Certificate Policy and Practice Statement for the NCSA Two Factor CA

National Center for Supercomputing Applications (NCSA)

Version 1.8 (Tue Feb 28 08:05:59 CST 2012)

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 resources of the National Center for Supercomputing Applications at the University of Illinois (herein referred to as "NCSA") 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 four CAs. Each CA has its own private key and certificate. It is expected that relying parties will generally trust all NCSA CAs, though a relying party may choose to trust any NCSA CA separately. These 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 11 days or shorter lifetime) to users based on Kerberos authentication and is henceforth referred to as the "NCSA Short-lived Certificate Service" or "NCSA-SLCS". One CA issues only short-lived certificates (with 11 days or shorter lifetime) to users based on federated web authentication and is henceforth referred to as the "NCSA GridShib CA" or "NCSA-GSCA". One CA issues only short-lived certificates (with 11 days or shorter lifetime) to users based on (strong) two-factor authentication and is henceforth referred to as the "NCSA Two Factor CA" or "NCSA-2FCA". One CA is a traditional CA that issues long-lived certificates to hosts, services, robots, 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, NCSA-GSCA, and NCSA-2FCA CAs for user certificates unless they have some need for a long-lived certificate from the NCSA-CA.

This document covers the policy that applies to the NCSA-2FCA. Figure 1 illustrates the overall architecture of the NCSA-2FCA. The CA is integrated with the NCSA user database and NCSA one-time password (RSA SecurID) authentication service for identity management. The NCSA accounting process enrolls users in the user database, creates a one-time password account for them, and assigns them a distinguished name.

To obtain credentials, NCSA-2FCA 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-2FCA via one-time password, issues a signed certificate request to the CA, and, if the request is approved, receives a signed certificate from the CA.

The NCSA-2FCA looks up the distinguished name in the user database that corresponds to the user's authenticated NCSA identity and issues a certificate with the appropriate distinguished name.

1.2 Document name and identification

Document title: Certificate Policy and Practice Statement for the NCSA Two Factor CA
This Policy is published at: `http://security.ncsa.illinois.edu/CA/`
Document version: 1.8
Document date: Tue Feb 28 08:05:59 CST 2012
OID: 1.3.6.1.4.1.4670.100.4.8

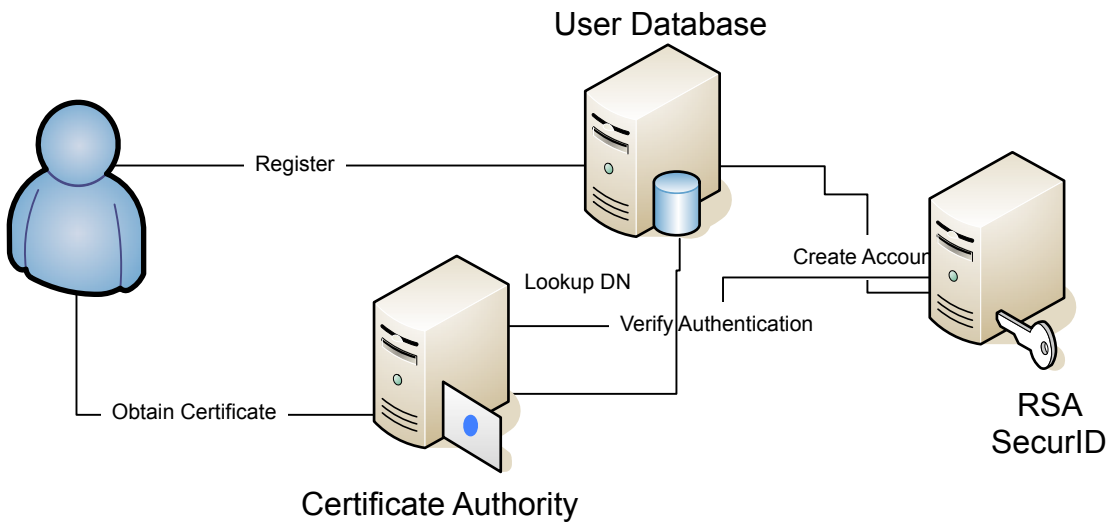

Figure 1: NCSA 2FCA CA Architecture

1.3 PKI participants

1.3.1 Certification authorities

This policy is valid for the NCSA-2FCA. The NCSA-2FCA 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-2FCA. They enroll users in the NCSA user database according to the enrollment process described in Section 4.1.2, create accounts for new users, and assign distinguished names to new users according to Section 3.1.

