National Center for High-performance Computing (NCHC)
Certificate Policy and Certification Practice Statement

Version 1.1.0

(November 22, 2005)

NCHC Policy Management Authority

Contents

1. Introduction

1.1 Overview

The National Center for High-performance Computing (NCHC) is a nonprofit organization in Taiwan. This document is the combined Certificate Policy and Certification Practice Statement of the NCHC Certification Authority. It describes the set of operation and procedures of the certification authority operated by NCHC, referred to as NCHC CA and is structured according to RFC 2527 [1]. Not all sections of RFC 2527 are used. Sections that are not included have a default value of "No stipulation". The rules and procedures in the document are approved by the NCHC Grid Policy Management Authority.

1.1.1 Type of Certificates

NCHC CA issues following types of certificates:

A. Client Certificate

B. Server Certificate:

- Host Certificate – used for Globus, Access Grid, Sensor Grid, and UNICORE.
- LDAP Server

1.1.2 Related Specification

No stipulation

1.2 Identification

This document is named *National Center for High-performance Computing (NCHC) Certificate Policy and Certification Practice Statement.* This OID is constructed as shown in the table 1 below:

Table 1 - Objects and OIDs

Object	OID
NCHC (National Center for High-performance Computing)	1.3.6.1.4.1.23308
NCHC Grid Operation Center (GOC)	1.3.6.1.4.1.23308.1
NCHC Grid Operation Center CA	1.3.6.1.4.1.23308.1.1
Certification Practices Statements (CPS)	1.3.6.1.4.1.23308.1.1.1.X *
CA Certificate Policy	1.3.6.1.4.1.23308.1.1.2
Globus Server Certificate Policy	1.3.6.1.4.1.23308.1.1.2.1.1
Access Grid / Conference Server Certificate Policy	1.3.6.1.4.1.23308.1.1.2.2.1
Sensor Net Server Certificate Policy	1.3.6.1.4.1.23308.1.1.2.3.1
Globus / Access Grid / Sensor Net Client Certificate Policy	1.3.6.1.4.1.23308.1.1.2.4.1
Unicore Server Certificate Policy	1.3.6.1.4.1.23308.1.1.2.5.1
Unicore Client Certificate Policy	1.3.6.1.4.1.23308.1.1.2.6.1
LDAP Server Certificate Policy	1.3.6.1.4.1.23308.1.1.2.7.1

* X is for each major CPS version

1.3 Community and Applicability

1.3.1 Organization

A. NCHC Policy Management Authority

The decision related to the management of NCHC CA will be performed by the NCHC Policy Management Authority (NCHC PMA), which will be responsible for:

- Draft and approve CP/CPS
- Apply countermeasures for compromise of private key of the Certificate Authority
- Apply countermeasures in emergencies
- Other important matters related to CA operations.

B. Operating Organization

Figure 1 shows the system architecture of NCHC CA

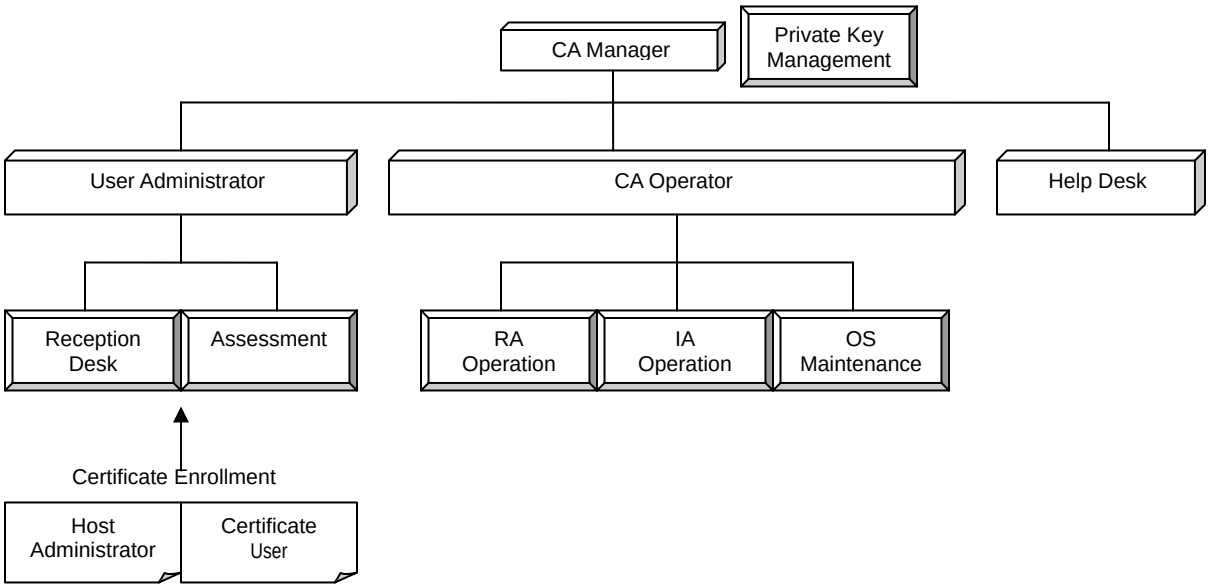

Figure 1 – The Architecture of NCHC CA

Table 2 shows the operating roles and functions.

Table 2 - Operating roles and functions

Role	Function
CA Manager	• Manage all CA tasks • Manage CA private key
CA Operator	• Manage CA and RA servers • Generate and distribute license IDs • Maintain CA system
User Administrator	• Accept user enrollment • Check users' information and approve them

Certificate User	Use a certificate issued by NCHC CA
Host Administrator	The administrator of a host using a certificate issued by NCHC CA
Help Desk	Help users related to CA operation

1.3.2 Applicability

The certificates issued by NCHC CA have to be used in the following purposes and must not be used for any other purposes.

The authorized uses of certificates issued by NCHC CA are:

A. Client Certificate: Client authentication (SSL) under the grid computing environment

B. Server Certificate:

- Globus server authentication
- Access Grid / Conference Server authentication
- Sensor Net server authentication
- Unicore server authentication
- LDAP server – Access to LDAP server

The certificates issued by NCHC CA must not be used for financial transactions.

1.3.3 End Entities

NCHC issues certificates for the following subjects:

- Users of National Center for High-performance Computing (NCHC).
- Users of National Applied Research Laboratories (NARL).
- Users or services involved in KING (Knowledge Innovation National Grid) and TWAREN (TaiWan Advanced Research and Education Network) Projects.
- Users or services, such as government organizations, academic communities, and hospitals, involved in NCHC's Grid Computing Resources
- Users of domestic Grid-based Applications / Projects.
- Foreign collaborators or institutes related to NCHC Grid research.

