in this document are to be interpreted as described in RFC 2119.

Activation data

Data values, other than keys, that are required to operate cryptographic modules and are required to be protected (e.g.,a PIN, or a password).

Authentication
The process used to establish the authenticity of an individual, organization, computer system, service or software component. Authentication is used to ensure that the subject is really who or what it claims to be. In the public key infrastructure (PKI) there are two different authentications. The first occurs after a request for a certificate is made and has the objective of verifying that the certificate will be issued to the correct subject (also known as identification). The second is a security service that provides assurances that the individual or organization applying for or seeking access to something under a certain name is, in fact, the proper individual or organization, or that the data sent electronically originated from the specific individual, organization, or device that claims to have sent it. Thus, it is said in the case of the latter, that a digital signature of a message authenticates the message's sender.

Certification Authority
A certification authority (CA) is a trusted authority that issues and manages public key certificates as part of a public key infrastructure (PKI).

Public-key Certificate (or just "certificate")
Electronic document binds a public key held by an entity (such as person, organization, account, device, or site) to a set of information that identifies the entity associated with use of the corresponding private key.

CA-certificate
A certificate for given CA's public key issued by another CA or, in the case of a self-signed CA-certificate, issued by the same CA.

Catch-All CA
A CA the issues certificates for subscribers belonging to several different home institutions.

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 CP might indicate applicability of a type of certificate to the authentication of parties engaging in business-to-business transactions for the trading of goods or services within a given price range.

Certification Practice Statement (CPS)
A statement of the practices that a certification authority employs in issuing, managing, revoking, and renewing or re-keying certificates.

Certificate Revocation List
A time stamped list containing the index number of the revoked certificates, which is signed by a CA and made available in the CA’s public repository.

Digital Signature
Refers to the use of the owner’s private key to sign an electronic document, for example a digitally signed email. The recipient(s) can use the owner’s public key (from the owner’s corresponding valid certificate) to verify that the owner was indeed the author of the document (see Authentication).

End Entity

The service or individual identified by a certificate. An end-entity certificate is distinguished from a CA certificate in that the CA certificate is an intermediate certificate used to validate the identity of an end-entity.

Identification

The process of establishing the identity of an individual or organization.

Issuing certification authority (issuing CA)

In the context of a particular certificate, the issuing CA is the CA that issued the certificate (see also subject certification authority).

Participant

An individual or organization that plays a role within a given PKI as a subscriber, relying party, CA, RA, certificate manufacturing authority, repository service provider, or similar entity.

Personal Certificate

A certificate used for authentication to establish the identity an individual person.

Public Key Infrastructure (PKI)

The set of hardware, software, people, policies and procedures needed to create, manage, store, distribute, and revoke PKCs based on public-key cryptography. 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 authority (RA)

An entity that is responsible for one or more of the following functions: the identification and authentication of certificate applicants; the approval or rejection of certificate applications; initiating certificate revocations or suspensions under certain circumstances; processing subscriber requests to revoke or suspend their certificates; and approving or rejecting requests by subscribers to renew or re-key their certificates. RAs, however, do 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 any digital signatures verified using that certificate. In this document, the terms "certificate user" and "relying party" are used interchangeably.

Relying party agreement (RPA)

An agreement between a certification authority and relying party that typically establishes the rights and responsibilities between those parties regarding the verification of digital signatures or other uses of certificates.

Repository

The on-line storage area where the CA stores issued certificates, CRLs, the root certificate etc.

Set of provisions

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

Signed e-mail

An e-mail message that has been check summed and signed by a valid certificate.

Short Lived Certificate

A certificate with a lifetime of no more than 1 million seconds.

Strong password

A characteristic of a password. The password used to protect the certificate must be strong. That means difficult to guess.

Subject Identification
The process of establishing the identity of a person.

Subject certification authority (subject CA)
In the context of a particular CA-certificate, the subject CA is the CA whose public key is certified in the certificate (see also Issuing certification authority).

Subscriber
A subject of a certificate to whom a certificate is issued.

Subscriber Agreement
An agreement between a CA and a subscriber that establishes the right and responsibilities of the parties regarding the issuance and management of certificates.

Validation
The process of identifying and verifying certificate applicants. *Validation* is a subset of *identification* and refers to identification in the context of establishing the identity of certificate applicants.

1.6.2 Acronyms

C Country
CA Certification Authority
CN Common Name
CDROM Compact Disc Read Only Memory
CP Certificate Policy
CPS Certificate Practice Statement
CRL Certificate Revocation List
CSR Certificate Signing Request
DN Distinguish name
DOE Department of Energy (U.S.)
ERCAP Energy Research Computer Allocations Process
LBNL Lawrence Berkeley National Laboratory
LDAP Lightweight Directory Access Protocol
MIME Multi-purpose Internet Mail Extensions
NCSA National Center for Supercomputing Applications
NERSC National Energy Research Scientific Computing Center
NIM NERSC Information Management System
NTP Network Time Protocol
O Organization
OID Object Identifier
OU Organizational Unit
PKI Public Key Infrastructure
RA Registration Authority
SLCS Short Lived Credential Services
SSL Secure Sockets Layer
TAGPMA The Americas Grid Authentication Policy Management Authority, http://www.tagpma.org/
UFF BrGrid CA Brazilian Grid Certificate Authority

UPS Uninterruptible Power Supply
URI Universal Resource Identifier
URL Universal Resource Locator

2 Publication and Repository Responsibilities

2.1 Repositories

An online repository of information relating to the NERSC Online CA is accessible through the WWW URL http://www.nersc.gov/nusers/services/Grid

2.2 Publication of certification information

The NERSC Online CA will operate a secure online repository at http://certs.nersc.gov that contains:

1. PEM and DER formatted certificates for the NERSC Online CA, signed by the ESnet Root CA;
   - PEM certificate: http://certs.nersc.gov/certificates/b93d6240.0
   - DER certificate: http://certs.nersc.gov/certificates/nerscca.crt
2. A link to the ESnet Root CA certificate;
3. The most recent copies of NERSC Online CA CP/CPS documents;
4. A contact email address for inquires and fault and incident reporting;
5. A postal contact address;
6. Any other information deemed relevant to the NERSC Online CA service.
7. Links to PEM and DER formatted versions of the list of revoked NERSC Online CA certificates (Certificate Revocation List).
   - PEM CRL: http://certs.nersc.gov/certificates/b93d6240.r0
   - DER CRL: http://certs.nersc.gov/certificates/nerscca.crl

The NERSC Online CA may optionally provide in the above repository:

1. Information to validate the integrity of the root certificate;

As an accredited CA member of the TAGPMA, the NERSC Online CA grants the IGTF and its PMAs the right of unlimited re-distribution of this information.

2.3 Time or frequency of publication

All information will be published with 24 hours following an update.

The published certificate revocation list (CRL) shall have a lifetime of at most 30 days. The NERSC Online CA must issue a new CRL at least 7 days before expiration, or immediately after having successfully processed a revocation, whichever comes first. A new CRL must be published immediately after its issuance.

