Certificate Policy and Practice Statement for the NCSA CA

National Center for Supercomputing Applications (NCSA)

Version 1.1 (Wed Apr 4 09:17:51 CDT 2007)

Contents

1 INTRODUCTION

1.1 Overview

This Certificate Policy and Practice Statement (herein referred to as the ”Policy”) specifies minimum requirements for the issuance and management of digital certificates that shall be used in authenticating users accessing National Center for Supercomputing Application at the University of Illinois (herein referred to as ”NCSA”) resources and the resources of other entities (relying parties) which accept those certificates. The Policy is issued and administered under the authority of the NCSA Policy Management Authority (herein referred to as the ”PMA”; see Section 1.4.2 for contact details). This document is structured according to Internet Engineering Task Force RFC 3647 (Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework).

NCSA runs two CAs. Each CA has it own key and certificate. It is expected that relying parties will trust both CAs, though a relying party may choose to trust only one CA or the other. These two CAs taken together along with the associated software and repositories used to distribute policies, CRLs and the like, are referred to as the ”NCSA PKI”. One CA issues only short-lived certificates (with one week or shorter lifetime) to users and is henceforth referred to as the “NCSA Short-lived Certificate Service” or “NCSA-SLCS”. One CA is a traditional CA that issues long-lived certificates to hosts, services and users requiring long-lived certificates. This CA is henceforth referred to as the “NCSA-CA”. It is expected that users will use the NCSA-SLCS for user certificates unless they have some need for a long-lived certificate.

This document covers the policy that applies to the NCSA-CA. Figure 1 illustrates the overall architecture of the NCSA-CA. The CA is integrated with the NCSA user database and Kerberos authentication service for identity management. The NCSA accounting process enrolls users in the user database, creates a Kerberos account with an initial default password for them, and assigns them a distinguished name. To obtain credentials, NCSA-CA subscribers run software on the host where their credentials are to be stored. The software generates the subscriber’s private key locally, authenticates the user to the NCSA-CA via Kerberos and their “default password” (two authentication factors), issues a signed certificate request to the CA, and, if the request is approved, receives a signed certificate from the CA. The NCSA-CA looks up the distinguished name in the user database that corresponds to the user’s authenticated identity, then issues a certificate with the appropriate distinguished name. For host and service certificate requests, the NCSA-CA also queries the NCSA Host database, maintained by NCSA networking staff, to verify the authenticated user is a registered administrator for the requested host. Further policy and implementation details are provided throughout the document.

1.2 Document name and identification

Document title: Certificate Policy and Practice Statement for the NCSA CA
This Policy is published at: `http://security.ncsa.uiuc.edu/CA/`
Document version: 1.1
Document date: Wed Apr 4 09:17:51 CDT 2007
OID: 1.3.6.1.4.1.4670.100.1.1

