

National Computational Science Alliance
Certificate Policy

Version 0.9.1

June 30, 1999

National Computational Science Alliance CERTIFICATE POLICY

1. *INTRODUCTION*
2. *GENERAL PROVISIONS*
3. *IDENTIFICATION AND AUTHENTICATION*
4. *OPERATIONAL REQUIREMENTS*
5. *PHYSICAL, PROCEDURAL, AND PERSONNEL SECURITY CONTROLS*
6. *TECHNICAL SECURITY CONTROLS*
7. *CERTIFICATE AND CRL PROFILES*
8. *POLICY ADMINISTRATION*
9. *DEFINITIONS*

1. INTRODUCTION.

1.1. Overview.

This Certificate Policy (herein referred to as the "Policy") specifies minimum requirements for the issuance and management of certificates that shall be used in authenticating users accessing National Computational Science Alliance (herein referred to as the "Alliance") resources specified in Section 1.3.5 of this Policy. The Policy is issued and administered under the authority of the Alliance Policy Management Authority (herein referred to as the "PMA"; see Section 1.3.7 for contact details).

1.2. Policy Identification.

This Policy is published on

<http://www.ncsa.uiuc.edu/alliance/partners/PACS/AllianceCP.html>

1.3. Community & Applicability.

1.3.1. Certification Authorities (CA).

This Policy is binding on each authorized Certificate Authority (CA) that issues certificates identifying this Policy as its authority, and governs its performance with respect to all certificates it issues that reference this Policy.

A CA may issue certificates that reference this Policy (as identified by the OID in section 1.2) only if such CA first qualifies as an Authorized CA by

- agreeing to be bound by, and comply with this Policy,
- undergoing and successfully completing the compliance audit specified in Section 2.7, and
- being approved by the PMA.

Specific practices and procedures by which the CA implements the requirements of this Policy, shall be set forth by the CA in a Certificate Practice Statement (CPS).

1.3.2. Registration Authorities.

The CA may delegate or subcontract performance of identification and authentication functions to a Registration Authority ("RA"), provided that the CA remains responsible for the performance of those services by such third parties in a manner consistent with the requirements of this Policy. The RA will be identified and the relationship between the CA and the RA will be described in the CA's CPS.

1.3.3. Repository Services Provider.

The CA may delegate or subcontract performance of certificate repository functions to a Repository Services Provider ("RSP"), provided that the CA remains responsible for performance of those services by such third party in a manner consistent with the requirements of this Policy. The RSP will be identified and the relationship between the CA and the RSP will be described in the CA's CPS.

1.3.4. Subscribers.

National Computational Science Alliance CERTIFICATE POLICY

A CA will issue certificates that reference this Policy to individuals ("subscribers") who have been authorized access to Partnership for Advance Computational Services (PACS) Advance Computational Resources and Services (ACRS) sites.

1.3.5. Resources.

A CA will issue certificates that reference this Policy to authorized systems administrators of Alliance resources at Advance Computational Resources and Services (ACRS) sites.

1.3.6. Qualified Relying Parties.

This Policy is intended for the benefit of the Alliance PACS/ACRS, and other Alliance entities that may accept and rely on certificates that reference this Policy, issued by an authorized CA.

1.3.7. Certificate Authorized Uses.

Certificates issued that reference this Policy are for the purpose of authenticating access to PACS/ACRS resources and other Alliance entities for which allocations have been approved. The certificate may be used to sign Alliance digital documents that have been pre-approved by the Alliance PMA. Digital signatures are not supported for sensitive transactions such as, financial transfers or legal forms as they are not legally binding.

1.3.8. Contact Details

This Policy is administered by the National Computational Science Alliance PMA:

Attn: Randy Butler

Phone number: (217) 244-8285

E-mail address: rbutler@ncsa.uiuc.edu

2. GENERAL PROVISIONS.

2.1. Obligations.

2.1.1. Certificate Authority Obligations.

Certificate Authorities (Section 1.3.1.) are responsible for all aspects of the issuance and management of a certificate referencing this Policy, including

- development of a detailed statement of practices and procedures (the CPS) by which the CA implements the requirements of this Policy,
- publish contact information,
- the certificate application/enrollment process,
- the verification of the identity of the applicant,
- the actual certificate creation process,
- the posting of the certificate in a public repository,
- the suspension and revocation of the certificate,
- the renewal of the certificate,

National Computational Science Alliance CERTIFICATE POLICY

- ensure that all aspects of the CA services and CA operations and CA infrastructure related to certificates issued under this Policy are performed in accordance with the requirements, representations, and warranties of this Policy,
- define and publish a dispute resolution procedure,
- record all disputes must for PMA review.