This CP/CPS will be published whenever it is updated and, in the case of major changes, once these have been approved by the TAGPMA.

2.4 Access controls on repositories

Public information on the NERSC Online CA web site is read-only accessible without any restriction.

The NERSC Online CA does not impose any read access control on its repositories. Write access is restricted to NERSC CA software and authorized NERSC staff. The online repository is maintained on a best effort basis and is available on a 24 hours per day, 7 days per week basis, subject to reasonable scheduled maintenance. Outside the period 09:00-17:00 (local time) Monday-Friday it may run unattended.

3 Identification and Authentication

3.1 Naming

3.1.1 Types of names

Subject distinguished names are X.500 names, with fixed and varying components

3.1.2 Need for names to be meaningful

A unique (see Section 3.1.5) "common name" is assigned to each user consisting of their legal name with a unique identifier (UID) appended in the case of name conflicts.

3.1.3 Anonymity or pseudonymity of subscribers

Anonymity and pseudonymity are not supported.

3.1.4 Rules for interpreting various name forms

All subject distinguished names in certificates issued by the NERSC Online CA begin with the following fixed component:
/DC=gov/DC=nersc

The next component takes the following form:
/OU=People/CN=*Full Name UID*
where *Full Name* is the user's full name, and *UID* is a unique, persistent identifier to disambiguate the name from other users with the same name.

The OU component is not expected to support any other values, other than "People". However, it is separated from the fixed component to maintain flexibility.

The complete DN for a certificate looks like:
/DC=gov/DC=nersc/OU=People/CN=*Full Name UID*

Thus, an example certificate distinguished name would look like this:
/DC=gov/DC=nersc/OU=People/CN=Jane Doe 12345

The signing certificate for the NERSC Online CA has the following DN:
/DC=net/DC=ES/OU=Certificate Authorities/CN=NERSC Online CA

The signing certificate and key are issued by the ESnet Root CA.

3.1.5 Uniqueness of names

The Distinguished Name (DN) in each certificate issued by the NERSC Online CA must be unique. Under this CP/CPS policy, two names are considered identical if they differ only in case, punctuation or whitespace; in other words, case, punctuation or whitespaces must not be used to differentiate names

Certificates must apply to unique individuals or resources. Every subject distinguished name must be linked to one and only one end entity throughout the entire life time of the NERSC Online CA. Subscribers must not share certificates.

Each subject name issued by the NERSC Online CA will be issued to one and only one individual as identified by NIM. NIM implements checks to ensure the uniqueness of assigned distinguished names. NIM records all UIDs that have been previously issued, so that any new UID, and thus any DN that includes this UID, is guaranteed to be unique.

A unique "common name" is assigned to each user consisting of their legal name and a unique, persistent UID appended in the case of name conflicts. This common name, along with the prefix (/DC=gov/DC=nersc/OU=People), creates globally unique distinguished names used in certificates issued by the NERSC Online CA to users. User records are never purged from the NIM database and UIDs are never reused, to ensure that distinguished names will never be reassigned to another individual.

3.1.6 Recognition, authentication, and role of trademarks

No stipulation.

3.2 Initial identity validation

3.2.1 Method to prove possession of private key

Certificate requests must be digitally signed. The possession of the private key by the requestor is considered proven when the digital signature of the certificate signing request (CSR) can be verified using the public key present in the request.

3.2.2 Authentication of organization identity

The NERSC Online CA will only issue certificates to individuals who are considered NERSC users. NERSC users are identified as individuals that meet all the following requirements:

1. Must have their identity established through the initial accounts and allocations process (described in section 4.1.2).
2. Must have a record in the NIM database.
3. Must have a current signed NERSC Computer Use Policy form on record with NERSC.
4. Must be part of an existing allocation at NERSC.

3.2.3 Authentication of individual identity

Initial user verification has already occurred during the NERSC accounts and allocations process described in section 4.1.2. The NERSC Online CA only issues certificates to valid users already in the NIM database. Authentication of identity for issuing certificates is done as follows:
User identity will be authenticated via LDAP, with the authenticated LDAP user name mapped to a unique Subject DN through NIM. The NERSC Online CA will accept an encrypted username and an authentication token from a client, and verify this against the LDAP password in the NIM database. The authentication path is as follows:

1. User initiates request for short-lived certificate from NERSC online CA using a MyProxy client.
2. Client creates a local private key and CSR.
3. Client sends CSR to NERSC Online CA for certificate signing.
4. Client sends LDAP username and password to NERSC Online CA over encrypted SSL channel.
5. NERSC Online CA performs secure LDAP authentication using the PAM LDAP module for the given username/password against the NIM LDAP database
6. If user is successfully authenticated by LDAP, the NERSC online CA generates a short-lived certificate and sends it back to the client, otherwise it returns an authentication error to the client.
7. All communications between the MyProxy client and the NERSC Online CA use the MyProxy protocol and are 128-bit TLS encrypted.

3.2.4 Non-verified subscriber information

The following information is gathered and verified during the initial accounts and allocations process:

- Name
- Citizenship
- Organization
- Email Address
- Work Phone Number
- Principal Investigator

Other information may not be verified.

The NERSC Online CA relies on the initial accounts and allocations process for subscriber information verification, and does not explicitly verify any of the above information.

3.2.5 Validation of authority

Users making requests for user certificates must be authenticated as the user identified in the certificate.

3.2.6 Criteria for interoperation

No Stipulation.

3.3 Identification and authentication for re-key requests

3.3.1 Identification and authentication for routine re-key

Every certificate request is treated as an initial registration with respect to key signing.

3.3.2 Identification and authentication for re-key after revocation

If the compromise is limited to just the temporary private key for the short-lived certificate, the request for re-key will be treated as an initial registration. If the compromise involved a user's password, the account and password will be locked and rendered temporarily unusable. In this case, the user must contact the NERSC accounts and allocations staff to re-establish their identity and password using verified information established during the accounts and allocations process. This includes PI verification, internal NERSC repository information, as well as contacting the user directly at the phone number and email address provided.

3.4 Identification and authentication for revocation request

CA Certificates will only be revoked at the instigation of designated NERSC Online CA operational personnel.

User certificate revocation must follow the same identification procedures as those used by the accounts and allocations process to perform password resets (Section 3.3.2, Section 4.1.2).

4 Certificate Life-Cycle Operational Requirements

4.1 Certificate Application

4.1.1 Who can submit a certificate application

Any existing NERSC user (as defined in section 3.2.2) can apply for a certificate from the NERSC online CA.

4.1.2 Enrollment process and responsibilities

NERSC Accounts and Allocations staff will create NIM accounts for NERSC users. Since all current NERSC users in the NIM database are automatically eligible for personal certificates from the NERSC Online CA, the NIM accounts and allocations process serves as the initial step in the enrollment process for CA subscribers.

