NCHC CP/CPS v 1.1.0

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. This document is structured according to the RFC3647

(RFC3647 obsolete RFC2527). Not all sections of RFC3647 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.

1.2. Document Name and 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	1.3.6.1.4.1.23308.1.1.2.0
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. PKI Participants

1.3.1. Certification Authority

The NCHC CA does not issue certificates to subordinate certification authorities.

1.3.2. Registration Authorities

The NCHC CA delegates the authentication of individual identity to Registration Authorities (RA). RAs must sign an agreement with the NCHC CA, stating their adherence to the procedures described in this document. The following is the NCHC RA registration procedure:

- RA applicant must accept the CP/CPS and agree to all RA responsibilities.
- RA applicant must be an employee of the institution or organization and provide work ID or proof of work.
- Complete the RA application form and fax it to NCHC CA.
- Send a verification e-mail to NCHC CA.
- NCHC CA will then arrange face-to-face meeting with the RA applicant.
- After completing the request, NCHC CA will publish the RA contact information on NCHC CA public website.

1.3.3. Subscribers (End Entities)

The NCHC CA issues person, host and service certificates for following subjects: 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.

1.3.4 Relying parties

NCHC CA's relying parties includes the following:

- Employees of NCHC or research institutes in Taiwan
- Employees of international research institutes which collaborate with NCHC in Grid computing area.
- Resource-sharing organizations with NCHC

Relying parties' obligations are as follows:

- Must read the procedures published by the NCHC CA.
- Must use the certificates for the permitted uses only.
- Must notify NCHC CA of any security incidents.
- May verify that the certificate is not on the CRL before validating a certificate.

1.3.5 Other participants

No stipulation.

1.4. Certificate Usage

1.4.1. Appropriate certificate uses

Certificates from NCHC CA may be used in applications for the following purposes:

- Grid middleware
- Other general or specific requirements of Grid computing

1.4.2. Prohibited certificate uses

Certificates issued by the CA must not be used for:

- Electronic commerce.
- Military usage.

1.5. Policy Administration

1.5.1. Organization administering the document

This policy is developed and maintained by NCHC PMA (Policy Management Authority), Taiwan.

1.5.2. Contact person

Contact point for questions related to this policy is:
Policy Management Authority

> *Huang, Weicheng*
> Grid Technology Team, NCHC
> No. 7, R&D Rd. VI, Hsinchu Science Park, Hsinchu, Taiwan, R.O.C. 30076
> Phone: +886-3-5776085 ext.323
> Email: nchcca@nchc.org.tw or whuang@nchc.org.tw

1.5.3. Person determining CPS suitability for the policy

See section 1.5.2.

1.5.4. CPS approval procedures

- Major changes must be approved by the APGrid PMA community.
- Minor changes can be done by NCHC CA PMA, and should be notified through the APGrid PMA mailing list.

1.6. Definitions and Acronyms

Certification authority (CA)

An authority trusted by one or more users to create and assign public key certificates. Optionally the CA may create the user's keys. The CA is responsible for the public key certificates during their whole lifetime, not just for issuing them.

Activation Data

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

CA certificate

A certificate for one CA's public key issued by another CA.

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 policy (CP)

A named set of rules that indicates the applicability of a certificate to a particular community or class of application with common security requirements. For example, a particular certificate policy might indicate applicability of a type of certificate to the authentication of electronic data interchange transactions for the trading of goods within a given price range.

Certification path

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

Certification practice statement (CPS)

A statement of the practices that a certification authority employs in issuing certificates.

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 time stamped list identifying revoked certificates, which is signed by a CA and made freely available in a public repository.

Issuing certification authority (issuing CA)

The CA that issues the certificate (see also Subject certification authority).

Public key certificate (PKC)

A data structure containing the public key of an end entity and some other information, which is digitally signed with the private key of the CA that issued it.

Public Key Infrastructure (PKI)

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

Registration authority (RA)

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

Relying party

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

Subject certification authority (subject CA)

In the context of a particular CA-certificate, the subject CA is the CA whose public key is certified in the certificate.

2. Publication and Repository Responsibilities

2.1. Repositories

NCHC CA operates a secure online repository at http://ca.goc.nchc.org.tw/ that contains:

- NCHC CA's certificate;
- All Certificates issued by NCHC CA;
- A Certificate Revocation List (CRL) signed by NCHC CA;
- A copy of this policy;
- Other information relevant to the NCHC CA.

2.2. Publication of certification information

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

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 shall be mailed to all relevant CA's participants.

2.3. Time or 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.

2.4. Access controls on repositories

- The online repository is available on a substantially 24X7 basis, subject to reasonable scheduled maintenance.