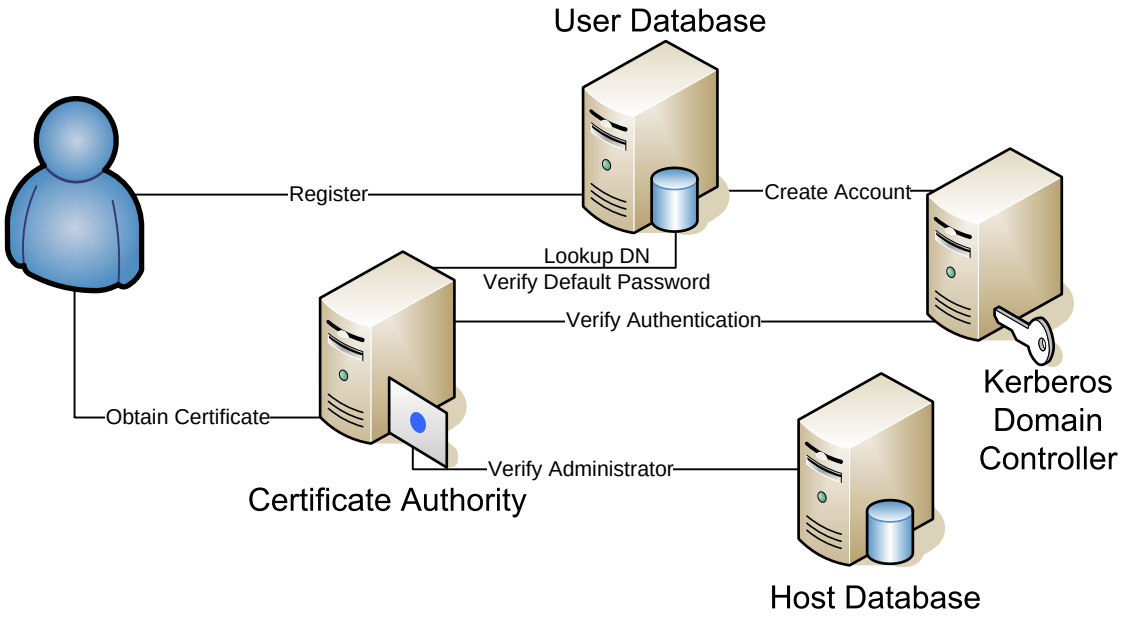

Figure 1: NCSA CA Architecture

1.3 PKI participants

1.3.1 Certification authorities

This policy is valid for the NCSA-CA. The NCSA-CA will only sign end entity certificates. There are no subordinate CAs.

1.3.2 Registration authorities

NCSA allocations group staff serve as registration authorities for the NCSA-CA. They enroll users in the NCSA user database according to the enrollment process described in Section 4.1.2, create Kerberos accounts for new users, assign a default password for the account, and assign distinguished names to new users according to Section 3.1. The NCSA-CA uses the Kerberos service to authenticate requests and queries the database to obtain the proper distinguished name for authenticated requesters. The NCSA-CA also uses the database to authenticate users' default passwords as a "second authentication factor". The NCSA user database and Kerberos service are used to authenticate NCSA's users and staff for access to NCSA high-performance computing resources, NCSA's email services and other production services.

Users are instructed to change their default password immediately upon receiving their account information and to keep their default password in a secure place for later reference. In the event that their current password is forgotten, it will be reset to this default. The default password is used as a "second authentication factor" in certificate requests, along with the user's current Kerberos password.

NCSA networking group staff serve a registration authority role for host and service certificate requests by maintaining a database of all NCSA hosts and their authorized system administrator(s). This allows requests for service certificates from a host's authorized administrator (authenticated via Kerberos) to be automatically processed. Requests for hosts that do not appear in this database (e.g., services run by NCSA collaborators) will be manually vetted by NCSA operations staff.

1.3.3 Subscribers

The NCSA-CA will serve the needs of the NCSA community by providing users and services at NCSA with x509v3 digital certificates. These certificates may be used for the purpose of authentication, encryption, and digital signing by those individuals to whom the certificates have been issued.

The CA will also issue server and service certificates to computers operating within the NCSA administrative domain and to computer systems from other domains that are providing services in support of NCSA projects.

Persons receiving certificates will be users of NCSA's computational facilities or staff employed at NCSA.

1.3.4 Relying parties

NCSA places no restrictions on who may accept certificates it issues.

1.3.5 Other participants

No stipulation.

1.4 Certificate usage

1.4.1 Appropriate certificate uses

One of the purposes of this policy is to promote a wide use of public-key certificates in many different applications. These applications may include, but are not limited to, login authentication, job submission authentication, encrypted e-mail, and SSL/TLS encryption for applications capable of making use of these technologies.

1.4.2 Prohibited certificate uses

Other uses of NCSA-CA certificates are not prohibited, but neither are they supported.

1.5 Policy administration

1.5.1 Organization administering the document

This policy is administered by the National Center for Supercomputing Applications at the University of Illinois, 1205 W. Clark, Urbana IL 61801 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 NCSA-CA is the Head of Security Operations for NCSA:

James J. Barlow
Phone number: +1 217-244-6403
Postal address: 1205 W. Clark, Urbana IL 61801 USA
E-mail address: jbarlow@ncsa.uiuc.edu
After hours contact information:
NCSA Security Operations and Incident Response: security@ncsa.uiuc.edu
NCSA 24x7 Operations: +1 217-244-0710

1.5.3 Person determining CPS suitability for the policy

The Head of Security Operations for NCSA leads the PMA for the CA and is ultimately responsible for determining the suitability of the CPS.