If an individual is not a member of a project that has a NERSC award, they may apply for a new allocation, if the project meets the DOE Office of Science Mission (http://www.nersc.gov/nusers/accounts/allocations/ercap/mission.php/) and requires high performance computing resources. The application is made through a process known as ERCAP (Energy Research Computer Allocations Process). Awards are made to group accounts known at NERSC as repositories or "repos". See the ERCAP allocations web page for more information: http://www.nersc.gov/nusers/accounts/allocations/ercap/

Once a project's ERCAP request has been approved and a resource allocation has been awarded to a repository, the project's PI (or designated PI Proxies and Project managers) can request, via the NERSC Information Management (NIM) web interface, that individual users be added to (given access to) the repository.

A new PI is automatically given a NIM account, but must request that he/she be given access to a given resource (and its repository), if desired.

Users new to NERSC must sign and return the Computer Use Policies form before they are added to a repository.

In order to get a NERSC account, a user must satisfy one of the following conditions:

- Be a NERSC employee
- Be a Principal Investigator (PI) with an allocation on NERSC computational resources approved through the DOE ERCAP process
- Be a Principal Investigator (PI) with a startup allocation requested through NERSC management
- Have a NERSC account requested on their behalf by an existing PI under that PI's existing repository

Identity vetting of NERSC employees is performed in person as part of the Lawrence Berkeley National Laboratory (LBNL) hiring process, in collaboration with the LBNL Human Resources department.

All Principal Investigators funded by the Office of Science are eligible to apply for an allocation of NERSC resources. The DOE Office of Science is directly responsible for vetting the identity of PIs during the ERCAP process. All requests for allocation through the ERCAP process are reviewed by DOE – identity vetting involves a combination of peer review for currently funded DOE projects, and contact with the home institution of the PI for projects not directly under DOE funding.

PIs requesting startup allocations require approval from NERSC management. Startup allocation requests must reviewed and approved by NERSC management PIs must be vetted directly by the NERSC allocations manager.

Identity vetting of individuals working on a project under the PI is handled by the PIs themselves. PIs are responsible for validating account requests on behalf of these individuals. It is expected that PIs will only authorize individuals that are directly known to them, and are working under the same project umbrella. Users must sign a NERSC Computer Use Policy Form before their request will be processed. PIs are required to update the list of current users in their repository and verify the information provided by the users annually. The PI must agree to these responsibilities when initially applying for a NERSC allocation, and this agreement must be renewed annually.

Once an account request has been generated, NERSC account and allocation staff will confirm the following information.

- Presence of a signed hard copy of the NERSC Computer Use Policy Form, (http://www.nersc.gov/nusers/accounts/usage.php) on file with NERSC with the following information:
    - Name
    - Citizenship
    - Organization
    - Email Address
    - Work Phone Number
    - Principal Investigator
- Institutional information.
- P.I. approval.
- Verification of above user information through face-to-face contact or telephone communication

NERSC accounts and allocations staff will then assign a temporary password and communicate this to the user through face-to-face contact or telephone communication. The user must then log in to the NIM interface to reset their password. As a Department of Energy facility, NERSC adheres to Department of Energy guidelines regarding passwords. The following requirements conform to the Department of Energy guidelines regarding passwords, namely DOE Order 205.3 and to Lawrence Berkeley National Laboratory's RPM §9.02 Operational Procedures for Computing and Communications:

- Passwords must contain at least eight nonblank characters.
- Passwords must contain a combination of upper and lowercase letters, numbers, and at least one special character within the first seven positions.
- Passwords must contain a nonnumeric letter or symbol in the first and last positions.
- Passwords must not contain the user login name.
- Passwords must not include the user's own or (to the best of his or her knowledge) a close friend's or relative's name, employee number, Social Security number, birthdate, telephone number, or any information about him or her that the user believes could be readily learned or guessed.
- Passwords must not (to the best of the user's knowledge) include common words from an English dictionary or a dictionary of another language with which the user has familiarity.
- Passwords must not (to the best of the user's knowledge) contain commonly used proper names, including the name of any fictional character or place.
- Passwords must not contain any simple pattern of letters or numbers such as "qwertyxx".

Password reset requests must happen through face-to-face or telephone contact with NERSC accounts and allocations staff, and users must be able to verify their identities by providing matching information from the NERSC computer use policy form.
A user with a valid NERSC account will have an entry in the NIM database, including the user’s full name, a unique identifier or UID that will not be reused by the NIM

database, and an md5 hash of the user's password. This information is available to the NERSC Online CA through an LDAP directory tree.

4.2 Certificate application processing

4.2.1 Performing identification and authentication functions

The NERSC Online CA authenticates all certificate requests as described in Section 3.2.3 using LDAP authentication against the NIM database. All communications are 128-bit TLS encrypted.

4.2.2 Approval or rejection of certificate applications

Certificate applications will be approved if the applicant can be authenticated via LDAP using their NIM password. If the applicant does not provide their valid NIM password applications will be rejected.

4.2.3 Time to process certificate applications

Certificate applications are processed immediately upon receiving the request since this is an automated CA service.

4.3 Certificate issuance

4.3.1 CA actions during certificate issuance

The NERSC Online CA receives a CSR and an encrypted username and password. The CA must verify the password for a given user in the NIM LDAP database. If successful the CA will automatically process the request and sign a short-lived certificate bearing that user's DN as described in section 3.1.4.

4.3.2 Notification to subscriber by the CA of issuance of certificate

User certificates are returned directly to the user through the application program they use to apply for a certificate.

4.4 Certificate acceptance

4.4.1 Conduct constituting certificate acceptance

Certificate acceptance is assumed.

4.4.2 Publication of the certificate by the CA

End entity certificates are not published.

4.4.3 Notification of certificate issuance by the CA to other entities

No notifications to other entities will be performed.

4.5 Key pair and certificate usage

4.5.1 Subscriber private key and certificate usage

Subscribers must:

- Exercise all reasonable care in protecting the private keys corresponding to their certificates, including but not limited to transmitting them over a network and never sharing them between people.
- Observe restrictions on private key and certificate use.
- Promptly notify the CA operators of any incident involving the suspected compromise of a private key.
- Never share their NIM password that is used to authenticate the user during certificate generation.

4.5.2 Relying party public key and certificate usage

A relying party should, upon being presented with a certificate issued by the NERSC Online CA, check

1. its validity by
    a) checking that it trusts the CA that issued the certificate,
    b) checking that the certificate hasn't expired
    c) consulting the NERSC Online CA CRL in effect at the time of use of the certificate or querying the certificate's validity using the OCSP facility if present.
2. the appropriate usage as outlined by this CP/CPS.
3. observe restrictions on private key and certificate use.
4. not presume any authorization of an end entity based on possession of a certificate from the NERSC Online CA or its corresponding private key.

4.6 Certificate renewal

Certificates from the NERSC Online CA are not explicitly renewed. Instead the original subscriber may request a new certificate, using the normal certificate issuance process.

4.6.1 Circumstance for certificate renewal

Not Applicable.

4.6.2 Who may request renewal

Not Applicable.