By issuing a certificate that references this Policy, the CA certifies to the subscriber, and to all Qualified Relying Parties who reasonably and in good faith rely on the information contained in the certificate during its operational period, that:

- the CA has issued, and will manage, the certificate in accordance with this Policy,
- there are no misrepresentations of fact in the certificate known to the CA, and the CA has taken reasonable steps to verify additional information in the certificate unless otherwise noted in its CPS, and
- the certificate meets all material requirements of this Policy and the CA's CPS.

2.1.2. Registration Authority Obligations.

Obligations of the RA (Section 1.3.2) will be determined by the CA, and will be outlined specifically in the CA's CPS.

2.1.3. Repository Service Provider Obligations.

Obligations of the RSP (Section 1.3.3) will be determined by the CA, and will be outlined specifically in the CA's CPS.

2.1.4. Subscriber Obligations.

In all cases, subscribers (Section 1.3.4) will be required to:

- generate a key pair using a trustworthy method,
- review and verify accuracy of their representations included in the published certificate,
- use the certificate exclusively for authorized and legal purposes, consistent with this Policy,
- instruct the CA to revoke the certificate promptly upon any actual or suspected loss, disclosure, or other compromise of the subscribers private key, and
- take reasonable precautions to prevent any loss, disclosure, or unauthorized use of the private key associated with the certificate, including:
 - selecting a pass phrase that is a minimum 16 characters,
 - using upper and lower characters or special characters in the pass phrase, and
 - protecting the pass phrase (private key) from others.

2.1.5. Resource Administrator Obligations.

In all cases, the resource administrator (Section 1.3.5) will be required to:

- generate a key pair using a trustworthy method,
- review and verify accuracy of their representations included in the published certificate,
- use the certificate exclusively for authorized and legal purposes, consistent with this Policy,
- instruct the CA to revoke the certificate promptly upon any actual or suspected loss, disclosure, or other compromise of the resource's private key, and

National Computational Science Alliance CERTIFICATE POLICY

- take reasonable precautions to prevent any loss, disclosure, or unauthorized use of the private key associated with the certificate.

2.1.6. Qualified Relying Party Obligations.

Qualified Relying Parties (Section 1.3.6) are expected to rely on certificates that reference this Policy as appropriate authentication of the subscriber if:

- the reliance is reasonable and in good faith in light of all the circumstances known to the relying party at the time of reliance,
- the purpose for which the certificate was used was appropriate under this Policy,
- the relying party checked the status of the certificate prior to reliance, or a check of the certificate's status would have indicated that the certificate was valid, and
- the reliance is for lawful purposes.

2.2. Liability.

The PMA and the CA assumes no liability for any direct or indirect damages suffered by relying parties caused by the failure of the CA to comply with either its Policy or CPS or resulting from the reliance of a relying party on a certificate issued by the CA.

However, the PMA retains the right to withdraw authority for a CA to issue certificates that reference this Policy if the CA fails to comply with the provisions of this Policy or its CPS, or if the CA is found negligent in the performance of its function.

2.3. Dispute Resolution Procedures.

CA must define a dispute resolution procedure within the CPS and publish it in a publicly accessible place. Further the CA should attempt to resolve disputes, and those they can't resolve will be handled by the PMA. All disputes must be recorded for PMA review and available for audit.

2.4. Fees.

CA shall not impose any usage fees on subscribers and relying parties for

- the reading of this Policy or the CA's CPS
- issuing certificates referencing this Policy,
- possessing certificates referencing this Policy,
- status information of certificates issued referencing this Policy, or
- revocation processes or lists related to certificates referencing this Policy.