As an accredited policy of the TAGPMA, all policy changes are subject to TAGPMA review and approval.

1.5.4 CPS approval procedures

As determined by TAGPMA and the Head of Security Operations for NCSA.

1.6 Definitions and acronyms

Certification Authority (CA) - An authority trusted by one or more users to create and assign public key certificates. Optionally the CA may create the user's keys. It is important to note that the CA is responsible for the public key certificates during their whole lifetime, not just for issuing them.

CA-certificate - A certificate for one CA's public key issued by another CA or self signed.

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 path - An ordered sequence of certificates which, together with the public key of the initial object in the path, can be processed to obtain that of the final object in the path.

Certification Practice Statement (CPS) - A statement of the practices, which a certification authority employs in issuing certificates.

Certificate revocation list (CRL) - A CRL is a time stamped list identifying revoked certificates, which is signed by a CA and made freely available in a public repository.

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).

Public Key Certificate (PKC) - A data structure containing the public key of an end entity and some other information, which is digitally signed with the private key of the CA which issued it.

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). Note: The term Local Registration Authority (LRA) is used elsewhere for the same concept.

Relying party - A recipient of a certificate who acts in reliance on that certificate and/or digital signatures verified using that certificate. In this document, the terms ”certificate user” and ”relying party” are used interchangeably.

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.

IPR - Intellectual Property Rights

2 PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 Repositories

The NCSA PKI will maintain a repository at `http://security.ncsa.uiuc.edu/CA/`.

2.2 Publication of certification information

This repository will contain:

- Self-signed, PEM-formatted certificates for all CAs in the NCSA PKI
- PEM-formatted CRLs for the NCSA-CA
- General information about the NCSA PKI
- The most recent copies of all Certificate Policies for the NCSA PKI CAs

2.3 Time or frequency of publication

The CRL will be published immediately after a certificate has been revoked as well as on a daily basis. The CRL This Update field will indicate the issue date of the CRL, and the Next Update field will be set to one week in the future, to indicate a one week validity period for the CRL.

The Policy shall be published immediately following any update.

2.4 Access controls on repositories

There are no restrictions on access to the repositories. Best effort will be provided to maintain their availability 24x7.

As a member of the TAGPMA, NCSA grants the IGTF and its PMAs the right of unlimited redistribution of this information.

3 IDENTIFICATION AND AUTHENTICATION

3.1 Naming

3.1.1 Types of names

Subject distinguished names are X.500 names, with components varying depending on the type of certificate.

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 serial number appended in the case of name conflicts.

The CN component of the subject name in service certificates includes the fully qualified DNS name of the service, which is usually that of the host supporting the service. The structure of a service's CN is designed to support SSL, TLS and Globus services.

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 NCSA PKI begin with C=US, O=National Center for Supercomputing Applications. The next component will be one of:

- OU=Certificate Authorities : for a CA's certificate. A CN component will follow the OU, naming the CA. All CA certificates will be self-signed.

  The distinguished name for the NCSA-CA is C=US, O=National Center for Supercomputing Applications, OU=Certificate Authorities, CN=CACL.

  Note: CACL is the name of the software implementing this CA.