4.6.3 Processing certificate renewal requests

Not Applicable.

4.6.4 Notification of new certificate issuance to subscriber

Not Applicable.

4.6.5 Conduct constituting acceptance of a renewal certificate

Not Applicable.

4.6.6 Publication of the renewal certificate by the CA

Not Applicable.

4.6.7 Notification of certificate issuance by the CA to other

Not Applicable.

4.7 Certificate re-key

Certificates from the NERSC Online CA are not explicitly re-keyed. Instead the original subscriber may request a new certificate, using the normal certificate issuance process.

4.7.1 Circumstance for certificate re-key

Not Applicable.

4.7.2 Who may request re-key

Not Applicable.

4.7.3 Processing certificate re-keying requests

Not Applicable.

4.7.4 Notification of new certificate issuance to subscriber

Not Applicable.

4.7.5 Conduct constituting acceptance of re-keyed certificate

Not Applicable.

4.7.6 Publication of the re-keyed certificate by the CA

Not Applicable.

4.7.7 Notification of certificate issuance by the CA to other

Not Applicable.

4.8 Certificate modification

Certificates from the NERSC Online CA are not modified. Instead new certificates will be issued using the normal certificate issuance process.

4.8.1 Circumstance for certificate modification

Not Applicable.

4.8.2 Who may request modification

Not Applicable.

4.8.3 Processing certificate modification requests

Not Applicable.

4.8.4 Notification of new certificate issuance to subscriber

Not Applicable.

4.8.5 Conduct constituting acceptance of modified certificate

Not Applicable.

4.8.6 Publication of the modified certificate by the CA

Not Applicable.

4.8.7 Notification of certificate issuance by the CA to other

Not Applicable.

4.9 Certificate revocation and suspension

The NERSC Online CA will support a Certificate Revocation List. Users should directly contact NERSC Accounts and Allocations support staff if they wish to revoke their certificates, in the event of a compromise of their private key. Users must contact NERSC Accounts and Allocations staff in the event of a compromise of their NIM password. In case of a compromised password, the NIM account will be locked, and certificate generation will be suspended for that user until identity can be re-established (see section 4.1.2) and the password is reset.

Also, if an individual is no longer a valid NERSC user, their account will be disabled and they will no longer be able to receive a certificate from NERSC.

4.9.1 Circumstances for revocation

Due to short certificate lifetimes, the NERSC Online CA may not explicitly support revocation for certificates with a lifetime of under 24 hours.

Certificates may be revoked under one or more of the following circumstances:

1. The subscriber's private key is suspected to have been compromised.
2. The subscriber has failed to comply with the NERSC Computer Use Policy.
3. The subscriber has failed to comply with the rules in this policy document.

Should the private key of NERSC Online CA be compromised or lost, the signing certificate of the NERSC Online CA will be revoked by the issuing ESnet root CA, thus effectively revoking all certificates signed by the NERSC Online CA.

4.9.2 Who can request revocation

Users should directly contact NERSC Accounts and Allocations support staff if they wish to revoke their own certificates, in the event of a compromise of their private key.

NERSC CA administrative personnel may also initiate a user certificate revocation request under the circumstances described in section 4.9.1.

A revocation request for the NERSC Online CA signing certificate must come from the NERSC Online CA administrative personnel, as described in the CP/CPS for the ESnet Root CA.

4.9.3 Procedure for revocation request

User certificate revocation may not be explicitly supported for certificates with lifetimes of under 24 hours.

User's wishing to revoke their certificates must contact NERSC Accounts and Allocations staff directly in person or via telephone, and establish their identity as described in section 4.1.2 in order to request a certificate revocation.

The procedure for revocation requests of the signing certificate is defined in the ESnet Root CA CP/CPS.

4.9.4 Revocation request grace period

No Stipulation.

4.9.5 Time within which CA must process the revocation request

The NERSC Online CA will act promptly to revocation requests in at most one working day, which means however that implementation may be delayed by weekends or public holidays.

4.9.6 Revocation checking requirement for relying parties

If revocation is not supported (certificates with lifetimes under 24 hours) there is no checking requirement for relying parties.

If revocation is supported, before using a certificate, the relying party should validate it against the most recently published CRL in the NERSC Online CA repository.

4.9.7 CRL issuance frequency (if applicable)

A new CRL will be published immediately after the certificate revocation is processed, or at least 7 days before the expiration of the current CRL.

Since certificates have short lifetimes, CRLs may not include expired certificates and may be empty if there are no currently active certificates that have been revoked.

4.9.8 Maximum latency for CRLs (if applicable)

The maximum latency between the generation of CRLs and posting of the CRLs to the repository will be one working day.

4.9.9 On-line revocation/status checking availability

The latest CRL will be available from the NERSC Online CA web site.

4.9.10 On-line revocation checking requirements

Relying parties should check the CRL before they use and trust a certificate. No access control shall limit the possibility to check the CRL.

4.9.11 Other forms of revocation advertisements available

No stipulation.

4.9.12 Special requirements re-key compromise

Users should directly contact NERSC Accounts and Allocations support staff if they wish to revoke their certificates, in the event of a compromise of their private key.
Users must contact NERSC Accounts and Allocations staff in the event of a compromise of their NIM password. In case of a compromised password, the NIM account will be locked, and certificate generation will be suspended for that user until identity can be re-established (see section 4.1.2) and the password is reset. While this does not explicitly result in a revocation, it will result in a suspension of the ability to acquire a new certificate.

4.9.13 Circumstances for suspension

The NERSC Online CA does not suspend certificates. However, new certificate issuance will be suspended if a user's account is locked in the NIM database.

4.9.14 Who can request suspension

The NERSC Online CA does not suspend certificates. However, a NERSC user may request for suspension of an account in case their password is suspected. NERSC accounts and allocations staff may also suspend an account at any time. Suspension of a user's account will prevent that user from acquiring a new certificate.

4.9.15 Procedure for suspension request

The NERSC Online CA does not suspend certificates. However NERSC users may request for suspension of an account by contacting NERSC accounts and allocations staff and establishing identity as defined in section 4.1.2.
NERSC accounts and allocations staff are authorized to suspend an account, if the account is suspected of being compromised, if the owner of the account is no longer a valid NERSC user, or if contact information for that user cannot be verifiably ascertained.
Account suspension will change the state of the user's account in NIM, such that authentication requests to the NERSC CA will be rejected. Suspension of a user's account will prevent that user from acquiring a new certificate. The account may be

unsuspended once all of the conditions that led to the suspension have been suitably resolved.

4.9.16 Limits on suspension period

The NERSC Online CA does not suspend certificates. There is no stipulation on the length of suspended accounts.

4.10 Certificate Status Services

4.10.1 Operational characteristics

The NERSC Online CA shall store in its public repository and make available via its web site the contents described in Section 2.2.

4.10.2 Service availability

The NERSC Online CA shall run this service continuously, except for unavoidable maintenance activities. Due to the nature of the Internet, this service cannot be guaranteed to be accessible always.