2.5. Publication & Repositories.

2.5.1. Publication of CA Information in the Repository.

Each Authorized CA shall operate a secure on-line repository that is available to Qualified Relying Parties and that contains

- certificates issued that reference this Policy,
- a Certificate Revocation List (CRL) or on-line certificate status database for certificates issued reference this Policy,

National Computational Science Alliance CERTIFICATE POLICY

- the CA's certificate for its signing key,
- past and current versions of the CA's CPS,
- a copy of this Policy, and
- other relevant information relating to certificates that reference this Policy.

2.5.2. Frequency of Publication.

All information to be published in the repository shall be published within 24 hours after such information is available to the CA.

Certificates issued by the CA that reference this Policy will be published within 24 hours. Information relating to the revocation of a certificate will be published in accordance with the requirements outlined later in this Policy.

2.5.3. Access Controls.

The Repository will be available to Qualified Relying Parties and subscribers on a substantially 24 hours per day, 7 days per week basis, subject to reasonable scheduled maintenance and the CA's then current terms of access.

The CA shall not impose any access controls on this Policy, or the CA's certificate for its signing key.

The CA may impose access controls on certificates, certificate status information, or CRLs at its discretion, subject to agreement between the CA, relying parties, and subscribers, in accordance with provisions published in its CPS or otherwise.

2.6. Compliance Audit.

Before initial approval as an Authorized CA, and thereafter at least once every year, the CA (and subcontractors, as applicable) shall fund and submit to a compliance audit.

The auditing team will consist of at least 3 individuals assigned by the PMA, and drawn from the PACS/ACRS sites. The team will be comprised of staff representing applications, infrastructure, and policy/management activities.

The purpose of the audit is to verify the quality of the services provided by the CA, that the CA complies with all of the requirements of this Policy and its CPS, and that the CPS is consistent with the requirements of this Policy. The PMA retains the right to withdraw authority for a CA to issue certificates that reference this Policy if the audit finds that the CA fails to comply with the provisions of this Policy or its CPS.

2.7. Confidentiality Policy.

Information regarding subscribers submitted on applications for certificates referencing this Policy will be retained on file and made available to Alliance resource centers on demand.

The foregoing shall not apply to information appearing on certificates, or to information regarding subscribers obtained by the CA from public sources.

Under no circumstances shall the CA (or any other entity involved in the certificate administration process) have access to the private keys of any subscriber to whom it issues a certificate that references this Policy.

3. Identification and Authentication.

3.1. Initial Registration.

Subject to the requirements noted below, certificate applications may be communicated from the applicant to the CA or RA,

- electronically via a secure method,
- by first class U.S. mail, or
- in person.

3.1.1. Types of Names.

The subject name used for certificate applicants shall be of the X.500 name form. Registration of Alliance distinguished names is the responsibility of Alliance Allocations/Account Management. The Alliance Dn will take the following form:

/c=us/o=National Computational Science Alliance /cn=firstname lastname(tiebreaker).

3.1.2. Name Meanings.

The subject name listed in a certificate must have a reasonable association with the authenticated name of the subscriber. In the case of individuals this should be a combination of first name and/or initials and surname.

3.1.3. Name Uniqueness.

The subject name listed in a certificate will conform to X.500 standards for name uniqueness and be unambiguous and unique for all certificates issued that reference this Policy. A subscriber may present a common name that they want to use for certificates. If this name is not unique as required by this Policy, additional numbers or letters may be appended to the common name to ensure the name's uniqueness within the domain of certificates issued by the CA.

In order to guarantee name uniqueness, all requesters will have a registered distinguished name with the Alliance X.500 service.

Certificates must apply to unique individuals or resources; users may not share certificates.

3.1.4. Verification of Key Pair.

The CA shall establish that the applicant is in possession of the private key corresponding to the public key submitted with the application in accordance with an appropriate secure protocol, such as that described in the IETF PKIX Certificate Management Protocol.

3.1.5. Authentication Confirmation Procedure.

Authenticity of the individual may be confirmed in one of the following ways:

National Computational Science Alliance CERTIFICATE POLICY

- Valid picture identification such as a driver's license or Passport presented in person.
- Verification of contact information via the Alliance Account Management database.