- OU=Services : for a service (including a host) certificate issued by the NCSA-CA. A CN component will follow the OU, naming the service and the fully qualified domain name (FQDN) at which the service can be contacted, separated by a slash character. When the service is https, the service name and separator will be absent. For example:

C=US, O=National Center for Supercomputing Applications, OU=Services, CN=ca.ncsa.uiuc.edu

- OU=People : for a user's certificate issued by the NCSA-CA. A CN component will follow the OU, containing the user's full name and, if needed, a numeric value to disambiguate the name from other users with the same name. For example:

  C=US, O=National Center for Supercomputing Applications, OU=People, CN=James J. Barlow

3.1.5 Uniqueness of names

Each subject name issued by the NCSA PKI will be issued to one and only one individual as identified by a record in the user database. The user database management system implements checks to ensure the uniqueness of assigned distinguished names. User records are never purged from the database or reused, to ensure that distinguished names will never be reassigned to another individual. The NCSA-CA and NCSA-SLCS may issue certificates with identical names, but only to the same individual. All names will be prefixed with the relative DN form of C=US, O=National Center for Supercomputing Applications to provide a globally unique namespace. A unique "common name" is assigned to each user consisting of their legal name with a serial number appended in the case of name conflicts. This common name along with the prefix create globally-unique distinguished names used in certificates issued by the NCSA PKI to users. For service certificates, the combination of service name and fully qualified domain name of the host on which the service resides serves to disambiguate the name.

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.

3.2.2 Authentication of organization identity

NCSA users are identified by their presence in the NCSA user database. Users obtain entries in the database according to the procedure described in 4.1.2.

3.2.3 Authentication of individual identity

User identity will be authenticated via Kerberos, with the authenticated Kerberos principal name mapped to a unique "common name" via the NCSA user database. The NCSA-CA also uses the database to authenticate users' "default passwords" as a "second authentication factor" as described in Section 1.3.2.

3.2.4 Non-verified subscriber information

Subscriber name and postal address are verified by NCSA's account creation process. Other gathered information is not verified.

3.2.5 Validation of authority

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

Requests for service certificates must come from a valid NCSA User and will be checked against NCSA's database of registered system administrators to ensure the user is a legitimate system administrator for the service identified in the certificate subject name.

3.2.6 Criteria for interoperation

The NCSA PKI is intended to interoperate with other CAs within TeraGrid and the International Grid Trust Federation.

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.

3.3.2 Identification and authentication for re-key after revocation

If the compromise was limited to just the private key, the request for re-key will be treated as an initial registration. If the compromise involved a user's password, that password will be reset via postal mail to the user's known postal address.

3.4 Identification and authentication for revocation request

CA Certificates will only be revoked at the instigation of NCSA Operational Security personnel.

Users may request revocation by contacting NCSA Security Operations. Requests will be handled as deemed appropriate by NCSA Security Operations.

Requests for revocation of service certificates from NCSA computer security personnel and from administrators of the systems hosting the services in question will be honored.

4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 Certificate Application

4.1.1 Who can submit a certificate application

Any user who appears in NCSA's User Database may request a certificate.

4.1.2 Enrollment process and responsibilities

NCSA allocations group staff serve as registration authorities for the NCSA-CA. They enroll users in the NCSA user database according to the following enrollment process. Additional details are available at `http://www.ncsa.uiuc.edu/UserInfo/Allocations/`.

To receive an entry in NCSA's user database, a user must satisfy one of the following conditions:

- Be an NCSA employee
- Have a guest account requested by NCSA management for key NCSA collaborators
- Be a Principal Investigator (PI) with a allocation on NCSA computational resources approved through an NSF-approved peer review process
- Have a project account requested on their behalf by an existing PI using that PI's allocation

Identity vetting of NCSA employees is performed in person as part of the University of Illinois hiring process, in collaboration with the NCSA Human Resources department. Identity vetting of guest accounts requires direct personal contact of an NCSA staff member, who takes responsibility for that person's account. Guest account requests are reviewed and approved by NCSA management and allocations group staff.

Identity vetting for PIs is performed via peer review. PIs submit proposals for supercomputing allocations to a Resource Allocations Committee, which consists of volunteers selected from the faculty and staff of U.S. universities, laboratories and other research institutions. All members serve a term of 2–5 years and have expertise in computational science or engineering. Each proposal is assigned to two committee members for review. The committee members can also solicit an external review. After several weeks of review, the entire committee convenes to discuss the relative merits of each proposal and award time based on availability of resources. To apply, the principal investigator (PI) must be a researcher or educator at a U.S. academic or non-profit research institution.