The NCSA-2FCA uses the NCSA one-time password (RSA SecurID) service to authenticate requests and queries the database to obtain the proper distinguished name for authenticated requesters. The NCSA user database and RSA SecureID service are used to authenticate NCSA users and staff to NCSA high-performance computing resources.

1.3.3 Subscribers

The NCSA-2FCA will serve the needs of the NCSA community by providing NCSA users and employees 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.

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, and SSL/TLS encryption for applications capable of making use of these technologies.

1.4.2 Prohibited certificate uses

Other uses of NCSA-2FCA 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-2FCA 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.illinois.edu
After hours contact information:
NCSA Security Operations and Incident Response: security@ncsa.illinois.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.illinois.edu/CA/`.

2.2 Publication of certification information

This repository will contain:

- Self-signed, certificates for all CAs in the NCSA PKI
- CRLs for the NCSA-2FCA
- General information about the NCSA PKI, including postal address and contact email address
- The most recent copies of all Certificate Policies for the NCSA PKI CAs, including this policy

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 two weeks in the future, to indicate a two week validity period for the CRL.

The Policy shall be published immediately following any update.

2.4 Access controls on repositories

Access to the repository for modification is restricted to NCSA operations staff, NCSA security operations staff, and NCSA system administration staff. See Section 5.2 for procedural controls regarding NCSA-2FCA systems.

Read access to the repository (via HTTP) is unrestricted. Repositories are publicly available for read access. 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.

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-2FCA is C=US, O=National Center for Supercomputing Applications, OU=Certificate Authorities, CN=Two Factor CA.

- CN=*User Name* : for a user's certificate issued by the NCSA-2FCA. The CN component will contain 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, 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 PKI 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.

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 by the private key associated with the public key in the request using a process that is run by the user on the client side of the request.

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 Section 4.1.2.

3.2.3 Authentication of individual identity

User identity will be authenticated via one-time password, with the authenticated NCSA login name mapped to a unique "common name" via the NCSA user database.

If traceability to a user is lost, i.e., NCSA is unable to contact a user based on the data associated with that user in the NCSA user database, then the user's NCSA login will be disabled to prevent further attempts to obtain certificates issued by the NCSA-2FCA. This also prevents authentication by the user to other NCSA services.

3.2.4 Non-verified subscriber information

No stipulation.

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

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 authentication token, that token will be revoked/re-issued according to Section 4.1.2.

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.

Others may request revocation if they can sufficiently prove compromise or exposure of the associated private key.

NCSA Security Operations will verify the authenticity of revocation requests by checking digital signatures on the request or by telephone to the requester's registered phone number.

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 and has an active NCSA-issued RSA SecurID may request a certificate.

4.1.2 Enrollment process and responsibilities

NCSA allocations group staff serve as registration authorities for the NCSA-2FCA. They enroll users in the NCSA user database according to the following enrollment process. Additional details are available at `http://www.ncsa.illinois.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.

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 a web form to request accounts for their project members. PIs can also use this form to remove project members. Access to this form requires authentication via NCSA one-time password. PIs validate 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. All users are required to sign an acceptable use policy, which educates users about secure and appropriate computing practices.

When a user no longer has any active projects, the user's NCSA RSA SecurID is disabled. The user's NCSA RSA SecurID may also be disabled for inactivity. User database entries are kept indefinitely for historical purposes.

When NCSA RSA SecurID tokens are requested, the user establishes 3 personal questions with NCSA and their corresponding answers. Then the token is either mailed to a verified address or issued in person (government issued ID required). After this, the user must activate the new token through a web form which will ask for the answers to these 3 questions that were established earlier.