1.4 Contact Details

1.4.1 Specification Administration Organization

This policy is developed and maintained by Grid Operation Center (GOC), NCHC, Taiwan.

1.4.2 Contact Person

Contact point for questions related to this policy is:

Tsung-Ying Wu

Grid Operation Center (GOC), NCHC

7, R&D Rd. VI, Hsinchu Science Park, Hsinchu 300, Taiwan.

Phone: + 886-3-5776085#287

Fax: + 886-3-5776082

Email:alex@nchc.org.tw

2. General Provisions

2.1 Obligations

2.1.1 Certification Authority Obligations

The CA will:

- Create and manage the CA private key in a secure environment.
- Issue certificates based on enrollment information from the Registration Authority (RA).
- Revoke user certificates and issue a Certificate Revocation List (CRL) based on the request from RA.
- Publish the CRL and certificate-related information in the repository promptly.
- Identify which CP/CPS was used to issue certificates.
- Make sure that users realize the importance of protecting their private data.

2.1.2 Registration Authority Obligations

The RA will:

- Approve user administrators of the operating organization.
- Issue license IDs to the user administrators.
- Verify enrollment requests by license IDs and send the requests to the CA.
- Authenticate the revocation requests and send the requests to the CA.
- Distribute certificates issued by the CA securely to the users.
- Archive enrollment information safely.

2.1.3 Certificate Users and Host Administrators Obligations

The certificate users and host administrators will:

- Provide correct information at the enrollment.
- Perform enrollment and key-pair creation based on this document.
- Manage the certificate and private key safely to prevent unauthorized uses. The pass phrase for the private key must be at lease 12 characters.
- Instruct the CA to revoke the certificate promptly if there is any actual or suspected loss, disclosure, or other compromise of the private key.
- Instruct the CA to revoke the certificate promptly when it is not used at all.
- Do not share any user certificate.
- Connect the server certificate with only a single network entity.

2.1.4 Relying Party Obligations

Check the following validity of certificates:

- The certificates shall not be modified.
- Within validity dates.
- The certificate is not revoked.
- Signed by the trusted CA.

2.1.5 User Administrator Obligations

User administrator will:

- Accept enrollments from users including host administrators and approve the correct enrollment information.

2.1.6 Repository Obligations

The repository will:

- Publish information specified in section 2.6.1 and enable users to retrieve certificates and CRL information from the repository.
- Operate within specified time in section 2.6.2.
- The repository will run at least on a best-effort basis, with an intended availability of 24X7.

2.2 Liability

2.2.1 CA Liability

NCHC CA has a liability:

- Issue the certificates based on enrollment information forwarded from RA.
- Revoke the certificates based on the request forwarded from the RA.
- Register client certificate information in the repository after issue and publish it along with a CRL, except in time of temporary suspension such as system maintenance or other emergency.
- Perform practices on the procedures based on this CPS and have authenticity for certificates and CRL issuing.
- Perform appropriate practices based on this CPS to prevent compromise of private key from stealing or losing.

2.2.2 RA Liability

NCHC RA has a liability:

- Send user enrollment request to the CA correctly.
- Send user revocation request to the CA promptly.
- Perform practices on the procedures based on this CPS to prevent unauthorized access contained in the enrollment requests.

2.2.3 Certificate Users and Host Administrators Liabilities

Certificate users and host administrators have liabilities to protect certificates and private key from compromise by theft and lost thread..

2.2.4 Relying Party Liability

No stipulation.

2.2.5 User Administrator Liability

User administrator has a liability to ensure that enrollment information to NCHC CA is accurate.

2.2.6 Repository Liability

The repository has a liability to response to retrieve requests within operating time defined in section 2.1.6.

2.3 Financial Responsibility

No financial responsibility is accepted.

2.4 Interpretation and Enforcement

2.4.1 Governing Law

Insofar as any of the conditions stipulated in this document are ambiguous or unclear, exclusive reference shall be referred to Taiwan law, subject to NCHC's status as a nonprofit organization.

2.5 Fees

No fees are charged for any service provided by NCHC CA.

2.6 Publication and Repository

2.6.1 Publication

The following will be published in the repository operated by the NCHC CA:

- Client certificate information used for grid map file
- The CA certificate
- The CA certificate fingerprint
- The CRL issued by NCHC CA
- A copy of this CPS
- Other information deemed relevant to the NCHC CA

2.6.2 Frequency of Publication

- CA certificate, CA certificate fingerprint, and client certificate information will be published in the repository as soon as they are issued.
- CRL will be published in the repository as soon as they are issued or refreshed on schedule update.
- All NCHC CA documents will be published in the repository as they are updated.

2.6.3 Access Control

The information specified in section 2.6.1 is accessible through NCHC network under adequate access control.

2.6.4 Repository

The repository will store the information as specified in section 2.6.1 and the information is accessible from NCHC network.

2.7 Compliance Audit

2.7.1 Frequency of Entity Compliance Audit

The NCHC CA will accept at least one external Compliance Audit per year. The NCHC CA

also performs operational self-assessment of CA/RA at least once per year.

2.7.2 Identity/Qualifications of Auditor

The CA will be audited by other cross-certifying CAs.

2.7.3 Auditor's Relationship to Audited Party

It is desirable that the auditor is a third-party to NCHC CA.

2.7.4 Topics Covered by Audit

The audit will focus on whether the NCCH CA certification duties are compliant to this CPS.

The NCHC CA is expected to operate according to the minimum CA requirements specified by the Asia Pacific Grid Policy Management Authority (http://www.apgridpma.org/).

2.7.5 Actions Taken as a Result of Deficiency

The NCHC PMA has the responsibility for improving the deficiency. When the NCHC CA receives an audit report from the auditor, an improving report including timetable will be sent to the auditor.

2.7.6 Notification of Audit Results

The result of the audit will be made available to the members of Policy Management Authorities and operation. The NCHC PMA can decide whether the results of the audit will release to the public.

2.8 Confidentiality

2.8.1 Confidential Information

Except the information specified in section 2.6.1, all related information will be treated as confidential. Confidential information will not be provided to any other people. Confidential information including documents and electronic media will be stored securely.

2.8.2 Information Considered Not Confidential

Information specified in section 2.6.1 is not confidential information in this system.

2.8.3 Disclosure of Certificate Revocation or Suspension Information

The revocation date and reasons will be included in the published CRL when the user certificate is revoked. These are not confidential information, but other details will not be published.

2.8.4 Release to Law Enforcement Officials

No stipulation.

2.8.5 Release as Part of Civil Discovery

No stipulation.