Proposals are judged on the following criteria:

- Scientific merit: sound scientific goals and approaches of high merit; timely problems of interest to researchers and scientists
- Potential for progress: a PI with a verifiable record of success, indicated by publications or other measures, with the necessary resources to conduct the proposed research
- Numerical approach: codes that employ correct and efficient numerical algorithms; a selection of temporal/spatial resolution that is appropriate for the research

- Justification for resources: an appropriate amount of time has been requested; proposed research requires the use of a supercomputer; applications have been optimized to achieve high single-processor and parallel performance; good scaling of applications on a parallel machine

Allocations are typically awarded for one year, though multi-year allocations may be granted for well-known PIs. PIs can submit renewal or supplemental proposals to the committee to extend their allocation.

PIs are instructed not to share their accounts with others. Instead, they use the Add User Form on the TeraGrid User Portal to request accounts for their project members. PIs can also use this form to remove project members. Access to this form requires authentication via Kerberos username and password. PIs submit name, telephone, and address information for the users on their project. For users on multiple projects, each project PI must complete the required information separately for each user to request the user to have access to the project's resources. The PI is notified by postal mail whenever a user is added to their project. All users are required to sign the TeraGrid User Responsibility Form, which educates users about secure and appropriate computing practices.

When a user no longer has any active projects, the user's Kerberos account is removed. User database entries are kept indefinitely for historical purposes.

All initial user passwords are distributed by postal mail. If a user requires a new password (e.g., they have lost their password), it will only be distributed via U.S. postal mail to their known address. Each user is assigned a unique username used as their Kerberos principal and Unix login name as described in 3.1.5.

4.2 Certificate application processing

4.2.1 Performing identification and authentication functions

The NCSA-CA authenticates all certificate requests as described in Section 3.2.3.

4.2.2 Approval or rejection of certificate applications

Certificate applications will be approved if the applicant can be authenticated and, in the case of service certificates, is validated as an authorized system administrator for the host in question, as described in Section 3.2.3.

4.2.3 Time to process certificate applications

Certificate applications are processed automatically.

4.3 Certificate issuance

4.3.1 CA actions during certificate issuance

Certificate applications are processed automatically.

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 never storing them on a networked file system or otherwise transmitting them over a network and never sharing them between people.
- Ensure that the private keys corresponding to their issued service certificates are stored in a manner that minimizes the risk of exposure.
- Observe restrictions on private key and certificate use.
- Promptly notify the CA operators of any incident involving a possibility of exposure of a private key.

4.5.2 Relying party public key and certificate usage

Relying parties must

- Be cognizant of the provisions of this document.
- Verify any self-signed CA certificates to their own satisfaction using out-of-band means.
- Accept responsibility for checking any relevant CRLs before accepting the validity of a certificate.

- Observe restrictions on private key and certificate use.
- Not presume any authorization of an end entity based on possession of a certificate from the NCSA PKI or its corresponding private key.

4.6 Certificate renewal

Certificates in the NCSA PKI are not explicitly renewed. Instead the original subscriber may request a new certificate, using the normal certificate issuance process.

4.7 Certificate re-key

Certificates in the NCSA PKI are not explicitly re-keyed. Instead the original subscriber may request a new certificate, using the normal certificate issuance process.

4.8 Certificate modification

Certificates in the NCSA PKI are not modified. Instead new certificates will be issued using the normal certificate issuance process.

4.9 Certificate revocation and suspension

4.9.1 Circumstances for revocation

Certificates issued by the NCSA-CA will be revoked in any of the following circumstances:

- The private key is suspected or reported to be lost or exposed.
- The information in the certificate is believed to be, or has become inaccurate.
- The certificate is reported to no longer be needed.

4.9.2 Who can request revocation

NCSA Security Operations personnel may request revocation of any certificate issued by the NCSA-CA.

The original subscriber for a certificate may request its revocation.

Entities other than the subscriber who suspect a certificate issued by the NCSA PKI may be compromised should contact NCSA Security Operations.