3. Identification and Authentication

3.1. Naming

3.1.1. Types of names

Identification of certificates will be according to X.500 distinguished name.
Table 2 shows the attribute values used for the name of certificates issued by the NCHC CA.

Table2 - Attributes used in certificates

Attributes	Meaning	Value
commonName	Subscriber's name	Based on application information
	Host name	Based on application information
organizationalUnitName	Name of organization unit	Based on application information
organizationName	Name of organization	Based on application information
country Name	Name of country	TW

3.1.2. Need for names to be meaningful

- Each host certificate must be linked to a single network entity.
- The common name of the host certificate must be the FQDN of the host.
- The Subject Name in a certificate MUST have a reasonable association with the End Entity.

3.1.3. Anonymity or pseudonymity of subscribers

The subscribers can not be anonymous or pseudonymous.

3.1.4. Rules for interpreting various name forms

See section 3.1.1.

3.1.5. Uniqueness of names

- The Distinguished Name(DN) must be unique for each subject name issued by the NCHC CA.
- For user certificates each CN component will include the full name of the subscriber and a serial number.

3.1.6. Recognition, authentication and role of trademarks

No Stipulation

3.2. Initial Identity Validation

3.2.1. Method to prove possession of private key

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

3.2.2. Authentication of organization identity

NCHC CA identifies the recognized organization within NCHC projects.

3.2.3. Authentication of individual identity

1. Users Certificate (from NCHC) :

- NCHC staff members will be identified by inspection of their badge IDs. Inspection will take place by the RA Operator.

1. User Certificate (from other participating organization):

- A subscriber requesting a user certificate must fill the personal data in enrollment form which is public on NCHC CA website and send to RA. RA will dispatch user administrator to check the identity of the person by comparing the information presented by enrollment form. The check will include at least the following items:
    - User Name
- Organization
- Mail address
- Work ID or National ID

1. Host or Service Certificate:

Requests must be authorized as a legal subscriber of the CA and RA's approval is required before issuing host/service certificates for a proof of the subscriber's title of the host/service FQDN.

3.2.4. Non-verified subscriber information

No Stipulation

3.2.5. Validation of authority

No Stipulation

3.2.6. Criteria for interoperation

No Stipulation

3.3. Identification and Authentication for Re-key Requests

3.3.1. Identification and authentication for routine re-key

Enrollment request is necessary if the certificate is expired

3.3.2. Identification and authentication for re-key after revocation

Rekey after revocation follows the same rules as an initial registration.

3.4. Identification and Authentication for Revocation Requests

Contact personally the CA/RA staff in order to verify his/her identity and the validity of the request.

4. Certificate Life-Cycle Operational Requirements

4.1 Certificate Application

4.1.1 Who Can Submit a Certificate Application

The subscriber can be the person in specific organization, described in session 1.3.3 .

4.1.2 Enrollment Process and Responsibilities

The subscriber is required to:

- Provide correct information at the enrollment.
- Manage the certificate and private key safely to prevent unauthorized uses.
- The pass phrase for the private key must be at least 12 characters and rsa key must be at least 1024 bits.
- 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.

Request process is as follow and more detailed describes are announced on NCHC CA public web :

1. Subscriber shall fill out the certificate application form and transfer it to the RA .
2. RA will contact and interview Subscriber to check the correctness of personal data according to session 3.2.3 .
3. If the interview examines is pass, NCHC CA will reply subscriber a confirmation email with License ID (12 characters) and URL which indicates the location for enrollment web page.
4. Subscriber can login the secure http web page (through personal information and the License ID in the confirmation email) and upload his/her CSR (Certificate Signing Request).
5. If previous process without mistake, NCHC CA will sign the CSR as soon as possible and reply subscriber with signed certificate by email.
6. NCHC CA will announce the issued certificate and related information on the NCHC CA public web

4.2. Certificate Application Processing

4.2.1. Performing identification and authentication functions

The NCHC CA will check :

- The information of application form
- The License ID and personal information.
- The key length of the certificate is at least 1024 bits.

4.2.2. Approval or rejection of certificate applications

- If approval, NCHC CA will reply subscriber with the issuance of certificate.
- If any condition specified in section 4.2.1 is not be satisfied, the certificate application is rejected and the CA notifies to the subscriber with the reason of the rejection.

4.2.3. Time to process certificate applications

CA will process certificate applications as soon as possible.

4.3. Certificate Issuance

4.3.1. CA actions during certificate issuance

- The CA will announce all of the issued certificate on the NCHC CA public web, and the subscriber can download these.

4.3.2. Notifications to subscriber by the CA of issuance of certificate

see session 4.2.2

4.4. Certificate Acceptance

- Subscriber and host administrator can register the certificate to the certificate stores (ex: explorer).
- If the issued certificate has any problem, the subscriber

should notify the CA that he can not accept the issued certificate with a proper reason within 7 days from issuance of the certificate.