A user who needs to reset a token (or activate an additional soft token) will also utilize the answers to these 3 questions. If they call the NCSA Help Desk to get a token reset, the help desk person will verify their identity by asking for the answers to those questions before proceeding. The web form to activate a new soft token associated with the same user account will also ask these same questions.

Each user is assigned a unique username used as their Unix login name as described in 3.1.5.

4.2 Certificate application processing

4.2.1 Performing identification and authentication functions

The NCSA-2FCA authenticates all certificate requests as described in Section 3.2.3. Communications between the subscriber, the CA, and the user database are encrypted and integrity protected using the TLS protocol to protect the chain of trust during application processing. The chain of trust is protected within the CA service by the secured process of translation from an authenticated certificate signing request to delivery of a signed certificate.

4.2.2 Approval or rejection of certificate applications

Certificate applications will be approved if the applicant can be authenticated via NCSA-issued RSA SecurID.

4.2.3 Time to process certificate applications

Certificate applications are processed automatically. Approved applications result in automatic certificate issuance. Non-approved applications are automatically rejected and logged.

4.3 Certificate issuance

4.3.1 CA actions during certificate issuance

Certificate applications are processed automatically. Approved applications result in automatic certificate issuance. Non-approved applications are automatically rejected and logged.

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.

- 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.

Subscribers are notified of these responsibilities in both CA documentation and an Acceptable Usage Policy (AUP). Subscribers are required to sign the AUP and return it to NCSA Allocations, thereby acknowledging reading of the AUP and agreeing to abide by its requirements.

4.5.2 Relying party public key and certificate usage

Relying parties should:

- 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 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 entities

Not applicable.

4.7 Certificate re-key

Certificates in the NCSA PKI are not 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 certification of a new public 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 a 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 entities

Not applicable.

4.8 Certificate modification

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

4.8.1 Circumstance for certificate modification

Not applicable.

4.8.2 Who may request certificate 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 entities

Not applicable.

4.9 Certificate revocation and suspension

4.9.1 Circumstances for revocation

Certificates issued by the NCSA-2FCA 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-2FCA.

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.illinois.edu or by phone to NCSA Operations 217-244-0710. Requests will be authenticated according to Section 3.4.

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 within one working day of the request being received.

4.9.6 Revocation checking requirement for relying parties

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

4.9.7 CRL issuance frequency (if applicable)

CRLs are issued daily and whenever a certificate is revoked.

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 On-line revocation checking requirements

None.

4.9.11 Other forms of revocation advertisements available

None.

4.9.12 Special requirements re key compromise

None.

4.9.13 Circumstances for suspension

Certificate suspension is not supported.

4.9.14 Who can request suspension

Not applicable.

4.9.15 Procedure for suspension request

Not applicable.

4.9.16 Limits on suspension period

Not applicable.

4.10 Certificate status services

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

4.10.1 Operational characteristics

No stipulation.

4.10.2 Service availability

No stipulation.

4.10.3 Optional features

No stipulation.

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.

4.12.1 Key escrow and recovery policy and practices

Not applicable.

4.12.2 Session key encapsulation and recovery policy and practices

Not applicable.

5 FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

5.1 Physical controls

5.1.1 Site location and construction

The NCSA-2FCA servers are located in NCSA's machine room in the National Petascale Computing Facility (NPCF) on the University of Illinois at Urbana-Champaign campus at 1725 South Oak Street in Champaign, Illinois.

5.1.2 Physical access

NCSA occupies all of NPCF. NPCF entrances and computer rooms are locked at all times and use and utilize a two factor HID keycard system to gain entry. The building entrances use iris scanners or randomized keypads as the second factor and the data center uses iris scanners exclusively as the second factor. The physical access control system for the data center uses anti-passback features to reduce the likelihood of tailgating. Video cameras are located at all entrances, in all the halls and public areas, the data center and command center. They are monitored by staff in the control room, and video is saved for a minimum of 1 month. NPCF is not open to the general public and is staffed at all times.

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 (see section 5.4) are archived weekly to a secondary storage facility in the NCSA Building on the University of Illinois at Urbana-Champaign campus at 1205 West Clark Street in Urbana, Illinois. The NCSA Building is approximately 3 miles away from NPCF, where the CA is located.