4.9.3 Procedure for revocation request

Requests for revocation should be made by email to security@ncsa.uiuc.edu or by phone to NCSA Operations 217-244-0710.

4.9.4 Revocation request grace period

No constraints.

4.9.5 Time within which CA must process the revocation request

Revocation requests will be processed with best effort as quickly as possible.

4.9.6 Revocation checking requirement for relying parties

Relying parties are advised to obtain and consult a valid CRL from `http://security.ncsa.uiuc.edu/CA/`

4.9.7 CRL issuance frequency (if applicable)

CRLs are issued when a certificate is revoked.

CRLs are issued daily.

4.9.8 Maximum latency for CRLs (if applicable)

One day.

4.9.9 On-line revocation/status checking availability

Aside from the published CRL, no on-line certificate status checking is available.

4.9.10 Other forms of revocation advertisements available

None.

4.9.11 Special requirements re key compromise

None.

4.10 Certificate status services

Aside from the published CRL, no on-line certificate status checking is available.

4.11 End of subscription

Subscribers may end their subscription by requesting revocation of their certificate.

4.12 Key escrow and recovery

No key escrow is performed.

5 FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

5.1 Physical controls

5.1.1 Site location and construction

The NCSA-CA server will be located in NCSA's machine room in the Advance Computation Building (ACB) on the University of Illinois at Urbana-Champaign campus.

5.1.2 Physical access

NCSA occupies all of ACB with the exception of space dedicated to mechanical systems and custodians. ACB entrances and computer rooms are locked at all times and use a keycard system to gain entry. Video cameras are located at all entrances and are monitored by staff in the control room. An intercom and remote lock release system is used at the main entrance to allow entry to authorized personnel who do not have keycard access. ACB is not open to the general public and is staffed 24x7x365.

5.1.3 Power and air conditioning

No stipulation.

5.1.4 Water exposures

No stipulation.

5.1.5 Fire prevention and protection

No stipulation.

5.1.6 Media storage

No stipulation.

5.1.7 Waste disposal

No stipulation.

5.1.8 Off-site backup

Audit logs are archived weekly to a secondary storage facility at the Beckman Institute on the University of Illinois at Urbana-Champaign campus.

5.2 Procedural controls

All persons with access to the systems hosting the NCSA-CA will be full-time NCSA employees. Personnel will be NCSA Operations staff, NCSA Security Operations staff, and NCSA System administration staff.

When any person with access to the NCSA-CA systems leaves NCSA or their administrative role, their access will be revoked and any relevant passwords changed.

NCSA will perform an operational audit of the CA/RA staff at least once per year. A list of CA and site identity management personnel will be maintained and verified at least once per year.

5.3 Personnel controls

Operators of the NCSA-CA will be qualified system administrators and operators at NCSA.

5.4 Audit logging procedures

5.4.1 Types of events recorded

The following items will be logged and archived:

- Certificate requests
- Certificate issuance

- Certificate revocations
- Issued CRLs
- Attempted and successful accesses to the systems hosting the NCSA PKI, and reboots of those systems

The NCSA user database maintains contact information for all subscribers.

5.4.2 Frequency of processing log

No stipulation.

5.4.3 Retention period for audit log

Audit logs are maintain indefinitely on NCSA's mass storage system in ACB.

5.4.4 Protection of audit log

No stipulation.

5.4.5 Audit log backup procedures

Audit logs are archived weekly to a secondary storage facility at the Beckman Institute on the University of Illinois at Urbana-Champaign campus.

5.4.6 Audit collection system (internal vs. external)

No stipulation.

5.4.7 Notification to event-causing subject

No stipulation.

5.4.8 Vulnerability assessments

No stipulation.

5.5 Records archival

The CA records and archives all requests for certificates, all issued certificates, all revocation requests, all issued CRLs, and the login/logout/reboot of the issuing machine. The CA keeps these records for at least three years. These records will be be made available to external auditors in the course of their work as auditor.

5.6 Key changeover

Best effort will be made to notify relying parties of any new public key for the NCSA-CA, and it may then be obtained in the same manner as the previous NCSA-CA certificates.