- Unaccepted certificate should be revoked and the certificate should be re-issued.

4.5. Key Pair and Certificate Usage

- NCHC CA certificates may be used for any software for grid computing.
- The certificates could be used in other capacities, but the NCHC CA does not recommend or warrant any other use of the certificates it signs.
- User certificates must not be shared between multiple people.
- Host certificates must be linked to a single network entity.
- The subscriber must manage his certificates and private keys securely. To protect the private key the subscriber must encrypt his private with a pass phrase. The pass phrase must not be less than 12 characters long.

4.6. Certificate Renewal

NCHC CA does not permit certificate signing request with the same key as the previous certificate.

4.7. Certificate Re-key

Subscriber should revoke this certificate in session 4.9, and then request a new certificate in session 4.1.

4.8. Certificate Modification

NCHC CA does not support certificate modification.

4.9. Certificate Revocation and Suspension

4.9.1. Circumstances for revocation

- NCHC CA can revoke the certificate and inform the subscriber if a certificate is revoked.
- subscriber must revoke his/her certificate when information is suspected security problems. These include situations where:
  - The subscriber's private key is compromised or is suspected to have been compromised.
- The subscriber's information in the certificate is suspected to be inaccurate.
- The subscriber is known to have violated his obligations which could induce a critical security hole.
- The subscriber leaves his/her organization.
- In case of host/service certificates, the corresponding host/service is retired.

4.9.2. Who Can Request Revocation

NCHC CA will accept a revocation request made by

- Any other entity presenting evidence of circumstances that the criteria described in section 4.2.1 has been violated.
- Any entities presenting evidence of the compromise of associated private key.

4.9.3. Procedure for Revocation Request

1. The subscriber shall send a revocation request to NCHC CA
2. RA will authenticate the subscriber as described in section 3.4.
3. Then RA will forward revocation request to CA.
4. CA will revoke the certificate and update the signed CRL in NCHC CA public web.A revocation notification is sent to the subscriber through the subscriber's email.

4.9.4. Revocation request grace period

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

4.9.5. Time within which CA must process the revocation request

The CA should process the certificate revocation request within 1 working day from the recognition of the request.

4.9.6. Revocation checking requirement for relying parties

No stipulation.

4.9.7. CRL Issuance Frequency (if applicable)

- The lifetime of the CRL is 30 days.
- A new CRL is issued immediately after a revocation or at least 7 days before expiration.

4.9.8. Maximum latency for CRLs (if applicable)

CRLs must be published in the repository after generation as soon as possible.

4.9.9. On-line revocation/status checking availability

Not support.

4.9.10. On-line revocation checking requirements

Not support.

4.9.11. Other forms of revocation advertisements available

No stipulation.

4.9.12. Special requirements re key compromise

No stipulation.

4.9.13. Circumstances for suspension

Not support.

4.9.14. Who can request suspension

Not support.

4.9.15. Procedure for suspension request

Not support.

4.9.16. Limits on suspension period

Not support.

4.10. Certificate Status Services

No stipulation.

4.11. End of Subscription

If a subscriber of NCHC CA end the subscription to the CA services :
The subscriber must do the following:

- Must not use any certificate issued from NCHC CA

The CA must do the following:

- Must revoked all certificates issued for the subscriber.

4.12. Key Escrow and Recovery

No stipulation.

5. Management, Operational, and Physical Controls

5.1. Physical Security Controls

5.1.1. Site location and construction

NCHC CA is located at NCHC which is a safe place to prevent some damage from water exposure, earthquake, fire and other disasters in Hsinchu, Taiwan.

5.1.2. Physical access

Both CA signing server and CA web server are running on dedicated machines and located in a secure environment where access is controlled. All events about the access to the room must be recorded.

5.1.3. Power and air conditioning

CA signing server and the web server are both protected by uninterruptible power supplies. Environment temperature in rooms containing CA related equipment is maintained at appropriate levels by suitable air conditioning systems.

5.1.4. Water exposures

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

5.1.5. Fire prevention and protection

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

5.1.6. Media storage

The NCHC CA key and backup copies of CA is securely kept in removable storage media stored in the safe place where adequate access control.

5.1.7. Waste disposal

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

5.1.8. Off-site backup

No stipulation.

5.2. Procedural Controls

5.2.1. Trusted roles

Table 3 shows the operating roles and functions.