3.2. Renewal Applications (Routine Re-key).

Within two (2) months prior to the scheduled expiration of the operational period of a certificate issued that references this Policy, and following authentication per the requirements of this Policy, a subscriber may request issuance of a new certificate, provided the original certificate has not been suspended or revoked. Such a request may be made electronically via a digitally signed message based on the old key pair in the original certificate.

3.3. Re-key After Revocation.

Revoked or expired certificates shall not be renewed. Applicants without a valid certificate, must re-apply just as would a first-time application, per the requirements of this Policy.

3.4. Revocation Request.

The CA will make a good-faith effort to authenticate the identity of the person submitting a revocation request. However, authentication efforts must consider the need to prevent unauthorized revocation requests balanced against the need to quickly revoke certificates.

4. OPERATIONAL REQUIREMENTS.

4.1. Certificate Application.

An applicant for a certificate shall complete a certificate application in a form prescribed by the CA and enter into a subscriber agreement with the CA. All applications are subject to review, approval and acceptance by CA.

An application for a resource certificate shall be submitted by the authorized Alliance resource systems administrator with a valid Alliance certificate.

4.2. Certificate Issuance.

Upon successful completion of the subscriber identification and authentication process per the requirements of this Policy, the CA will:

- issue the requested certificate,
- notify the applicant thereof, and
- publish the certificate.

4.3. Certificate Revocation.

4.3.1. Circumstances for Revocation.

4.3.1.1. Permissive Revocation.

A subscriber may request revocation of his or her certificate at any time for any reason.

The issuing CA may also revoke a certificate upon failure of the subscriber to meet its obligations under this Policy, the applicable CPS, or any other agreement, regulation, or law applicable to the certificate that may be in force.

4.3.1.2. Required Revocation.

A subscriber shall promptly request revocation of a certificate

- whenever any of the information on the certificate changes or becomes obsolete,
- whenever the private key, or the media holding the private key, associated with the certificate is or is suspected of having been compromised, or
- when the subscriber no longer needs the certificate to access a Qualified Relying Party's resources (Section 1.3.5).

The issuing CA shall revoke a certificate

- upon request of the subscriber,
- upon failure of the subscriber to meet its material obligations under this Policy, any applicable CPS, or any other agreement, regulation, or law applicable to the certificate that may be in force,
- whenever the private key, or the media holding the private key, associated with the certificate is or is suspected of having been compromised,
- if the CA determines that the certificate was not properly issued in accordance with this Policy and/or any applicable CPS, or
- in the event that the CA ceases operations. In this situation, all certificates issued by the CA shall be revoked prior to the date that the CA ceases operations.

4.3.2. Who Can Request Revocation.

The only persons permitted to request revocation of a certificate issued pursuant to this Policy are the subscriber and the issuing CA.

4.3.3. Procedure for Revocation Request.

A certificate revocation request should be promptly communicated to the issuing CA, either directly or through a RA.

A certificate revocation request may be communicated electronically if it is digitally signed with the private key of the subscriber. Alternatively the subscriber may request revocation by contacting the CA or an authorized RA in person and providing adequate proof of identification in accordance with this Policy.

Within one (1) hour following revocation, the CRL or certificate status database in the repository, as applicable, shall be updated. All revocation requests and the resulting actions taken by the CA shall be archived.

4.3.4. Revocation Request Grace Period.

The CA will act on requests for revocation within 4 hours of receipt during business working days.

4.3.5. Certificate Suspension.

No stipulation.

4.3.6. CRL Issuance Frequency.

An up-to-date CRL shall be issued at least once per day.

4.4. Computer Security Audit Procedures.

All significant security events on the CA system should be automatically recorded in audit trail files.

The audit log shall be reviewed for anomalous behavior at least once a week.

Such files shall be retained for at least six (6) months locally, and thereafter shall be securely archived for two years.

4.5. Records Archival.

4.5.1. Types of Records Archived.

The following data and files must be archived by [or on behalf of] the CA:

- All computer security audit data,
- All certificate application data,
- All certificates, and all CRLs or certificate status records generated,
- Revocation requests,
- Key histories, and
- All correspondence between the CA and subcontractors and subscribers.