5.7 Compromise and disaster recovery

5.7.1 Incident and compromise handling procedures

All incidents will be handled by NCSA Security Operations and Incident Response as they determine appropriate.

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

No stipulation.

5.7.3 Entity private key compromise procedures

Any private key compromise will result in revocation of the associated certificate.

5.7.4 Business continuity capabilities after a disaster

No stipulation.

5.8 CA or RA termination

No stipulation.

6 TECHNICAL SECURITY CONTROLS

6.1 Key pair generation and installation

6.1.1 Key pair generation

The NCSA-CA does not generate any private keys but its own.

User private keys will be generated by client software on the host where they will be stored. They will be stored on non-networked filesystems.

System and service administrators will generate private keys for their services, on the service hosts themselves if at all possible.

6.1.2 Private key delivery to subscriber

Not necessary.

6.1.3 Public key delivery to certificate issuer

Public keys are delivered under Kerberos authentication and integrity protection.

6.1.4 CA public key delivery to relying parties

The public keys of NCSA PKI CAs are available at `http://security.ncsa.uiuc.edu/CA/`.

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 NCSA-CA does not enforce key usage restrictions by any means beyond the X.509v3 extensions in the certificates it issues. In User and Service certificates, those extensions will mark the associated keys as valid for Digital Signature and Key Encipherment. CA certificates will have the Key Usage extension set to allow Digital Signature, Certificate Signing, and CRL Signing.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic module standards and controls

The NCSA-CA will use a FIPS 140-2 level 3 Hardware Security Module (SafeNet Luna PCI) for storage of its private key.

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

No stipulation.

6.2.3 Private key escrow

NCSA-CA private keys are not escrowed.

6.2.4 Private key backup

NCSA-CA private key is replicated on two identical cryptographic modules on two identical hosts in the NCSA machine room to provide for failure protection. If a system hosting one CA should fail, that CA will temporarily be hosted on the other system until such time as a replacement system can be arranged.

6.2.5 Private key archival

NCSA-CA private keys are not archived.

6.2.6 Private key transfer into or from a cryptographic module

NCSA-CA private keys will initially be replicated on two identical cryptographic storage modules in a secure manner. After that point they will not be exported from the cryptographic modules.

6.2.7 Private key storage on cryptographic module

NCSA-CA private keys are stored on cryptographic modules meeting FIPS 140-2 level 3.

6.2.8 Method of activating private key

The private key is activated automatically at server startup to allow immediate NCSA-CA operation.

6.2.9 Method of deactivating private key

HSM utilities on the server support deactivating the private key.

6.2.10 Method of destroying private key

The HSM Security Officer can reinitialize the HSM to destroy the private key.

6.2.11 Cryptographic Module Rating

The hardware security modules meet FIPS 140-2 level 3.

6.3 Other aspects of key pair management

6.3.1 Public key archival

No stipulation.

6.3.2 Certificate operational periods and key pair usage periods

The certificate for NCSA-CA will have a lifetime of 10 years.

NCSA-CA User and Service certificates will have a lifetime of not more than one year.

6.4 Activation data

No stipulation.

6.5 Computer security controls

6.5.1 Specific computer security technical requirements

The NCSA-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 both host-based and network-based intrusion detection systems. 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 NCSA's network.

6.8 Time-stamping

No stipulation.

7 CERTIFICATE, CRL, AND OCSP PROFILES

7.1 Certificate profile

End-entity certificates will be X509v3, 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 the CA certificate:

- keyUsage (critical): Digital Signature, Certificate Sign, CRL Sign
- basicConstraints (critical): CA:true
- X509v3 Subject Key Identifier
- X509v3 Authority Key Identifier
- CRLDistributionPoints: URI:`http://ca.ncsa.uiuc.edu/9b95bbf2.r0`

For user and service certificates:

- Basic Constraints (critical): CA:false
- X509v3 Subject Key Identifier
- X509v3 Authority Key Identifier
- X509v3 Certificate Policies: OID: 1.3.6.1.4.1.4670.100.1.1
- Key Usage (critical): Digital Signature, Non Repudiation, Key Encipherment, Data Encipherment
- CRLDistributionPoints: URI:`http://ca.ncsa.uiuc.edu/9b95bbf2.r0`
- SubjectAltName:

  For user certificates, the NCSA email address of the subscriber responsible for the certificate.