2.8.6 Disclosure upon Owner's Request

The following information will be disclosed after the owner has been authenticated.

- Contents of the certificate
- Certificate Status

2.8.7 Other Information Release Circumstances

No stipulation.

2.9 Intellectual Property Rights

NCHC CA does not claim any IPR on issued certificates.

3. Identification and Authentication

3.1 Initial Registration

3.1.1 Types of Names

Identification of certificates will be according to X.500 distinguished name.

3.1.2 Name Meanings

Table 3 shows the attribute values used for the name of certificates issued by the NCHC CA.

Table 3 - Attributes used in certificates

Attributes	Meaning	Value
commonName	User name (Clients certificates)	
	Host name (Globus Server certificate)	GThost
	Host name (AG Server certificate)	AGhost
	Host name (Sensor Server certificate)	Sensorhost
organizationalUnitName	Name of organization unit	GOC
organizationName	Name of organizatin	NCHC
countryName	Name of country	TW

3.1.3 Rules for Interpreting Name Forms

Identifiers will be according to those regulated in table 3.

3.1.4 Uniqueness of Names

The distinguished name must be unique for each subject name issued by the NCHC CA.

3.1.5 Name Claim Dispute Resolution Procedure

No stipulation.

3.1.6 Recognition, Authentication and Role of Trademarks

No stipulation.

3.1.7 Method to Prove Possession of Private Key

NCHC RA confirms to prove possession of private key by verification of certificate issue request (CSR) signature.

3.1.8 Identity of Organizations

NCHC CA identifies the recognized organization within NCHC projects.

3.1.9 User Identity Authentication

A. Users from NCHC:

NCHC staff members will be identified by inspection of their badge IDs with photos on them. Inspection will take place in person by the user administrator.

B. Users from other participating organization:

Users from other participating organization will be identified through in-person interview by the user administrator. Photo-id or valid official documents must be presented at the interview.

3.2 Routine Rekey

Enrollment request is necessary if the certificate is expired

3.3 Rekey after Revocation

Rekey after revocation follows the same rules specified in section 3.1.

3.4 Revocation Request

Revocation request is confirmed that user and organization is authenticated by certificates issued based on section 3.1.

4. Operational Requirements

The requirements of this chapter are suitable for user and server certificates, not for CA self-signed certificates.

4.1 Certificate Application

4.1.1 Certificate Application

Users must present application form to the user administrator by e-mail. User administrator will examine it based on section 3.1.9. If the application is approved, then the user administrator will safely send a license ID (12 digit characters) which was issued by the CA and a URL which indicates the location for obtaining related information by e-mail.

4.1.2 Certificate Enrollment

Users need to create a key pair on user's machine. Then send a certificate signing request which contains the public key to the user administrator. Communication path to this enrollment will be encrypted.

4.2 Certificate Issuance

Users are provided an enrollment tool which supports creation of key pairs, making CSR, and the web enrollment functions provided in the standard Windows environment between NCHC CA and the users.

4.2.1 Receipt Certificate Enrollment

RA will perform the following steps after receiving the user certificate request:

- Prompt the user to input license ID.
- Verify the license ID.
- Prompt enrollment information including the subject information in the certificate.
- Send the certificate signing request to the CA server.

4.2.2 Certificate Issuance

The CA server will issue the user certificate signed with the CA private key, containing user public key information.

4.2.3 Certificate Subscription

Users retrieve certificates issued by the CA server via the RA server.

4.3 Certificate Acceptance

User and host administrator will register the certificate to the certificate stores based on the user's operational document.

4.4 Certificate Suspension and Revocation

The procedure is as same as the certificate enrollment. All communications are encrypted.

4.4.1 Circumstances for Revocation

A certificate will be revoked when the information it contains is suspected to be incorrect or compromised. This includes situations where:

- the user's private key is lost or suspected to be compromised.
- the information in the user's certificate is suspected to be inaccurate.
- the user violates his/her obligation specified in section 2.1.3.
- the CA private key is compromised.

4.4.2 Who Can Request Revocation

The certificate user can request revocation to the CA (RA server).The RA server will forward a revocation request to the CA based on user’s request.

4.4.3 Procedure for Revocation Request

The certificate user will send a revocation request to NCHC CA (RA Server) when the revocation circumstance occurs. RA server will authenticate the user as described in section 3.4. Then RA server sends revocation request to CA server. The CA server will revoke the certificate and update the signed CRL in the repository. When a certificate is revoked, the owner of the certificate will be notified the revocation by Email.

4.4.4 Revocation Request Grace Period

NCHC CA will process revocation as soon as it receives the request. The information of revocation will be posted in the repository.

4.4.5 Circumstances for Suspension

The NCHC CA does not support Certificate suspension.

4.4.6 Who Can Request Suspension

The NCHC CA does not support Certificate suspension.

4.4.7 Procedure for Suspension Request

The NCHC CA does not support Certificate suspension.

4.4.8 Limits on Suspension Period

The NCHC CA does not support Certificate suspension.

4.4.9 CRL Issuance Frequency

The NCHC CA will issue a new CRL and publish it in the repository. The CRL is valid for 30 days, and it will be reissued at least 7 days before expiration.

4.4.10 CRL Checking Requirements

A relying party will verify a certificate by retrieving the newest CRL published in the repository.

4.4.11 Availability of On-line Revocation/Status Checking

No stipulation.

4.4.12 Requirements for On-line Revocation Checking

No stipulation.

4.4.13 Other Available Methods Validity Checking

No stipulation.

4.4.14 Verification Requirements for Other Available Validity Checking Methods

No stipulation.

4.5 Security Audit Procedures

The NCHC CA will retain records as much as possible so that the NCHC CA could trace anything if something illegal would happen. Auditors are allowed to access to the information as part of auditing and such information must be kept confidential.

4.5.1 Types of Events Recorded

A. CA server logs:

- CA server access log
- Certificate and CRL issue and revocation log
- Error log
- OS login, logout, reboot log

B. RA server logs:

- CRL publisher activity log
- CRL publisher error log
- RA server access log
- Certificate issue, revocation log
- Error log
- OS login, logout, reboot log
- HSM log

C. CA room logs

4.5.2 Frequency of Processing Logs

No stipulation.

4.5.3 Retention Period for Audit Log

The minimum retention period is 3 years.

4.5.4 Protection of Audit Log

Access logs and system logs are protected and provided by the operating system. Access logs and system logs are periodically backed up to the offline media which is stored in a safe box. For logs of physical access to the CA room, each paper sheet is signed by the user administrator. Filled paper sheets and access logs to the CA room are stored in a safe box.