4.5.2. Archive Management.

Archives of the certificate information must be retained for at least four years. Archives of the audit trail files must be retained for at least six months.

The archive media must be protected from alteration and inappropriate disclosure.

Adequate backup procedures must be in place so that in the event of the loss or destruction of the primary archives, a complete set of backup copies will be readily available in less than one day.

Three weeks of backup information must be maintained to recover from incidents that are discovered late.

4.5.3. Procedures to Obtain and Verify Archive Information.

During the compliance audit required by this Policy, the auditor shall verify the integrity of the primary archives and the backup archives.

If either of the archives are found to be corrupted or damaged in any way it shall be replaced with the other copy held at separate location.

4.6. Compromise and Disaster Recovery.

4.6.1. Disaster Recovery Plan.

The CA must have in place an appropriate disaster recovery/business resumption plan and must set up and render operational a facility that is capable of providing CA Services in accordance with this Policy within 96 hours of an unanticipated emergency.

Such plan shall include a complete and periodic test of readiness for such facility. Such plan shall be [detailed/referenced] within the CPS or other appropriate documentation available to Qualified Relying Parties.

4.6.2. Key Compromise Plan.

The CA must have in place an appropriate key compromise plan that addresses the procedures that will be followed in the event of a compromise of the private signing key used by the CA to issue certificates, or used by any higher level CA.

Such plan shall include procedures for revoking all affected certificates and promptly notifying all subscribers and all Qualified Relying Parties.

4.7. CA Termination.

In the event that the CA ceases operation, all subscribers, sponsoring organizations, RAs, RSPs, and Qualified Relying Parties will be promptly notified of the termination.

In the event that CA is involuntarily terminated the PMA will determine the proper course of action.

In addition, all CAs with which cross-certification agreements are current at the time of cessation will be promptly informed of the termination.

All certificates issued by the CA that reference this Policy will be revoked no later than the time of termination.

5. Physical, Procedural, And Personnel Security Controls.

5.1. Physical Security—Access Controls.

The CA, and all RAs and RSPs, shall implement appropriate physical security controls to restrict access to the hardware and software (including the server, workstations, and any external cryptographic hardware modules or tokens) used in connection with providing CA Services.

Access to such hardware and software shall be limited to those personnel performing in a Trusted Role as described in Section 5.2.1.

Access shall be controlled through the use of: electronic access controls, mechanical combination locksets, or deadbolts.

Such access controls must be manually or electronically monitored for unauthorized intrusion at all times.

5.2. Procedural Controls.

5.2.1. Trusted Roles.

All employees, contractors, and consultants of the CA (collectively "personnel") that have access to or control over cryptographic operations that may materially affect the CA's issuance, use, suspension, or revocation of certificates, including access to restricted operations of the CA's repository are serving in a trusted role.

Such personnel include, but are not limited to, system administration personnel, operators, engineering personnel, and executives who are designated to oversee the CA's operations.

5.2.2. Multiple Roles (Number Of Persons Required Per Task).

To ensure that one person acting alone cannot circumvent safeguards, multiple roles and individuals should share responsibilities at a CA server. Each account on the CA server shall have limited capabilities commensurate with the role of the account holder.

CAs supporting this Certificate Policy should recognize multiple distinct roles to accomplish its cryptographic operations. No one individual should perform multiple roles. Duties should be split between multiple personnel so that the approach taken provides reasonable resilience to insider attack.

5.2.3. Minimal individuals.

The minimal number of individuals required to provide reliability, availability, and multiple roles (see 5.2.2) shall be granted trusted roles.

5.3. Personnel Security Controls.

5.3.1. Background and Qualifications.

CAs and subcontractors shall formulate and follow personnel and management policies sufficient to provide reasonable assurance of the trustworthiness and competence of their employees and of the satisfactory performance of their duties in manner consistent with this Policy.

5.3.2. Background Investigation.

CAs shall conduct appropriate reference checks for all personnel who serve in trusted roles (prior to their employment), to verify their trustworthiness and competence in accordance with the requirements of this Policy and the CA's personnel practices or equivalent.