4.10.3 Optional features

No Stipulation.

4.11 End of Subscription

The subscription ends with the expiry of the certificate. Additionally a user will no longer be able to acquire new certificates if they are no longer a valid NERSC user.

4.12 Key Escrow and Recovery

4.12.1 Key escrow and recovery policy and practices

No key escrow or recovery services are provided. The key owner must take reasonable steps to prevent loss of his/her private key.

4.12.2 Session key encapsulation and recovery policy and practices

See Section 4.12.1.

5 Facility, Management, and Operational Controls

5.1 Physical Controls

The NERSC Online CA is located in the NERSC center at Lawrence Berkeley National Laboratory. The NERSC center is currently located at the Oakland Scientific Facility at 415 20th St., Oakland, CA 94612, USA.

The NERSC Online CA may be moved to a secure facility on the main LBNL campus at 1 Cyclotron Road, Berkeley, CA 94720, USA in the future.

5.1.1 Site location and construction

The NERSC site is located at Lawrence Berkeley National Laboratory, at the address mentioned above in section 5.1.

The NERSC Online CA is located in a restricted access room that can be accessed through the main computer room area of the NERSC center. Both the main computer room, and the restricted server room require badged access and access is restricted to authorized LBNL employees and contractors. All access to badged areas is logged.

5.1.2 Physical access

The NERSC Online CA machine is housed in a controlled environment, where access is restricted to authorized NERSC personnel and logged. The CA itself is stored in a restricted server room with access limited to a very restricted subset of NERSC staff members using an ID badge reader. Access to this room is through the main computer room area at NERSC. The main computer room area is limited to NERSC staff members, authorized contractors and other designated LBNL employees; access is controlled through another set of ID badge readers. Entry to the computer room floor is monitored by security guards and surveillance cameras. Visitors accessing the main computer room area must be accompanied by authorized personnel.

5.1.3 Power and air conditioning

The NERSC Online CA machine will be on Uninterrupted Power Supply (UPS).

5.1.4 Water exposures

No Stipulation.

5.1.5 Fire prevention and protection

The NERSC computer room area and restricted server area are both regularly surveyed and inspected by the LBNL Fire Marshall.

5.1.6 Media storage

All media used for storing backup copies of the CA's private key are stored in a locked safe to which only authorized personnel have access.
Backups of the CA machine's disks and software are stored in HPSS.

5.1.7 Waste disposal

Any waste containing the private key of the CA shall not be disposed unless it can be guaranteed that the information may not be obtained or re-used.

5.1.8 Off-site backup

No Stipulation.

5.2 Procedural Controls

5.2.1 Trusted roles

All persons with access to the systems hosting the NERSC Online CA will be full-time NERSC employees. Personnel will include:

a. NERSC Operations staff
b. NERSC Networking And Security Team staff
c. NERSC System administration staff.
d. NERSC CA administrators.
e. NERSC approved contractors and maintenance personnel with authorized access.

There are only two roles defined within these personnel.

1. Staff with full administrative privileges on the NERSC Online CA.
2. Staff with operator level privileges for on the machine. At this level staff will have physical access to the machine, and may be able to perform basic operations like starting and stopping the machine, but will not be able to perform duties that require full system administrative privileges.

5.2.2 Number of persons required per task

No Stipulation

5.2.3 Identification and authentication for each role

All NERSC Online CA personnel will be full-time NERSC staff members. Role based access will be limited by restricting credentials for full system administrative privileges to authorized personnel. No additional authorization is required for specific roles.

5.3 Personnel Controls

5.3.1 Qualifications, experience, and clearance requirements

NERSC Online CA personnel will be qualified system administrators and operators at NERSC.

5.3.2 Background check procedures

No stipulation.

5.3.3 Training requirements

NERSC CA administrators must be familiar with the principles of PKI and grid certificates, as well as NERSC security policies and requirements. Other NERSC staff must be familiar with NERSC security policies and requirements. No formal training is defined – it is the responsibility of the designated NERSC staff to be familiar with the above requirements.

5.3.4 Retraining frequency and requirements

No stipulation.

5.3.5 Job rotation frequency and sequence

No Stipulation.

5.3.6 Sanctions for unauthorized actions

Unauthorized actions, abuse of authority or unauthorized use of entity systems by CA personnel will be dealt with according to LBNL policy as defined in the Regulations and Procedures Manual (RPM).

5.3.7 Independent contractor requirements

No stipulation.

5.3.8 Documentation supplied to personnel

NERSC Online CA administrators will have access to

1. A copy of the NERSC Online CA CP/CPS
2. Internal NERSC system administration documentation (currently hosted on the NERSC Staff TWiki)

5.4 Audit Logging Procedures

5.4.1 Types of events recorded

The following items will be logged and archived:

- Certificate requests
- Certificate issuance
- Attempted and successful accesses to the systems hosting the NERSC Online CA
- Reboots of NERSC online CA systems
- Certificate revocations and CRLs

5.4.2 Frequency of processing log

The log files shall be processed and archived daily into HPSS (High Performance Storage System mass storage.

5.4.3 Retention period for audit log

The minimal retention period for the log files is 3 years.

5.4.4 Protection of audit log

Audit logs are protected by filesystem permissions (both locally and in the mass storage system) and are only accessible to NERSC system administrators with full system administrative privileges on the relevant systems.

5.4.5 Audit log backup procedures

All log files are automatically backed up into HPSS. Full backups are performed once a week, and incremental backups are performed daily. Additionally the system logs are sent to a central syslog collector that is only accessible within NERSC to a very restricted set of NERSC Networking And Security Team personnel.

5.4.6 Audit collection system (internal vs. external)

The audit collection system is internal to NERSC.

5.4.7 Notification to event-causing subject

No stipulation

5.4.8 Vulnerability assessments

The NERSC Networking And Security Team will perform an audit of the NERSC Online CA machine and logs, and will scan the machine for vulnerabilities on a periodic basis. Additionally the BRO intrusion detection system (http://www.bro-ids.org/) will monitor network traffic and audit data on the NERSC Online CA for intrusion detection.

5.5 Records Archival

5.5.1 Types of records archived

See Section 5.4.1.

5.5.2 Retention period for archive

The archive is not deleted. The minimum retention period will be at last 3 years.

5.5.3 Protection of archive

The archive stored in HPSS shall only be accessible to authorized external auditors (see Section 8.3), NERSC CA administrative personnel and authorized NERSC system administrators.

5.5.4 Archive backup procedures

See section 5.4.5

5.5.5 Requirements for time-stamping of records

Archive records are time-stamped using Unix file. For online systems (RA), the clock is synchronized through NTP.

5.5.6 Archive collection system (internal or external)

The archive collection system is internal to NERSC

5.5.7 Procedures to obtain and verify archive information

No Stipulation.

5.6 Key changeover

In the case of a changeover of the NERSC Online CA's key pair, best effort will be made to notify relying parties of any new public key for the NERSC Online CA, which may then be obtained in the same manner as the previous NERSC Online CA certificates.