4.5.5 Audit Log Backup Procedures

CA operators will get each type of log recorded by the CA server and other systems in the external media weekly, and store them monthly.

4.5.6 Audit collection system

No stipulation.

4.5.7 Recorded Event Notification

No stipulation.

4.5.8 Vulnerability Assessments

No stipulation.

4.6 Records Archival

4.6.1 Types of Event Recorded

The NCHC CA will store the following archive data:

- All certificates and the CRL issued by the NCHC CA
- All enrollments submitted by users and any notifications sent to users
- All records related to the CA key
- All the logs as specified in section 4.5.1.
- All auditing records
- This CPS and operational procedures documents
- Other important materials related to decisions of the NCHC PMA

4.6.2 Retention Period for Archive

Archived data will be stored for 3 years.

4.6.3 Protection of Archive

The protection of archive logs are specified in section 4.5.4. Archive data will be protected in a safe box with appropriate entry control.

4.6.4 Archive Backup Procedures

CA operators will archive the CA server and other data in the external media weekly, and store them monthly.

4.6.5 Requirements for Time-stamping of Records

Archive data stored in electronic form will be time stamped.

4.6.6 Archive Collection System

No stipulation

4.6.7 Procedures to Verify Archive Information

No stipulation.

4.7 Key Changeover

4.7.1 User Certificate Validity

Each user certificate will be required renewal within the validity period:

Table 4 - User certificate validity

Type		Validity
Client certificate		1 year
Server certificate	Globus server	1 year
	Access Grid / Conference Server	1 year
	Sensor Net Server	1 year
	Unicore Server	1 year
	LDAP Server	1 year

4.7.2 CA Certificate Validity

The CA will stop issuing new user certificates with the CA private key when the validity of CA certificate is less than the validity of user certificate. The validity of CA certificate is 10 years.

4.8 Compromise and Disaster Recovery

4.8.1 Computing Resources, Software, and Data Are Corrupted

If hardware, software and data are corrupted, the system must be recovered as soon as possible.

4.8.2 CA Private Key Is Compromised

If the CA private key is compromised through theft of the HSM, loss of the management keys, or other means, all related persons will be notified, and operation will be stopped. If it is determined that the CA private key has been compromised, all certificates will be revoked so that any relying party does not trust the CA.

If the CA manager determines that it is too difficult to continue operation using the same private key, the CA certificate will be revoked. Once the security of the CA is confirmed, a new NCHC CA key pair will be generated, and the CA system will be rebuilt.

4.8.3 Secure Facilities after Natural or Other Disaster

The procedures are given as in section 4.8.1

4.9 CA Termination

The certification manager will inform any related parties in advance regarding the termination of the CA operations and preservation of related backup data.

5. Physical, Procedural, and Personnel Security Controls

5.1 Physical Security Controls

5.1.1 Site Location and Construction

NCHC CA system will be located at a safe place to prevent some damage from water exposure, earthquake, fire and other disasters.

5.1.2 Physical Access

The CA server is located at a locked room and physical access to the room is restricted to explicitly authorized person. All events about the access to the room must be recorded in the CA room logs. The events include the names of CA operators, date and time of entering/leaving the room, and the purpose of the access to the room.

5.1.3 Power and Air Conditioning

The CA room will be equipped with adequate air conditioning to maintain a suitable environment for the CA server, other relevant devices, and the CA staff to perform their duties.

5.1.4 Water Exposures

No stipulation.

5.1.5 Earthquake and Protection

A building is earthquake resistant construction and has countermeasures against equipment to fall down.

5.1.6 Fire Prevention and Protection

A building is fire-resistant construction and the room is fire prevention cell with fire protection.

5.1.7 Media Storage

Media will be stored in the safe box in CA room where adequate access control is done.

5.1.8 Waste Disposal

It is according to the NCHC waste disposal process for the document or media containing confidential information.

5.1.9 Off-Site Backup

No stipulation.

5.2 Procedural Controls

5.2.1 Trusted Roles

The staff is assigned trusted roles as defined in section 1.3.

5.2.2 Number of Persons Required Per Task

The number of staff required for each of the tasks is defined in section 1.3.2 and the number of persons for each task is described the following:

- CA Manager: 3
- CA Operators: 4
- User Administrator: 1

All the staff can be act as a help desk staff.

5.2.3 Identification and Authentication for Each Role

The system will identify and authenticate the operators when the staff operates the system.

5.3 Personnel Security Controls

All of personnel controls will be regulated in other document.

5.3.1 Background Checks and Clearance Procedures for CA Personnel

CA personnel are recruited from the NCHC.

5.3.2 Background Checks and Security Procedures for Other Personnel

No stipulation.

5.3.3 Training Requirements and Procedures

Internal training is given to CA operators.

5.3.4 Training Period and Retraining Procedures

No stipulation.

5.3.5 Frequency and Sequence of Job Rotation

No stipulation.

5.3.6 Sanctions against Personnel

No stipulation.

5.3.7 Controls on Contracting Personnel

No stipulation.

5.3.8 Documentation Supplied to Personnel

The relevant procedural manuals required for operation of the NCHC CA will be provided to the staff according to their roles.

6. Technical Security Controls

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

A. CA Key:

The CA Key pair is generated by the operation staff using Hardware Security Module (HSM).

B. User Key:

The User key pair is generated by software in each user's hardware.

6.1.2 Private Key Delivery to Entity

The user's private key is generated by the user. Therefore, it will not be distributed by the NCHC CA.

6.1.3 Public Key Delivery to Certificate Issuer

The user's public key will be sent to the Certificate Issue Request (CSR) at the time of enrollment.

6.1.4 CA Public Key Delivery to Users

The CA certificate is published in the repository.

6.1.5 Key Sizes

For client certificate the key size is 1024 bits (RSA). For server certificate the key size is 1024 bits (RSA). NCHC CA key length is 2048 bits (RSA).

6.1.6 Public Key Parameters Generation

No stipulation.

6.1.7 Parameter Quality Checking

No stipulation.

6.1.8 Hardware/Software Key Generation

It is defined in the section 6.1.1.

6.1.9 Key Usage Purposes (X.509 v3 KeyUsage Field)

The user's private key is used for digital signatures and shared-key encryption. The purpose will be set in the extension field of "KeyUsage" of the certificate.

6.2 Private Key Protections

6.2.1 Cryptographic Module Standards

The CA private key is protected by HSM compliant with FIPS140-1 Level3.

6.2.2 Private Key Multi-Person Control

NCHC CA implements multi-person control for the access to the CA server as described in the section 5.1.2.

6.2.3 Private Key Escrow

No stipulation.