5.3.3. Training Requirements.

All CA and subcontractor personnel must receive proper training in order to perform their duties, and update briefings thereafter as necessary to remain current.

5.3.4. Documentation Supplied To Personnel.

All CA and subcontractor personnel must read or study the comprehensive user manuals detailing the procedures for certificate creation, update, renewal, suspension, and revocation, and software functionality.

5.3.5. Identify Information System Security Officer.

In order to ensure that security policies are enforced, the CA will identify an Information Security Officer (and a backup) that has overall responsibility for information security issues, activities, and incident response.

5.4. Incident Reporting.

Early notification of actual or potential problems (incidents) will be provided Alliance resource centers within 4 hours.

Further such reports will be provided in a secure (encrypted) fashion so as to limit the possibility that the incident information is exposed to a wider audience.

6. Technical Security Controls.

6.1. Key Pair Generation and Installation.

6.1.1. Key Pair Generation.

Key pairs for users (CAs, subcontractors, and subscribers) must be generated in such a way that only the authorized user of the key pair knows the private key. Acceptable ways of accomplishing this include:

- users generating their own keys on a trustworthy system, and not reveal the private keys to anyone else; or
- keys being generated by or on behalf of the users in hardware tokens from which the private key cannot be extracted.

6.1.2. Subscriber Public Key Delivery to CA.

The subscriber's public key must be transferred to the CA or RA in a way that ensures that

- it has not been changed during transit,
- the sender possesses the private key that corresponds to the transferred public key, and
- the sender of the public key is the legitimate user claimed in the certificate application.

6.1.3. CA Public Key Delivery to Users.

The public key of the CA signing key pair may be delivered to subscribers in an on-line transaction in accordance with IETF PKIX Part 3, or via another appropriate mechanism.

6.1.4. Key Sizes.

The Alliance users will use 2048 bit RSA private keys.

The Alliance CA will use a 2048 bit RSA signing key.

6.2. CA Private Key Protection.

National Computational Science Alliance CERTIFICATE POLICY

The CA and subscribers shall each protect their private key in accordance with the provisions of this Policy.

6.2.1. Private Key (N-M) Multi-Person Control.

No stipulation.

6.2.2. Private Key Escrow.

CA signing private keys shall not be escrowed.

6.2.3. Private Key Backup.

Private key backups must use a local device or protected network.

Backup media must be stored and transported in a protected manner.

6.2.4. Private Key Archival.

An entity may optionally archive its own private key.

6.2.5. Private Key Entry into Cryptographic Module

No stipulation.

6.2.6. Method of Activating Private Key.

The CA private key shall be at least pass phrase protected. See section 2.1.4.

6.2.7. Method of Destroying Private Key.

Upon expiration or revocation of a certificate, or other termination of use of a private key for creating signatures, all copies of the private key shall be securely destroyed.

6.3. Other Aspects of Key Pair Management

6.3.1. Public Key Archival.

No stipulation.

6.3.2. Key Replacement.

CA key pairs must be replaced at least every 5 years. RA, resource and subscriber key pairs must be replaced at least every 3 years and a new certificate issued.

6.3.3. Restrictions on CA's Private Key Use.

The CA's signing key used for issuing certificates that conform to this Policy shall be used only for signing certificates and CRLs.

National Computational Science Alliance CERTIFICATE POLICY

A private key used by a RA or RSP for purposes associated with its RA or RSP function shall not be used for any other purpose without the express permission of the CA.

A private key held by a CA and used for purposes of manufacturing certificates for the CA

- is considered the CA's signing key,
- is held by the CMA as a fiduciary for the CA, and
- shall not be used for any reason without the express permission of the CA.

Any other private key used by a CMA for purposes associated with its CMA function shall not be used for any other purpose without the express permission of the CA.

6.4. Activation Data.

No stipulation.