Since subscriber certificates are short-lived and easily reissued, key changeover is not expected to significantly impact subscribers.

5.7 Compromise and Disaster Recovery

5.7.1 Incident and compromise handling procedures

If a user's password is suspected of being compromised that user's account will be locked and the user will not be able to acquire a certificate from the NERSC online CA, until the password can be reset, and the user's identity re-established as described in section 4.1.2.

If the private key of the NERSC online CA is suspected of being compromised, the NERSC CA administrator must:

- make every reasonable effort to notify subscribers.
- terminate the issuing and distribution of certificates.
- request revocation of the compromised certificate.
- generate a new CA key pair and certificate and publish the certificate in the repository.
- notify relevant security contacts.
- notify relying parties and cross-certifying CAs, of which the CA is aware, as widely as possible.
- revoke all of the valid certificates that have been previously signed by the compromised key.
- publish the new CRL on the NERSC Online CA repository signed with the newly generated key

5.7.2 Computing resources, software, and/or data are corrupted

The NERSC Online CA will take best effort precautions to enable a quick recovery. In case of corruption, the CA systems are either repaired or rebuilt from the last good backup. If a good backup cannot be identified, the systems will be reinstalled from scratch.

The private key of the CA will be stored on an Aladdin eToken Pro 64 USB device (HSM). In the event that the HSM device is corrupted or unusable due to failure, there will be multiple backup HSM devices, with an identical configuration and private key of the NERSC Online CA. Thus, the HSM device can be trivially replaced in case of failure or corruption. Backup HSM devices with the private key are stored in a safe and access is restricted to authorized personnel. The HSM device itself is certified at FIPS 140-level 3 and will not allow the private key to be read externally.

5.7.3 Entity private key compromise procedures

Given the short lifetime of the certificates, end entity private key compromises have a limited risk. For certificates with lifetimes greater than 24 hours, the corresponding certificate will be revoked, and a new CRL will be published. The NERSC Online CA may also revoke certificates with shorter lifetimes, if the revocation incident warrants such a response (as determined by NERSC Security). The NERSC Online CA will make a best effort to notify all relying parties about the the compromise.

5.7.4 Business continuity capabilities after a disaster

No Stipulation.

5.8 CA or RA Termination

Prior to CA termination, the NERSC Online CA will attempt to provide 30 days notice to:

1. Notify the Root CA of the termination.
2. Notify all subscribers and relying parties of the termination.
3. Make information of its termination widely available.

The NERSC Online CA will stop issuing certificates 11 days (or the maximum lifetime of a short lived certificate) prior to the termination.

6 TECHNICAL SECURITY CONTROLS

6.1 Key pair generation and installation

6.1.1 Key Pair generation

The key pair for the NERSC Online CA is generated on an offline system. The certificate is signed by the ESnet Root CA on an offline signing machine. The keys are generated using OpenSSL and must be from a verified random source. CA Key signing must happen in-person between the NERSC CA administrator and the ESnet Root CA manager.

The NERSC Online CA does not generate private keys for subjects. The key pairs for end entities (personal certificates), host or service certificates are generated by the requesting parties themselves on their own system.

6.1.2 Private key delivery to subscriber

The HSM device used by the NERSC Online CA will be physically attached to the offline system that has generated the key pair and the key will be transferred to one or more HSM devices (additional devices are used for backup).

The generated certificate (or public key) will also be transferred to removable media.

Once the key pair has been successfully copied on to all target devices, the original key will be destroyed from the initial system, so that the keys only exist on HSM devices.

The NERSC Online CA does not generate private keys for NERSC Online CA subscribers. Subscribers generate private keys themselves on their own local systems.

6.1.3 Public key delivery to certificate issuer

The MyProxy software creates an 128-bit TLS session between the client (subscriber) and the server (CA). The public key is delivered through this secure connection.

6.1.4 CA public key delivery to relying parties

The public keys or signing certificates of the NERSC online are made available to relying parties through the NERSC Online CA website. Alternatively, the certificate can also be obtained from the IGTF's TACAR repository (see Section 1.3.5) to which a copy of certificate will be securely transferred once accreditation of the NERSC Online CA has been approved by the TAGPMA.

6.1.5 Key sizes

The CA private key will be 2048 bits in length. Public RSA keys shorter than 1024 bits will not be signed.

6.1.6 Public key parameters generation and quality checking

No stipulation.

6.1.7 Key usage purposes (as per X.509 v3 key usage field)

The NERSC Online CA does not enforce key usage restrictions by any means beyond the X.509v3 extensions in the certificates it issues. Uses for an end-entity certificate may include:

a) Authentication;
b) data and key encipherment;
c) object integrity (especially messages);
d) session establishment; and
e) proxy creation and signing.

Other uses may also be permissible.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic module standards and controls

The NERSC Online CA will use a Hardware Security Module rated at FIPS 140 Level-3 (Aladdin eToken Pro64 USB) for storage of its private key. This device is installed inside the NERSC Online CA machine, via an internal USB port.

Access to the HSM device configuration requires full system administrative privileges on the CA machine. In order to access the device configuration, staff must authenticate themselves individually using a One Time Password token or a secure credential. Direct console access in the restricted server room is also permitted, since staff must be individually authenticated using an ID badge reader. Only authorized staff will be granted full system administrative privileges.

End entities may only have their certificates signed by the HSM device through the MyProxy server interface.

6.2.2 Private key (n out of m) multi-person control

No stipulation.

6.2.3 Private key escrow

No stipulation.

6.2.4 Private key backup

The NERSC Online CA private key will be backed up on two or more additional equivalent cryptographic modules. One of these HSM devices will be attached to a backup CA machine that has been configured to replace the original CA machine in case of failure. The backup CA machine will have the same physical security requirements as the primary CA machine.

Other HSM devices will be stored in a safe, with access restricted to authorized personnel.

6.2.5 Private key archival

NERSC Online CA private keys are not archived.

6.2.6 Private key transfer into or from a cryptographic module

NERSC Online CA private keys will initially be replicated on three or more (1 for the primary CA machine, 1 for the backup CA machine, and 1 or more in a secure offline location) identical cryptographic storage modules in a secure manner. After that point they will not be exported from the cryptographic modules. During the replication process, the private key never exists in plain-text form on intermediate storage devices. All private key plain-text operations are performed in memory, which is cleared when the source machine is powered down.

6.2.7 Private key storage on cryptographic module

NERSC Online CA private keys are stored in an encrypted form on hardware security modules meeting the FIPS 140 level 3 cryptographic requirements.

6.2.8 Method of activating private key

The private key is activated automatically by the server software on startup to allow immediate SLCS CA operation. The key is activated by a PIN known to the server software and to the NERSC Online CA administrator.

6.2.9 Method of deactivating private key

The private key may be deactivated by

1. Disabling the HSM device through software utilities.
2. Physically removing the HSM device from the CA machine.
3. Powering off the CA machine.