6.2.4 Private Key Backup

A. CA private key:

The backup of the CA private key will be saved in the HSM token and stored in a safe place. Backup is made by the CA manager and CA operation staff.

B. User private key:

The users will backup and management their own private keys.

6.2.5 Private Key Archive

No stipulation.

6.2.6 Private Key Entry into Cryptographic Module

When the CA private key is generated or recovered from backup media, it must be protected by a pass phrase of at least 15 characters and must be done by the CA manager and operation staff. The pass phrase is known by only the CA manager and the operation staff.

6.2.7 Method for Activating a Private Key

The CA private key will be activated in HSM by a CA manager and a member of operation staff.

6.2.8 Method of Deactivating a Private Key

The CA private key will be deactivated in HSM by a CA manager.

6.2.9 Method of Destroying a Private Key

No stipulation.

6.3 Other Aspects of Key Pair Management

6.3.1 Public Key Archive

No stipulation.

6.3.2 Usage Periods for Public and Private Keys

Usage periods for public and private keys are specified in the section 4.7.1.

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

The CA private key is activated using a password and HSM physical key. The password is made by the operation staff.

6.4.2 Activation Data Protection

The password must be at least 15 characters. The HSM physical key is protected by the CA manager and kept in a lockable cabinet.

6.4.3 Other Aspects of Activation Data

No stipulation.

6.5 Computer Security Controls

6.5.1 Specific Computer Security Technical Requirements

The CA server is only equipped with the functionalities required to operate the NCHC CA, and only used for the jobs regulated in this CPS. CA server is a dedicated to the CA

operation.

6.5.2 Computer Security Ratings

No stipulation.

6.6 Life Cycle Technical Controls

6.6.1 System Development Controls

No stipulation.

6.6.2 Security Management Controls

No stipulation.

6.6.3 Life Cycle Security Ratings

No stipulation.

6.7 Network Security Controls

The CA and RA servers will be placed in an independent network segment with a dedicated connection to each other. Communication between the CA and RA servers is done in a secure way to prevent the unauthorized access.

6.8 Cryptographic Module Engineering Controls

No stipulation.

7. Certificates and CRL Profile

7.1 Certificate Profile

Certificate profile is described in a separate document, “NCHC CA Certificate and CRL Profile”.

7.2 CRL Profile

CRL profile is described in a separate document, “NCHC CA Certificate and CRL Profile”.

8. Specification Administration

8.1 Specification Change Procedures

If necessary, the NCHC PMA can change this document.

8.2 Publication and Notification Policies

This document and any older versions are available in repository given in section 2.1.6.

All major changes related to policy, technology or security must be approved by NCHC PMA. Revision is made and approved by NCHC PMA. Minor changes related to editorial problems can be made without approved by NCHC PMA. New OID will be assigned to major changes and will not be assigned to minor changes.

All the changes and revision to this document must be declared in repository. If there are substantial changes, notification should be mailed to all relevant CA's participants.

8.3 CPS Approval Procedures

All major changes must be approved by the NCHC PMA.

9. Glossary

Accreditation Authority (AA) – An ESI management Entity with the authority to permit a subordinate ESI Entity to operate within a particular domain. The PA is the accreditation authority for all connections to the AESI. A particular department within an Agency may be assigned the role of accreditation authority for the Level One CA within that Agency.

Activation Data – The private data that are required to access cryptographic modules (pass phrase, biometric authentication, any items other than the direct cryptographic keys).

Affiliated Certificate – A certificate issued to an affiliated individual. (*see* Affiliated Individual)

Affiliated Individual – a person affiliated with an organization (i) as an officer, director, employee, partner, contractor, intern, or other role within the organization, or (ii) as a person maintaining a contractual relationship with the organization where the organization has business records providing strong assurances of the identity of such person. (*see* Affiliated Certificate)

Authentication – relates to the process where one party has presented an identity and claims to be that identity. Authentication of a Subscriber by a CA or RA enables the Relying Party to be confident that the assertion is legitimate.

Authenticating Entity – the Entity performing authentication and asserting that the Subscriber is the party they are represented to be.

Authority Revocation List (ARL) – A list of revoked CA certificates. An ARL is a CRL for CA cross–certificates.

Archive – to store records and associated journals for a given period of time for security, backup, or auditing purposes.

Arizona Electronic Signature Infrastructure (AESI) –This is the set of organizations, policies, processes and equipment used to administer Arizona's electronic signature tools and the instruments created from their use. [This is an extension of the definition of PKI to include the fact that Arizona's statute recognizes the possibility of non–PKI based electronic signatures.] The AESI is defined and managed by the Policy Authority with support from the Office of the Secretary of State, GITA and State Treasurer's Office as defined in the Administrative Rules and Statute.

Audit – a procedure that validates that appropriate controls are in place. An audit would include recording and analyzing activities to detect intrusions or abuses of the information system. Inadequacies are appropriately reported.

Availability – the extent that information or processes are reasonably accessible and usable as needed by authorized Entities allowing timely performance of time–critical operations.

Binding – an affirmation by a CA (or its LRA) of the relationship between a named Entity and its Public Key.

Certification – The process where a CA issues a Certificate for a Subject's Public Key and sends that Certificate to the Subject for acceptance and, on acceptance, posts that certificate in a Repository. [Some non–AESI systems employ a less restrictive process]

Certificate – The public PKI–based key of a Subscriber (or non–PKI technology based equivalent), together with related information, digitally signed with the private PKI–based key of the Certification Authority that issued it(or non–PKI technology based equivalent). The certificate technology is in accordance with standards established by GITA.

The Certificate data record, at a minimum: (a) identifies the Issuing CA; (b) 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 signed by the Issuing CA. As used by AESI, the term of "Certificate" refers to certificates that expressly reference the OID of a specific Certificate Policy in the "*CertificatePolicies*" field of a PKI Certificate or the non–PKI equivalent..

Certificate Repository – The party maintaining a list of valid PGP certificates. They may or may not have a CRL or a list of certificates showing when they were valid for validation after the fact.

Certificate Revocation List (CRL) – A list maintained by a Certification Authority of the certificates that it has issued that have been revoked before their scheduled expiration date.

A CRL is a time stamped list identifying revoked certificates which is signed by a CA and made available in a Repository. Each revoked certificate is identified in a CRL by its certificate serial number. When a End–Entity uses a Certificate (e.g., for verifying a Subject's electronic signature), the End–Entity not only checks the certificate signature and validity but also acquires a reasonably current CRL and checks that the certificate serial number is not on that CRL. The appropriate CP and CPS will define what is "reasonably current," but it usually means the most recently–issued CRL. A CA issues a new CRL on a regular periodic basis (e.g., hourly, daily, or weekly). CAs may also issue CRLs when an important key is deemed compromised and the CA wishes to expedite notification of that fact.