6.5. Computer Security Controls.

All CA servers must include the following functionality either provided by the operating system, or through a combination of operating system, PKI application, and physical safeguards:

- Establish configuration management controls to track hardware and software security upgrades to the CA.
- All recommended and applicable security patches must be applied to all CA servers prior to their installation on the network.
- The operating systems on the CA servers will be maintained at a high level of security by applying all applicable security patches.
- Software and hardware upgrades will be announced to the relying parties in advance.
- The CA will have a fallback strategy for all hardware and software upgrades.
- Security features of the servers will be tested after system changes to verify they are still working correctly.
- All network service daemons will have the ability to log all transactions and should have the added capability to limit access to hosts within the trusted local domain only.
- Monitoring (COPS, Tripwire, etc.) will be done on the servers to detect unauthorized software changes.
- All unnecessary daemons including nfs, sendmail, ftpd, fingerd, rstatd and rexecd will be removed from servers.
- Unencrypted X-Window traffic to and from the servers will be prohibited.
- All servers will have security audits at least annually using tools such as ISS.
- All server transactions that can be logged will be logged. Those logs will be scanned at least weekly to look for security anomalies.
- Accounts on the servers will not be shared (no group accounts).
- Root access to the servers will be restricted to the console or through securely authenticated and encrypted network sessions.
- Access to root accounts will identify who is using the privileges (aka su/ksu)
- The number of individuals with server administrative access will be limited to the minimum necessary.
- All account passwords will be changed at least every 180 days and rule-sets will enforce strong passwords.
- Administrative server accounts will be escrowed to reduce the risk of reduced access due to a lost password.

National Computational Science Alliance CERTIFICATE POLICY

- The CA server and repository must be protected through application level (proxy) firewalls (or separate ports of a single firewall) configured to allow only the protocols and commands required for the CA's services.

7. Certificate and CRL Profiles.

7.1. Certificate Profile.

Certificates that reference this Policy shall contain public keys used for authenticating the sender of an electronic message and verifying the integrity of such messages—i.e., public keys used for digital signature verification.

All certificates that reference this Policy will be issued in the [X.509 version 3] format and will include a reference to the OID for this Policy within the appropriate field. The CPS shall identify the certificate extensions supported, and the level of support for those extension.

7.2. CRL Profile.

If utilized, CRLs will be issued in the [X.509 version 2] format. The CPS shall identify the CRL extensions supported and the level of support for these extensions.

8. Policy Administration.

8.1. Policy Change Procedures.

8.1.1. List Of Items.

Periodically the PMA may consider proposed changes to this policy that could materially impact users of this Policy (other than editorial or typographical corrections, or changes to the contact details).

Proposed changes to this Policy will be provided to Authorized CAs, and will be posted on the World Wide Web site of the PMA.

8.1.2. Publication & Notification Procedures.

A copy of this Certificate Policy is available in electronic form as note in section 1.2 of this document. Authorized CAs shall post copies of this Policy in their repositories.

9. Definitions.

Audit. A review of a CA's compliance with the specific requirements of this policy.

Authorized CA. Means a certification authority that has been authorized by the Policy Administering Organization to issue certificates that reference this policy.

CA. Certification Authority

Certificate. A record that, at a minimum: (a) identifies the certification authority issuing it; (b) names or otherwise identifies its subscriber; (c) contains a public key that corresponds to a private key under the control of the subscriber; (d) identifies its operational period; and (e) contains a certificate serial number and is digitally

National Computational Science Alliance CERTIFICATE POLICY

signed by the certification authority issuing it. As used in this Policy, the term of "Certificate" refers to certificates that expressly reference this Policy in the "certificatePolicies" field of an X.509 v.3 certificate.

CMA. See Certificate Manufacturing Authority

Certificate Manufacturing Authority" (CMA). An entity that is responsible for the manufacturing and delivery of certificates signed by a certification authority, but is not responsible for identification and authentication of certificate subjects (i.e., a CMA is delegated or outsourced the task of actually manufacturing the certificate on behalf of a CA).

Certificate Revocation List (CRL). A time-stamped list of revoked certificates that has been digitally signed by a certification authority.

Certification Authority. A certification authority is an entity that is responsible for authorizing and causing the issuance of a certificate. A certification authority can perform the functions of a registration authority (RA) and a certificate manufacturing authority (CMA), or it can delegate or outsource either of these functions to separate entities.