  For service certificates, the dnsName of the service and the NCSA email address of the responsible system administer.

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

All certificates will have one of the following name forms:

- C=US, O=National Center for Supercomputing Applications, OU=Services, CN=**svcname/FQDN**
- C=US, O=National Center for Supercomputing Applications, OU=Services, CN=**FQDN**
- C=US, O=National Center for Supercomputing Applications, OU=People, CN=**user name**
- C=US, O=National Center for Supercomputing Applications, OU=Certificate Authorities, CN=**CA name**

Where:

- **svcname** is “host” or an identifier of the service the certificate is associated with.
- **FQDN** is the fully qualified domain name of the host on which the service the certificate is associated with is homed.
- **user name** is a unique name for the subscriber, which may have appended digits to disambiguate.
- **ca name** is the name of a CA.

7.1.5 Name constraints

All certificates issued by the NCSA PKI will have names with the following prefix:

"C=US, O=National Center for Supercomputing Applications"

7.1.6 Certificate policy object identifier

1.3.6.1.4.1.4670.100.1.1

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

7.2.1 Version number(s)

The version number will be 1 indicating a version 2 CRL.

7.2.2 CRL and CRL entry extensions

No stipulation.

7.3 OCSP profile

OCSP is not supported.

8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS

NCSA-CA will accept being audited by other IGTF accredited CAs to verify compliance with the rules and procedures specified in this document.

9 OTHER BUSINESS AND LEGAL MATTERS

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

9.1 Confidentiality of business information

Information and data maintained in electronic media on University of Illinois computer systems are protected by the same laws and policies, and are subject to the same limitations, as information and communications in other media. Before storing or sending confidential or personal information, NCSA-CA users should understand that most materials on University systems are, by definition, public records. As such, they are subject to laws and policies that may compel the University to disclose them. The privacy of materials kept in electronic data storage and electronic mail is neither a right nor is it guaranteed.

9.2 Intellectual property rights

The NCSA-CA asserts no ownership rights in certificates issued to subscribers.

Acknowledgment is hereby given to the Fermilab PKI, the DOE Science Grid and to the CERN Certification Authority for inspiration of parts of this document.

9.3 Representations and warranties

The NCSA-CA and its agents make no guarantee about the security or suitability of a service that is identified by a NCSA certificate. The NCSA-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.

9.4 Disclaimers of warranties

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

9.5 Limitations of liability

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

9.6 Indemnities

No stipulation.

9.7 Term and termination

9.7.1 Term

This policy becomes effective on its posting to `http://security.ncsa.uiuc.edu/CA/`.

9.7.2 Termination

This policy may be terminated at any time without warning.

9.7.3 Effect of termination and survival

No stipulation.

9.8 Individual notices and communications with participants

No stipulation.

9.9 Amendments

9.9.1 Procedure for amendment

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

Changes will go into effect on the publishing of this document to NCSA-CA.

9.9.2 Notification mechanism and period

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

9.9.3 Circumstances under which OID must be changed

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

9.10 Dispute resolution provisions

NCSA Security Operations will resolve all disputes regarding this policy.

9.11 Governing law

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

9.12 Compliance with applicable law

No stipulation.

9.13 Miscellaneous provisions

No stipulation.

9.14 Other provisions

No stipulation.

10 DOCUMENT SOURCE

This source for this document can be found in the CVSROOT of :pserver:anonymous@cvs.ncsa.uiuc.edu:/CVS/ncsa-ca in the ncsa-cp repository.

The CVS version of the source for this document is $Revision$: 1.18. Changes in the version of this source could be due to minor editorial changes and do not by themselves imply a change of policy.

This document was generated from source on Wed Apr 4 09:17:51 CDT 2007 using GNU m4 1.4.2 .