On– line methods of revocation notification may be applicable as an alternative CRL in some circumstances. PKIX defines a protocol known as OCSP [OCSP] to facilitate on–line checking of the status of certificates. On–line revocation checking may significantly reduce the delay between a revocation report and the information reaching Relying Parties. This requires a trusted Validation Authority rather than the trust indifference in using a CRL, that is, this method is faster but imposes new security requirements since the Relying Party must trust the on–line Validation Authority while the repository does not need to be trusted.

CA Applicant – an Entity submitting a CA application to the PA requesting to become a CA or subordinate CA under the terms of a CP. (*see* Subscriber)

Certificate Applicant – an Entity requesting the issuance of a Public Key Certificate by an CA. (*see* CA Applicant; Subscriber)

Certificate Application – a request from a Certificate Applicant to a CA for the issuance of a Certificate. (*see* Certificate Applicant; Certificate Signing Request)

Certificate Chain – an ordered list of Certificates containing an End–Entity Subscriber Certificate and CA Certificates (*see* Valid Certificate)

Certificate Expiration – the time and date specified in the certificate when the operational period ends, without regard to any earlier suspension or revocation.

Certificate Extension – a PKI certificate may employ extension fields to convey additional information about the Public Key being certified, the Subscriber, the Certificate Issuer, and elements of the certification process (such as identifying the Certificate Policy by OID).

Standard extensions will be used by CAs within AESI. Custom extensions can also be defined within a Certificate Policy issued by the Policy Authority.

Certificate Hierarchy – the ESI domain of CAs, each categorized with respect to its role in a "tree structure" of subordinate CAs. A CA issues and manages Certificates for End–Entity Subscribers and/or for one or more CAs at the next level. The CP defining an ESI establishes certain uniform practices for addressing issues such as naming, maximum number of levels, etc., to assure integrity of the domain and thereby ensure uniform accountability, auditability, and management through the use of trustworthy operational processes. A CA in an ESI is in a trust hierarchy and shall conform to the practices established in the CP..

Certificate Issuance – the actions performed by a CA creating a certificate and notifying the certificate Applicant (anticipated to become a Subscriber) listed in the Certificate's contents.

Certificate Management – certificate management includes, but is not limited to, storage, dissemination, publication, revocation, and suspension of certificates. An CA undertakes certificate management functions by serving as a Registration Authority for Subscriber Certificates. A CA designates issued and accepted Certificates as valid by publication to a Repository.

Certificate Serial Number – a value that unambiguously identifies a Certificate generated by a CA.

Certificate Signing Request (CSR) – a machine–readable form of a certificate application. (*see* Certificate Application)

Certification Authority (CA) – An authority trusted by one or more users to issue and manage Certificates and CRLs. Each CA within the AESI may issue certificates under a choice of policies based on the assurance level the CA has been accredited to and the requirements and role of the Subscriber. It is important to note that the CA is responsible for the certificates during their whole lifetime, not just for issuing them.

Certificate Manufacturer (CM)– the Entity that manufactures and delivers PGP Certificates. The Subscriber may do this themselves, but this may be delegated to another. The CM is not responsible for identification and authentication of certificate Subjects, the RA is.

Certificate Manufacturing Authority (CMA) – the Entity that manufactures and delivers the Certificates signed by an CA. The CA may do this itself, but it may subcontract this activity. The CMA is not responsible for identification and authentication of certificate Subjects, the CA is.

Certificate Policy (CP) – a named set of rules that indicates the applicability of a certificate to a particular community with a class of applications having common security requirements. For example, a particular certificate policy might indicate applicability of a type of certificate to the authentication of electronic procurement transactions within a given price range.

Certification Authority Software – The cryptographic software required to manage the PKI keys (or non–PKI technology based equivalent) of End Entities.

Certification Practice Statement (CPS) – a statement of the practices that a Certification Authority employs in issuing, suspending, revoking, and renewing Certificates and providing access to them. The CPS is a statement of the CA's practices that fulfill and expand on the specific requirements the Policy Authority has published in the Policy Authority Practices document and in the specific Certificate Policy document that the CPS is bound to.

Class [n] Certificate – A certificate of a specified level of trust (denoted as n).

Compromise – an unauthorized disclosure (or loss of control) of sensitive information may have occurred in violation (or suspected violation) of a security policy *(see* Data Integrity). Usually discussed in terms of compromise of a Certificate's Private Key.

Confidentiality – the need to keep sensitive data secret and disclosed only to authorized parties.

Confirmation Of Certificate Chain – the process of validating a certificate chain and subsequently validating a Subscriber certificate. (*see also* Valid Certificate)

The Relying Party, to authenticate the public key (in each certificate), must confirm that each certificate in the chain is valid, that each was issued within the operational period of the corresponding CA certificate, and that all parties (CAs, Subscribers, and Relying Parties) have operated in accordance with the appropriate CP as well as the appropriate CA's CPS for each certificate in the chain.

Cross–Certificate – A Certificate used to establish a trust relationship between two Certification Authorities.

A Cross–Certificate is a Certificate issued by one CA to another CA which contains a public CA key associated with the private CA signature key used for issuing Certificates. Typically, a cross– certificate is used to allow End Entities in one ESI to communicate security with End Entities in another ESI (but may also occur within a single ESI). Use of a cross–certificate

issued from CA#1 to CA#2 allows Entity#a (who trusts, has a Certificate issued by, CA#1) to accept a certificate used by Entity#b (who trusts, hase a Certificate issued by CA#2). Cross–certificates between two CA's can be issued in one direction only, or in both directions. The cross–certification often is for a specific Class or for a specific Class and "higher" so cross–certification involves a "mapping" of Certificate Class attributes between the two CAs to assure a correct match between them.

Cryptographic Algorithm – a clearly defined mathematical computation, that is, a complete set of rules to produce a prescribed result.

Cryptography – is both a mathematical method and a discipline using that method.

The mathematical method assures the confidentiality and authentication of data by replacing it with a transformed version that can be converted back into the original data but only by someone possessing the appropriate cryptographic algorithm and key for converting it back to the original form.

The discipline employs the method along with related principles, means, and processes for transforming data to 1) hide its content, 2) prevent it being modified without detection, and 3) prevent unauthorized uses of it.

Data Integrity – Assurance that the data are unchanged from creation to reception.