5.2 Procedural controls

All persons with access to the systems hosting the NCSA-2FCA 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-2FCA 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.

5.2.1 Trusted roles

No stipulation.

5.2.2 Number of persons required per task

No stipulation.

5.2.3 Identification and authentication for each role

No stipulation.

5.2.4 Roles requiring separation of duties

No stipulation.

5.3 Personnel controls

Operators of the NCSA-2FCA will be qualified system administrators and operators at NCSA.

5.3.1 Qualifications, experience, and clearance requirements

No stipulation.

5.3.2 Background check procedures

No stipulation.

5.3.3 Training requirements

No stipulation.

5.3.4 Retraining frequency and requirements

No stipulation.

5.3.5 Job rotation frequency and sequence

No stipulation.

5.3.6 Sanctions for unauthorized actions

No stipulation.

5.3.7 Independent contractor requirements

No stipulation.

5.3.8 Documentation supplied to personnel

No stipulation.

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

See Section 5.1.8.

5.4.3 Retention period for audit log

Audit logs are maintain for at least three years.

5.4.4 Protection of audit log

Events are recorded in real-time via syslog to the local system and to NCSA's central syslog collector service, which provides an independent, protected log collection point that is physically and logically separated from CA systems. Access to the syslog collector service is restricted to NCSA security operations staff.

5.4.5 Audit log backup procedures

See Section 5.1.8.

5.4.6 Audit collection system (internal vs. external)

Audit logs are stored on the local system, on NCSA's central syslog collector service, and in off-site backups (see Section 5.1.8). In all cases the logs are maintained on NCSA systems, in NCSA buildings, under control of NCSA staff.

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 made available to external auditors in the course of their work as auditor.

5.5.1 Types of records archived

No stipulation.

5.5.2 Retention period for archive

No stipulation.

5.5.3 Protection of archive

No stipulation.

5.5.4 Archive backup procedures

No stipulation.

5.5.5 Requirements for time-stamping of records

No stipulation.

5.5.6 Archive collection system (internal or external)

No stipulation.

5.5.7 Procedures to obtain and verify archive information

No stipulation.

5.6 Key changeover

Best effort will be made to notify relying parties of any new public key for the NCSA-2FCA, and it may then be obtained in the same manner as the previous NCSA-2FCA 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-2FCA 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.

6.1.2 Private key delivery to subscriber

Not necessary.

6.1.3 Public key delivery to certificate issuer

Public keys are delivered under TLS 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.illinois.edu/CA/`
- `http://security.teragrid.org/TG-CAs.html`
- `http://vdt.cs.wisc.edu/certificate_authorities.html`
- `https://dist.eugridpma.info/distribution/igtf/`
- `https://www.tacar.org/repos/`

6.1.5 Key sizes

The CA private key will be 2048 bits in length. Public RSA keys shorter than 2048 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-2FCA does not enforce key usage restrictions by any means beyond the X.509v3 extensions in the certificates it issues. The certificate extensions are specified in Section 7.1.2.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic module standards and controls

The NCSA-2FCA uses a FIPS 140-2 level 3 Hardware Security Module (SafeNet Luna PCI) for storage of its private key, operated in FIPS 140-2 level 2 mode.

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

No stipulation.

6.2.3 Private key escrow

NCSA-2FCA private keys are not escrowed.

6.2.4 Private key backup

NCSA-2FCA private key is replicated on two identical cryptographic modules on two identical hosts in the NCSA machine room to provide for failure protection. The replication procedure involves transferring the private key from one cryptographic module to the other in an encrypted file. The private key is never exported in plain text form. 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-2FCA private keys are not archived.

6.2.6 Private key transfer into or from a cryptographic module

NCSA-2FCA 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. The private key is never exported in plain text form.

6.2.7 Private key storage on cryptographic module

NCSA-2FCA private keys are stored on cryptographic modules meeting FIPS 140-2 level 3, operated in FIPS 140-2 level 2 mode.

6.2.8 Method of activating private key

The private key is activated automatically at server startup to allow immediate NCSA-2FCA 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-2FCA will have a lifetime of up to 20 years.