6.2.10 Method of destroying private key

The NERSC Online CA administrator can reinitialize the HSM to destroy the private key.

6.2.11 Cryptographic Module Rating

The hardware security modules meet FIPS 140 level 3.

6.3 Other aspects of key pair management

6.3.1 Public key archival

The public key will be archived along with regular system backups of the NERSC Online CA machine.

6.3.2 Certificate operational periods and key pair usage periods

The certificate for NERSC Online CA will have a maximum lifetime of 10 years.

End entity certificates signed by the NERSC Online CA will have a lifetime of not more than 1 million seconds.

6.4 Activation data

6.4.1 Activation data generation and installation

The NERSC Online CA private key is activated by a PIN. The PIN should be at least 10 characters long, should contain at least 1 numeric and 1 alphabetic character and should not contain common dictionary words or well known sequences of characters.

6.4.2 Activation data protection

The PIN will only be known to
1. NERSC CA software used to generate certificates
2. NERSC CA System Administrative Staff
3. NERSC Operators

A copy of the PIN will reside in a locked safe, with access restricted to authorized personnel. The only other unencrypted copy of the PIN will reside on the NERSC CA machine itself, for the CA software to activate the HSM. This copy will be protected by file system permissions. Only authorized system administrative staff will be able to access the PIN, and must authenticate themselves using an OTP token or secure credential before they can access the PIN. Direct console access regulated by an ID badge reader will also be permitted.
Additionally the HSM device will only use a single PIN. A second "administrator" PIN with master override capabilities will not be configured.

6.4.3 Other aspects of activation data

Not defined.

6.5 Computer security controls

6.5.1 Specific computer security technical requirements

The NERSC Online CA software runs on a dedicated machine, running no other services than those needed for the CA operations. The server's network is protected by a dedicated hardware firewall, and the server itself runs an operating system firewall. The server is monitored via a network-based intrusion detection system (BRO). Login access is subject to hardware-based one-time password authentication using hardware tokens

and permitted only for administrative personnel that require access to the system for its operation.

6.5.2 Computer security rating

No stipulation.

6.6 Life cycle technical controls

No stipulation.

6.7 Network security controls

Network security controls (software and hardware firewalls) allow inbound connections only for certificate requests and download of CA certificates and CRLs from hosts outside the NERSC network.

6.8 Time-stamping

No stipulation.

7 CERTIFICATE, CRL, AND OCSP PROFILES

7.1 Certificate profile

End-entity certificates will be X.509v3, compliant with RFC 3280.

7.1.1 Version number(s)

The version number will have a value of 2 indicating a Version 3 certificate.

7.1.2 Certificate extensions

For user certificates:

- Basic Constraints (critical): CA:false
- X.509v3 Subject Key Identifier
- X.509v3 Authority Key Identifier
- X.509v3 Certificate Policies: OID:
    - CP/CPS OID: 1.2.840.113613.1.5.1.0
    - SLCS OID: 1.2.840.113612.5.2.2.3.2.1
- Key Usage (critical): Digital Signature, Key Encipherment, Data Encipherment
- SubjectAltName: For user certificates, the NERSC email address of the subscriber responsible for the certificate.
- crlDistributionPoints: URI of DER formatted CRL

7.1.3 Algorithm object identifiers

- Hash Function: id-sha1 1.3.14.3.2.26
- RSA Encryption: rsaEncryption 1.2.840.113549.1.1.1
- Signature Algorithm: sha1WithRSAEncryption 1.2.840.113549.1.1.5

7.1.4 Name forms

Each end entity will be given a unique and unambiguous Distinguished Name (DN) by the NERSC Online CA. The DN will be of the form:
/DC=gov/DC=nersc/OU=People/CN=*Full Name UID*
Where *Full Name* is the full name of the subscriber and *UID* is a unique identifier that is uniquely and persistently associated with the subscriber to disambiguate naming conflicts.

7.1.5 Name constraints

All certificate issued by the NERSC Online CA will have the following prefix:
/DC=gov/DC=nersc
There are no other name constraints than those that are to be derived from the stipulations in Sections 7.1.4, 3.1.2 and 3.1.1.

7.1.6 Certificate policy object identifier

Each NERSC Online CA certificate policy has a unique associated object identifier (OID). The OID for this policy is given in Section 1.2.

7.1.7 Usage of Policy Constraints extension

No stipulation.

7.1.8 Policy qualifiers syntax and semantics

No stipulation.

7.1.9 Processing semantics for the critical Certificate Policies extension

No stipulation.

7.2 CRL Profile

The NERSC Online CA may not publish CRLs for certificates with a lifetime of under 24 hours. Revocation services and CRLs will be supported for revoked certificates that have a lifetime of more than 24 hours.

7.2.1 Version number(s)

The NERSC Online CA will create and publish X.509 version 1 CRLs.

7.2.2 CRL and CRL entry extensions

The NERSC Online CA must publish a CRL with currently active certificates that have been revoked. It is not required to include stale or expired certificates that have been revoked.

Each CRL entry will include the revoked certificate's serial number and the date of revocation.

7.3 OCSP Profile

Not currently supported.

7.3.1 Version number(s)

Not Applicable

7.3.2 OCSP extensions

Not Applicable

8 Compliance Audit and Other Assessment

The NERSC Online CA will accept being audited by the TAGPMA to verify compliance with the rules and procedures specified in this document. The NERSC Online CA will also undergo internal audits to verify compliance with this document, and NERSC security policy on an annual basis minimally.

8.1 Frequency or circumstances of assessment

The NERSC Online CA shall carry out an internal audit annually, to check the compliance of the operation with the CP/CPS document in effect, when deemed necessary by the NERSC Networking And Security Team.

It is recommended that this audit take place following any major revisions to the CP/CPS.

The NERSC Online CA will also accept being periodically audited by the TAGPMA, as recommended by the current SLCS profile.

8.2 Identity/qualifications of assessor

Internal Audit: Assessor must be authorized by the NERSC Networking And Security Team to conduct an audit.
TAGPMA Audit: Assessor must be authorized by TAGPMA, and NERSC to conduct an audit. Assessor must additionally meet NERSC access requirements as defined by current NERSC security policy.

8.3 Assessor's relationship to assessed entity

No Stipulation.

8.4 Topics covered by assessment

The audit will verify that the services provided by the CA comply with the latest approved version of the CP/CPS.

8.5 Actions taken as a result of deficiency

If an assessment reveals a conflict between the provisions of the CP/CPS document and actual practice, the NERSC online CA must either update the CP/CPS to reflect current practice, or it must announce steps to alter current practice so that it meets the requirements defined by the CP/CPS.

Specific actions will be defined on a case-by-case basis.

8.6 Communication of results

Results of internal audits will be made available to NERSC Networking And Security Team personnel and the NERSC Online CA administrative staff.

Results of a TAGPMA audit will be made available to the TAGPMA.

In case the audit reveals confidential or sensitive information that could compromise the security of NERSC, the NERSC Online CA or its subscribers, the results may be limited to authorized parties at the discretion of the NERSC Networking And Security Team.