Digital Signature – The result of a transformation of a message by means of a cryptographic system using keys such that a person who has the initial message can determine: (a) whether the transformation was created using the key that corresponds to the signer's key; and (b) whether the message has been altered since the transformation was made. [Note that Digital Signature is commonly associated with PKI–based technology whereas Arizona recognizes a wider range of possible signature technologies – see Electronic Signature.]

Distinguished Name (DN) – a data set that identifies an Entity in the real world (such as a natural person) in the electronic context. *(e.g.,* countryName=US, state=California, organizationName=Electronic Inc., commonName=JohnDoe).

Electronic Signature – [Note that whereas Arizona recognizes a wider range of possible signature technologies, most common current implementations employ PKI–based technology – see Digital Signature.]

Electronic Signature Infrastructure (ESI) – A set of organizations, policies, processes and equipment established within AESI to administer a specific community or class of applications. [This is an extension of the definition of PKI to include the fact that Arizona's statute recognizes the possibility of non–PKI based electronic signatures.]

Encryption – the process of transforming ordinary text data into an unintelligible form (ciphertext) so the original data cannot be either recovered directly (one–way encryption) or through an inverse decryption process (two–way encryption).

Enrollment – the process of an applicant applying for a Certificate.

Extensions – the extension fields in PKIX based certificates.

End–Entity – An entity that uses the keys and certificates created within the ESI for purposes other than the management of the aforementioned keys and certificates. An End–Entity may be a Subscriber, a Relying Party, a device, or an application.

Entity – Any autonomous element within the Electronic Signature Infrastructure. This may be a CA, an LRA, or an End–Entity.

Government Information Technology Agency (GITA) – Agency directed by Arizona's CIO.

Issuing Authority Certificate – a certificate issued by an superior IA/CA to a subordinate IA/CA. (*see* Issuing Authority, topCA, Level One CA, and Level Two CA)

Identification / Identify – the process of confirming a person's identity. Certificates facilitate identification in public key cryptography (and non–PKI equivalent systems).

Internet Engineering Task Force (IETF) – is a large, open international community of network designers, operators, vendors, and researchers collaborating on the evolution of the Internet architecture to improve the operation of the Internet.

Issuing CA –the CA that signed and issued the particular certificate. (*see* Issuing Authority)

Issuing Authority (IA) – the CA that signed and issued the particular certificate.

Key Generation – the trustworthy process of creating a Private Key and Public Key pair. The Public Key is supplied to a CA during the certificate application process while the Private Key is only supplied to the Subscriber.

Key Pair – two keys mathematically related such that (i) one key can be used to encrypt a message which can then only be decrypted using the other key, and (ii) even knowing one key, it is computationally infeasible to discover the other key (or the non–PKI equivalent).

Key Pair Recovery – Some CPs will provide for having key exchange or encryption keys "backed up" or recoverable in case the key is lost and access to previously encrypted information is needed. This will seriously damage any claim for Non–Repudiation and is only used in implementations where the importance of information recovery over–rides the need for Non–Repudiation. The issue is generally to read e–mail or other documents encrypted by or for a particular employee when that employee is no longer available to access the document. In such a case, the Subject's Private Key is backed up by a CA or by a separate key backup system. If Subject or the Subject's employer needs to recover these backed up key materials, the ESI must provide a system that permits the recovery without an unacceptable risk of compromise of the Private Key. Key Pair Recovery Repositories should never include Certificates where Non–Repudiation is paramount. Inclusion in such a Repository opens a challenge to any claim for Non–Repudiation.

Level One CA – The highest level CA within a State agency. Level One CAs are cross–certified with the AESI and may also be cross–certified with subordinate departmental (Level Two) CAs.

Level Two CA – Any CA within a State agency that is subordinate to the Agency's Level One CA.. Level Two CAs are cross–certified with the Agency (Level One) CAs with that cross–certification process subject to approval by the PA.

Local Registration Authority (LRA) – A person or organization that is responsible for the identification and authentication of certificate Subscribers before certificate issuance, but does not actually sign or issue the certificates. A LRA is delegated certain tasks on behalf of a CA. [see Registration Authority]

Notary - a natural person authorized by State of Arizona to perform notarial services which include witnessing or attesting to signatures.

Non–Repudiation – asserts proof of the origin or delivery of data in order to protect the sender against a false denial by the recipient that the data has been received or to protect the recipient against false denial by the sender that the data has been sent. Only a trier of fact (someone with the authority to resolve disputes) can actually make a determination of nonrepudiation. An electronic signature verified in accordance with the relevant CPS can provide proof in support of a determination of nonrepudiation by a trier of fact, but does not by itself constitute nonrepudiation.

Object Identifier (OID) – The unique alphanumeric/numeric identifier registered under the ISO registration standard to reference a specific object or object class. In the AESI PKI they are used to uniquely identify each of the eight policies and cryptographic algorithms supported.

Operational Authority – Agency personnel who are responsible for the overall operation of an AESI CA.

Operational Certificate – a certificate within its operational period at the specified date and time.

Operational Period – the period beginning with the date and time the certificate was issued (or on a later date and time if so stated in the certificate) and ending with the earlier date and time of either when it expired or when was revoked.

Organization – A agency, department, corporation, partnership, trust, joint venture, or other association or governmental body.

Out–of–band – parties communicate by a different method from the current method of communication (e.g., one party using U.S. Postal mail to communicate with the other party while current communication is done online).

Policy Authority (PA) – The State of Arizona body responsible for setting, implementing, and administering policy decisions regarding CPs and CPSs throughout the AESI.

The PA signs and manages the cross–certificates of State of Arizona Agency Level One CAs. The PA also signs and manages cross–certificates with non–State of Arizona CAs. The PA does not manage any Subscriber certificates.

Private Key – The key of a key pair used to create a digital signature. It is the publicly *unknown* half of the Public/Private key pair employed by PKI technology to uniquely link a key pair to the entity possessing the Private key of the pair while the world possesses the Public key of the pair (used here to also define the non–PKI technology based equivalent of these elements).

Public Key – The key of a key pair used to verify a digital signature. It is the publicly *known* half of the Public/Private key pair employed by PKI technology to uniquely link a key pair to the entity possessing the Private key of the pair (used here to also define the non–PKI technology based equivalent of these elements).

Public Key Infrastructure (PKI) – A set of organizations, policies, processes, and equipment used to administer public/private keys and certificates created from their use. [Note that Arizona's statute recognizes the possibility of non–PKI based electronic signatures.]