NCSA-2FCA certificates will have a lifetime of not more than 11 days.

6.4 Activation data

The NCSA-2FCA private key is activated automatically at boot time.

6.4.1 Activation data generation and installation

Activation data is generated using the operator interface of the SafeNet Luna PCI module and stored on the local CA server filesystem.

6.4.2 Activation data protection

Activation data is readable only by the root account on the local CA server filesystem.

6.4.3 Other aspects of activation data

No stipulation.

6.5 Computer security controls

The NCSA-2FCA 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 (OTP) authentication using hardware tokens and permitted only for administrative personnel that require access to the system for its operation.

The one-time password and NCSA user database servers likewise run on dedicated machines, running no other services than those needed for one-time password NCSA user database operations, located in NCSA's machine room in the National Petascale Computing Facility on the University of Illinois campus. The servers are monitored via both host-based and network-based intrusion detection systems, and login access is subject to hardware-based one-time password (OTP) authentication.

6.5.1 Specific computer security technical requirements

No stipulation.

6.5.2 Computer security rating

No stipulation.

6.6 Life cycle technical controls

No stipulation.

6.6.1 System development controls

No stipulation.

6.6.2 Security management controls

No stipulation.

6.6.3 Life cycle security 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 5280.

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): Certificate Sign, CRL Sign
- basicConstraints (critical): CA:true
- X509v3 Subject Key Identifier
- X509v3 Authority Key Identifier

For user certificates:

- Basic Constraints (critical): CA:false
- X509v3 Subject Key Identifier
- X509v3 Authority Key Identifier
- X509v3 Certificate Policies:
  - Policy: 1.3.6.1.4.1.4670.100.4.8 (this document)
  - Policy: 1.2.840.113612.5.2.2.3 (Short-Lived Credential Services)
  - Policy: 1.2.840.113612.5.2.3.2.1 (Identity Vetting by a Trusted Third Party)
  - Policy: 1.2.840.113612.5.2.3.1.2 (Private Key Protection: Key material held in files)
- Key Usage (critical): Digital Signature, Key Encipherment, Data Encipherment
- CRLDistributionPoints: URI:`http://ca.ncsa.illinois.edu/679cff61.crl`

7.1.3 Algorithm object identifiers

- Hash Functions: sha1 1.3.14.3.2.26, sha256 2.16.840.1.101.3.4.2.1, sha384 2.16.840.1.101.3.4.2.2, sha512 2.16.840.1.101.3.4.2.3
- RSA Encryption: rsaEncryption 1.2.840.113549.1.1.1
- Signature Algorithms: sha1WithRSAEncryption 1.2.840.113549.1.1.5, sha256WithRSAEncryption 1.2.840.113549.1.1.11, sha384WithRSAEncryption 1.2.840.113549.1.1.12, sha512WithRSAEncryption 1.2.840.113549.1.1.13

7.1.4 Name forms

All certificates will have the following name form:

C=US, O=National Center for Supercomputing Applications, CN=**user name**

Where:

user name is a unique name for the subscriber, which may have appended digits to disambiguate.

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

1.3.6.1.4.1.4670.100.4.8

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.

7.3.1 Version number(s)

Not applicable.

7.3.2 OCSP extensions

Not applicable.

8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS

NCSA-2FCA will accept being audited by other IGTF accredited CAs to verify compliance with the rules and procedures specified in this document. NCSA-2FCA audit records will be made available to external auditors in the course of their work as auditor.

8.1 Frequency or circumstances of assessment

No stipulation.

8.2 Identity/qualifications of assessor

No stipulation.

8.3 Assessor's relationship to assessed entity

No stipulation.

8.4 Topics covered by assessment

No stipulation.

8.5 Actions taken as a result of deficiency

No stipulation.

8.6 Communication of results

Audit results will be made available to the TAGPMA upon request.

9 OTHER BUSINESS AND LEGAL MATTERS

9.1 Fees

No fees will be charged by the NCSA-2FCA nor any refunds given.

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

No financial responsibility is accepted.