A certification authority performs two essential functions. First, it is responsible for identifying and authenticating the intended subscriber to be name in a certificate, and verifying that such subscriber possesses the private key that corresponds to the public key that will be listed in the certificate. Second, the certification authority actually creates (or manufactures) and digitally signs the certificate. The certificate issued by the certification authority then represents that certification authority's statement as to the identity of the person named in the certificate and the binding of that person to a particular public-private key pair.

Certification Practice Statement (CPS). A "certification practice statement" is a statement of the practices that a certification authority employs in issuing, suspending, and revoking certificates and providing access to same.

CMA. See Certificate Manufacturing Authority.

CPS. See Certificate Practices Statement.

CRL. See Certificate Revocation List.

IETF. Internet Engineering Task Force. The Internet Engineering Task Force is a large open international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture and the smooth operation of the Internet.

Incident. Evidence of a likely penetration or compromise of the CA server(s) affecting more than one certificate.

Key pair. Means two mathematically related keys, having the properties that (i) one key can be used to encrypt a message that can only be decrypted using the other key, and (ii) even knowing one key, it is computationally infeasible to discover the other key.

Registration Authority. 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).

RA. See "Registration Authority."

National Computational Science Alliance CERTIFICATE POLICY

Object Identifier. An object identifier is a specially-formatted number that is registered with an internationally-recognized standards organization.

OID. See Object Identifier.

Operational Period Of A Certificate. The operational period of a certificate is the period of its validity. It would typically begin on the date the certificate is issued (or such later date as specified in the certificate), and ends on the date and time it expires as noted in the certificate or is earlier revoked or suspended.

PIN. Personal Identification Number

PKI. Public Key Infrastructure

PKIX. An IETF Working Group developing technical specifications for a PKI components based on X.509 Version 3 certificates.

Policy. Means this Certificate Policy.

Policy Administering Organization. The entity specified in Section 1.4.

Private Key. Means the key of a key pair used to create a digital signature. This key must be kept a secret.

Public Key. Means the key of a key pair used to verify a digital signature. The public key is made freely available to anyone who will receive digitally signed messages from the holder of the key pair. The public key is usually provided via a certificate issued by a certification authority and is often obtained by accessing a repository. A public key is used to verify the digital signature of a message purportedly sent by the holder of the corresponding private key.

RA. See Registration Authority.

Registration Authority. An entity that is responsible for identification and authentication of certificate subjects, but that does not sign or issue certificates (i.e., an RA is delegated certain tasks on behalf of a CA).

Relying Party. A recipient of a digitally signed message who relies on a certificate to verify the digital signature on the message.

Repository. A trustworthy system for storing and retrieving certificates and other information relating to those certificates.

Repository Services Provider (RSP). An entity that maintains a repository accessible to the public [or at least to relying parties] for purposes of obtaining copies of certificates and/or verifying the status of such certificates.

Responsible Individual. A person designated by a sponsor to authenticate individual applicants seeking certificates on the basis of their affiliation with the sponsor.

Revoke A Certificate. Means to prematurely end the operational period of a certificate from a specified time forward.

RSP. See Repository Services Provider.

Subject. A person whose public key is certified in a certificate.

National Computational Science Alliance CERTIFICATE POLICY

Also referred to as a "subscriber".

Subscriber. A subscriber is a person who (1) is the subject named or identified in a certificate issued to such person and (2) holds a private key that corresponds to a public key listed in that certificate, and (3) the person to whom digitally signed messages verified by reference to such certificate are to be attributed. See "subject."

Suspend a certificate. Means to temporarily suspend the operational period of a certificate for a specified time period or from a specified time forward.

Trustworthy System. Means computer hardware, software, and procedures that: (a) are reasonably secure from intrusion and misuse; (b) provide a reasonable level of availability, reliability, and correct operation; (c) are reasonably suited to performing their intended functions, and (d) adhere to generally accepted security procedures.

Valid Certificate. Means a certificate that (1) a certification authority has issued, (2) the subscriber listed in it has accepted, (3) has not expired, and (4) has not been revoked. Thus, a certificate is not "valid" until it is both issued by a certification authority and has been accepted by the subscriber.