"A collection of certificates, with their issuing CA's, subjects, relying parties, RA's, and repositories, is referred to as a Public Key Infrastructure, or PKI." from the IETF draft *Internet X.509 Public Key Infrastructure PKIX Roadmap* (draft–ietf–pkix–roadmap–02.txt)

Registration – The process where a Subject: 1) applies for a Certificate with a CA (directly, or through an RA), and 2) the CA issues a Certificate(s) for that Subject. Registration involves: 1) the Subject's providing the personal information required for the Class of Certificate applied for, and other attributes needed to be put in the Certificate, followed by 2) the CA's (possibly with help from the RA) verifying in accordance with its CPS that the name and other attributes are correct.

Registration Authority (RA) – an entity that may be given responsibility for performing some of the administrative tasks necessary in the registration of Subjects, such as: confirming the Subject's identity; validating that the Subject is entitled to have the attributes requested in a Certificate; and verifying that the Subject has possession of the Private Key associated with the Public Key requested for a Certificate. [see Local Registration Authority]

Relying Party – A person who: 1) uses a certificate signed by a AESI CA to authenticate an electronic signature or to encrypt communications to the certificate Subject, and 2) is a Subscriber of a AESI CA or a ESI that is cross–certified with the AESI.

Repository – A location where CRLs, ARLs and Certificates are stored for access by End–Entities. (*see* Repository Services Provider)

Responsible Individual - represents the sponsoring organization with respect to the issuance and management of certificates. The Responsible Individual is responsible for properly indicating which subscribers are to receive Certificates.

Revocation – A Certificate is expected to be in use for its entire validity period when it is issued. But various circumstances can invalidate a certificate prior to its expiration date. Such circumstances include change of Subject name, change of association between Subject and

CA, and compromise or suspected compromise of the Certificate's Private Key. The CA will then need to revoke the certificate. Current protocols define one method of certificate revocation which involves each CA periodically issuing a signed data structure called a CRL (*see* Certificate Revocation List).

Root CA (rootCA) – a CA that is directly trusted by an end entity [the process of securely acquiring the value of a root CA public key requires some out–of–band step(s)]. Note that this term is not meant to imply that a root CA is necessarily at the top of any hierarchy, simply that the CA in question is trusted directly. [For top of a hierarchy CA, see topCA]

Repository Services Provider (RSP) - a Certificate Authority or their agent that maintains the CA's Repository. An RSP by provide services to more than one CA. (see Certificate Authority, Repository)

RSA – An public–key encryption technology developed by RSA Data Security, Inc. The acronym RSA stands for the technique's inventors: Rivest, Shamir, and Adelman. They developed the RSA algorithm from the fact that there is no efficient way to factor very large numbers. Therefore deducing an RSA key requires an extraordinary amount of computer processing power and time. RSA has become the de facto standard for industrial–strength encryption, especially for data sent over the Internet.

Sponsor – A Sponsor in the AESI is the Agency, department or public servant who has nominated that a specific individual or organization be issued a certificate. (e.g., for an employee this may be the employee's manager). In the case of a certificate for a citizen or a commercial enterprise the Sponsor could be the manager of the State of Arizona business unit that has a requirement to communicate with that Entity.

The Sponsor might suggest an appropriate DN for the certificate and will be responsible for either supplying or confirming that the certificate attribute details to the LRA. The Sponsor is also responsible for informing the CA or LRA if the Sponsor's relationship with the Subscriber is terminated or has changed such that the certificate should be revoked or updated.

Subject – a subject is the entity (CA or End–Entity) named in a Certificate. Subjects can be natural persons, devices or even software agents.

Subordinate CA – a CA that is not a rootCA for the End Entity in question. A subordinate CA will usually not be a rootCA for any entity but this is not mandatory

Subscriber – An individual or organization whose Public Key is certified in a Certificate. In the AESI this could be a public servant, a citizen, or a government client or supplier. Subscribers may have one or more certificates from a specific CA associated with them; most will have at least two active certificates – one containing their Electronic Signature verification key; the other containing their Confidentiality encryption key.

Time Stamp – a notation indicating the correct date and time of an action and the identity of the End–Entity that sent or received the time stamp.

Token – a hardware security token containing an End Entity's Private Key(s), Public Key Certificate, and, optionally, a cache of other Certificates, including all certificates in the End–Entity's Certification Chain.

Top CA (topCA) – a CA that is at the top of the ESI hierarchy. Note: this is often also called a "root CA" since, in data structures terms and in graph theory, the node at the top of a tree is the "root". However, to minimize confusion, it is here called the "Top CA" or "topCA" with "root CA" reserved for the CA directly trusted by the user. [Readers should be aware that these terms are not used consistently throughout the Electronic/Digital Signature community. Some documents use "root CA" to refer to what other documents call a "top CA", and "most–trusted CA" to refer to what this and other documents call a "root CA".]

Transaction – an electronic transfer of information (typically over the Internet).

Trust – the assumption that an Entity will behave substantially as expected. Trust may be only extended for one specific function. The key role of this term within Authentication is to describe the relationship between an authenticating Entity and a CA. An authenticating Entity must be certain that it can trust the CA to create only valid and reliable Certificates, and that Relying Parties and other users of those Certificates rely upon the authenticating Entity's determination of trust.

Trusted Person – a person who serves in a trusted position and is qualified to serve in it in accordance with the governing CP and CPS. *(see* Trust; Trusted Position; Trusted Third Party)

Trusted Position – the role within a CA that includes access to or control over operations that may materially affect the issuance, use, suspension, or revocation of certificates.

Trusted Root – a trusted root is the Public Key that an Entity will find reaffirmed as bound to a CA. Software and systems implementing authentication based on PKIX and Certificates assume that this key value has been correctly obtained. It is confirmed by always accessing it from a trusted system Repository that can only be modified by identified and trusted administrators.

Type (Of Certificate) – the critical properties of a certificate that limit its intended purpose to a class of applications uniquely associated with that type. (*see* Class [n] Certificate)

Uniform Resource Locator (URL) – the addressing method used for identifying and locating certain records and other resources located on the World Wide Web.

Validation Authority (VA) –

Valid Certificate – a Certificate that

- was issued by an Approved CA.
- was accepted by the Subscriber listed in it.
- has not expired.
- has not been revoked.

A Certificate is not "valid" until it is both issued by an Approved CA and been accepted by the Subscriber.

Validate A Certificate Chain - see Confirmation of Certificate Chain.

Verify (A Digital Signature) – to determine for a given digital signature and message that

- the digital signature was created while the Certificate was valid.
- the message has not been altered since the digital signature was created.
- some Certificate Policies will also require Confirmation of the Certificate Chain, that is, that each Certificate in the chain was valid at the time the digital signature was created.

10. References

[1] RFC2527, "Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework", March 1999. http://www.ietf.org/rfc/rfc2527.txt