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

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-2FCA 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.

9.3.1 Scope of confidential information

No stipulation.

9.3.2 Information not within the scope of confidential information

No stipulation.

9.3.3 Responsibility to protect confidential information

No stipulation.

9.4 Privacy of personal information

The privacy of personal information collected by the NCSA-2FCA is neither a right nor is it guaranteed. See Section 9.3.

9.4.1 Privacy plan

The NCSA-2FCA does not have a specific privacy plan other than implementing the privacy polices applied to all University of Illinois computer systems.

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 NCSA-2FCA 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.

9.6 Representations and warranties

The NCSA-2FCA and its agents make no guarantee about the security or suitability of a service that is identified by a NCSA certificate. The NCSA-2FCA 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.

9.6.1 CA representations and warranties

No stipulation.

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 NCSA-2FCA denies any financial or any other kind of responsibility for damages or impairments resulting from its operation.

9.8 Limitations of liability

The NCSA-2FCA is operated substantially in accordance with NCSA'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 posting to `http://security.ncsa.illinois.edu/CA/`.

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.

Changes will go into effect on the publishing of this document to `http://security.ncsa.illinois.edu/CA/`.

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

NCSA Security Operations 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 Illinois, where the conforming CA is established.

9.15 Compliance with applicable law

No stipulation.

9.16 Miscellaneous provisions

No stipulation.

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 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. It is online at:
`http://cvs.ncsa.uiuc.edu/viewcvs.cgi/ncsa-cp/?cvsroot=ncsa-ca`.

The CVS version of the source for this document is $Revision : 1.48$. 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 Tue Feb 28 08:05:59 CST 2012 .

11 REVISION HISTORY

This section captures the revision history for the Certificate Policy and Practice Statements of the NCSA PKI. The Certificate Policy and Practice Statements of the CAs in the NCSA PKI share a common source and are versioned in a coordinated fashion, given that changes to policy often affect all the CAs. Not all revisions listed below may pertain to this policy.

1.8 The changes in this version are:

- Introduced the NCSA-2FCA.
- In Section 5.1.1, changed location from the Advanced Computation Building (ACB) to the National Petascale Computing Facility (NPCF).
- Replaced instances of "no stipulation" with "not applicable" where appropriate.

1.7 Added support for Robot certificates in the NCSA-CA according to the "Guideline on IGTF Approved Robots".

1.6 Added SHA-256, SHA-384, and SHA-512 in Section 7.1.3 (algorithm object identifiers) to enable move to SHA-2 hash functions per the NIST Policy on Hash Functions.

1.5 The changes in this version are:

- Updated Section 4.1.2 to allow the new capability in the TeraGrid User Portal for new users to choose their initial passwords during initial registration, rather that distributing initial passwords via postal mail.
- Updated Section 6.3.2 to increase the maximum lifetime of certificates issued by the NCSA-CA to 1 year and 1 month and by the NCSA-SLCS and NCSA-GSCA to 11 days.
- Updated addresses from uiuc.edu to illinois.edu as appropriate. Note that old uiuc.edu addresses will automatically redirect to their new illinois.edu versions. Note also that some services, such as CRL distribution, still use uiuc.edu addresses.

1.4 Introduced the GridShib CA (NCSA-GSCA). Updated off-site backup location (moved from the Beckman Institute to the new NCSA Building). Added IGTF policy OIDs. Replaced RFC 3280 reference with RFC 5280. Updated to strictly conform to RFC 3647 outline. GridShib CA approved by TAGPMA May 2009.

1.3 The SLCS CA now issues CRLs.

1.2 Updated password reset process in Section 4.1.2 to include password resets via the TeraGrid User Portal for the SLCS CA. Approved by TAGPMA April 2008. Began issuing certificates May 2008.

1.1 NCSA-CA and NCSA-SLCS approved by TAGPMA April 2007 and began issuing certificates May 2007.

- Documented allocations process with PIs acting as RAs.

- MICS CA updated to issue user certificates with OU=People.
- MICS CA issues version 2 CRLs.

1.0 Presented at TAGPMA Face-to-Face Meeting in Mexico City (March 2007).