9 OTHER BUSINESS AND LEGAL MATTERS

No fees will be charged by the NERSC Online CA nor any refunds given. No financial responsibility is accepted.

9.1 Fees

NERSC Online CA does not currently charge fees for services provided

9.1.1 Certificate issuance or renewal fees

Not Applicable

9.1.2 Certificate access fees

Not Applicable

9.1.3 Revocation or status information access fees

Not Applicable

9.1.4 Fees for other services

Not Applicable

9.1.5 Refund policy

Not Applicable

9.2 Financial responsibility

NERSC funds the costs associated with the NERSC Online CA.

9.2.1 Insurance coverage

No stipulation.

9.2.2 Other assets

No stipulation.

9.2.3 Insurance or warranty coverage for end-entities

No stipulation.

9.3 Confidentiality of business information

9.3.1 Scope of confidential information

NERSC Online CA maintains subscribers' full names and UIDs. Some of this information is used to construct unique, meaningful subject names in the issued certificates.

NERSC Online CA accepts a TLS encrypted password to authenticate the user. This password is considered confidential and will always be encrypted in any communications between the CA software modules.

9.3.2 Information not within the scope of confidential information

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

9.3.3 Responsibility to protect confidential information

NERSC Online CA does not have access to or generate the private keys of a digital signature key pair, such as those used in user certificates. These key pairs are generated and managed by the client and are the sole responsibility of the subscriber.

Lawrence Berkeley National Laboratory operates NERSC computer systems under contract to the U.S. Department of Energy. NERSC computer systems are the property of the United States Government and are for authorized use only. Users (authorized or unauthorized) have no explicit or implicit expectation of privacy. Any or all uses of a NERSC system and all files on the system may be intercepted, monitored, recorded, copied, audited, inspected, and disclosed to site, Department of Energy, and law enforcement personnel, as well as authorized officials of other agencies, both domestic and foreign. By using a NERSC system, the user consents to such interception, monitoring, recording, copying, auditing, inspection, and disclosure at the discretion of authorized site or Department of Energy personnel.

9.4 Privacy of personal information

9.4.1 Privacy plan

No stipulation.

9.4.2 Information treated as private

No stipulation

9.4.3 Information not deemed private

No stipulation

9.4.4 Responsibility to protect private information

No stipulation

9.4.5 Notice and consent to use private information

No stipulation

9.4.6 Disclosure pursuant to judicial or administrative process

No stipulation

9.4.7 Other information disclosure circumstances

No stipulation

9.5 Intellectual property rights

The NERSC Online CA asserts no ownership rights in certificates issued to subscribers.

Acknowledgment is hereby given to the NCSA PKI, the DOEGrids CA and to the UFF BrGrid CA for inspiration of parts of this document.

9.6 Representations and warranties

9.6.1 CA representations and warranties

The NERSC Online CA makes no guarantee about the security or suitability of an entity that is identified by a NERSC certificate. The NERSC Online CA 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.

9.6.2 RA representations and warranties

No stipulation

9.6.3 Subscriber representations and warranties

No stipulation

9.6.4 Relying party representations and warranties

No stipulation

9.6.5 Representations and warranties of other participants

No stipulation

9.7 Disclaimers of warranties

The NERSC Online CA denies any financial or any other kind of responsibility for damages or impairments resulting from its operation.

9.8 Limitations of liability

The NERSC Online is operated substantially in accordance with NERSC's own risk analysis. No liability, explicit or implicit, is accepted.

9.9 Indemnities

No stipulation.

9.10 Term and termination

9.10.1 Term

This policy becomes effective on its approval by the TAGPMA.

9.10.2 Termination

This policy may be terminated at any time without warning.

9.10.3 Effect of termination and survival

No stipulation.

9.11 Individual notices and communications with participants

No stipulation.

9.12 Amendments

9.12.1 Procedure for amendment

Changes to this document will be presented to the TAGPMA for approval before taking effect.

9.12.2 Notification mechanism and period

Best effort notification of all relying parties will be made with as much advance notice as possible.

9.12.3 Circumstances under which OID must be changed

Any substantial change of policy will incur a change of OID.

9.13 Dispute resolution provisions

NERSC will resolve all disputes regarding this policy.

9.14 Governing law

Interpretation of this policy is according to the laws of the United States of America and the State of California, where the conforming CA is established.

9.15 Compliance with applicable law

Unauthorized or improper use of a NERSC system may result in administrative disciplinary action and civil and criminal penalties.

9.16 Miscellaneous provisions

9.16.1 Entire agreement

No stipulation.

9.16.2 Assignment

No stipulation

9.16.3 Severability

No stipulation

9.16.4 Enforcement (attorneys' fees and waiver of rights)

No stipulation

9.16.5 Force Majeure

No stipulation.

9.17 Other provisions

No stipulation.

10 References

1. Profile for SLCS X.509 Public Key Certification Authorities with Secured Infrastructure Version 2.1; S. Cholia (editor).

2. RFC 3647, Internet X.509 Infrastructure Certificate Policy and Certification Practices Framework; S. Chokani, W. Ford, R. Sabett and S.Wu; November 2003; http://www.ietf.org/rfc/rfc3647.txt.

3. MyProxy Credential Management Service; http://grid.ncsa.uiuc.edu/myproxy/.

4. Nersc Information Management System; http://www.nersc.gov/nusers/accounts/nim/.

5. Grid Certificate Profile; D. Groep, M. Helm, J. Jensen, M. Sova, S. Rea, R. Karlsen-Masur, U. Epting, M. Jones; May 2007.

6. The UFF Brazilian Grid Certification Authority Certificate Policy and Certification Practice Statement Version 1.0; July 2006.

7. Certificate Policy and Practice Statement for the NCSA SLCS Version 1.1; April 2007

8. DOE Grids Certificate Policy And Certification Practice Statement Version 2.9; December 2006.

9. RFC 2119, Key words for use in RFCs to Indicate Requirement Levels; S. Brader; March 1997; http://www.ietf.org/rfc/rfc2119.txt.

10. Energy research Computer Allocations Process; http://www.nersc.gov/nusers/accounts/allocations/ercap/.

11. DOE Office of Science Mission Statements; http://www.nersc.gov/nusers/accounts/allocations/ercap/mission.php.

12. NERSC Accounts and Allocations; http://www.nersc.gov/nusers/accounts/.

13. ESnet Root CA Certificate Policy And Certification Practice Statement Version 1.3; September 2003; T. Genovese

14. RFC 3280, Internet X.509 Public Key Infrastructure: Certificate and Certificate Revocation List (CRL) Profile; R. Housley, W. Polk, W. Ford and D. Solo; April 2002. http://www.ietf.org/rfc/rfc3280.txt.

15. Bro Intrustion Detection System; http://www.bro-ids.org/.

16. LBNL Regulations and Procedures Manual; http://www.lbl.gov/Workplace/RPM/