Table 3 - Operating roles and functions

Role	Function
CA Manager	Manage all CA tasks Manage CA private key and its copy Approve CA and RA operator to operate affairs
CA Operator	Operate and maintain the CA signing server and CA web server Operate CA tasks
RA Operator	Accept subscribing request

	Check subscribers' information and approve them
Subscriber	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

5.2.2. Number of persons required per task

The number of staff required for each of the tasks is defined in section 5.2.1 and the number of persons for each task is described the following:

- CA Manager: 3
- CA Operators: 4
- RA Operator: 1
- All the CA/RA staffs 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.

5.2.4. Roles requiring separation of duties

No stipulation.

5.3. Personnel Security Controls

All access to the servers and applications that comprise the NCHC CA is limited to NCHC CA security staffs.

5.3.1. Qualifications, experience, and clearance requirements

CA personnel are recruited from the NCHC.

5.3.2. Background check procedures

CA personnel must be a formal member of NCHC.

5.3.3. Training requirements

Internal training is given to CA/RA Operators.

5.3.4. Retraining frequency and requirements

No stipulation.

5.3.5. Job rotation frequency and sequence

No stipulation.

5.3.6. Sanctions for unauthorized actions

No stipulation.

5.3.7. Independent contractor requirements

No stipulation.

5.3.8. Documentation supplied to personnel

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

5.4. Audit Logging 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.

5.4.1. Types of events recorded

- Access log of CA signing server and CA online web server
- Issue and revocation log of certificate
- Issue and publish log of CRL
- OS login, logout, reboot log

5.4.2. Frequency of processing log

CA personnel will record each type of log at least once every month.

5.4.3. Retention period for audit log

The minimum retention period is 3 years.

5.4.4. Protection of audit log

The CA shall protect the electronic audit log system and audit information captured electronically or manually from unauthorized viewing, modification, deletion or destruction.

5.4.5. Audit log backup procedures

The CA shall back up or copy all audit logs and audit summaries.

5.4.6. Audit collection system (internal vs. external)

No stipulation.

5.4.7. Notification to event-causing subject

No stipulation.

5.4.8. Vulnerability assessments

No stipulation.

5.5. Records Archival

5.5.1. Types of records archived

The NCHC CA will store the following archive data:

- All certificates and the CRL issued by the NCHC CA
- All enrollments or revocations, including all supporting documents, submitted by users
- All records related to the CA key
- All the logs as specified in section 5.4.1
- All auditing records
- This CPS and operational procedures documents
- Other important materials related to decisions of the NCHC PMA

5.5.2. Retention period for archive

Archived data will be stored for 3 years.

5.5.3. Protection of archive

Archive data with digital form will be stored in a secure operation system or back media, archive data with manual will be protected in a safe box with appropriate entry control.

5.5.4. Archive backup procedures

A second copy of all material retained or backed up must be stored in read-only media like CD-ROM.

> The second copy must be protected either by physical security alone, or a combination of physical and cryptographic protection.

5.5.5. Requirements for time-stamping of records

Archive data stored in electronic form will be time stamped.

5.5.6. Archive collection system (internal or external)

No stipulation.

5.5.7. Procedures to obtain and verify archive information

No stipulation.

5.6. Key Changeover

- Old CA's cryptographic data will not be used for signing purpose until new cryptographic data is generated when the CA's cryptographic data needs to be changed (ex: private key expired or some other security reason).
- The overlap of the old and new CA certificate must be at least the longest time an end-entity certificate can be valid during 1 year.
- The old CA certificate will be valid and available to verify old signatures and the secret key to sign CRLs until all the certificates signed using the associated private key have also expired.
- Usage periods for key lifetime are specified in session 6.3.2.

5.7. Compromise and Disaster Recovery

5.7.1 Incident and Compromise Handling Procedures

If it is detected that hardware, software or data are corrupted or damaged

- Recover the system by using backup hardware, software, or data as quickly as possible.

If a CA's private key is compromised or suspected to be compromised, the NCHC CA will

- Notify subscribers, RAs and relying parties.
- Revoke all issued certificates.
- Terminate the certificates and CRLs distribution service for certificates/CRLs issued using the compromised private key.
- Create a new pair of key and re-build the CA system.

5.7.2 Computing Resources, Software, and/or Data Are Corrupted

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

5.7.3 Entity Private Key Compromise Procedures

no stipulation.

5.7.4 Business Continuity Capabilities After a Disaster

no stipulation.

5.8. CA or RA Termination

Before NCHC CA terminates its services it will

- Make publicly available information of its termination.
- Stop issuing certificates and CRLs.
- Destroy its private key's and all copies.
- backup all the operating data and archive these.

6. Technical Security Controls

6.1. Key Pair Generation and Installation

6.1.1. Key pair generation

- A CA key pair is generated by CA staff on NCHC CA signing machine which is kept offline.
- End entities' cryptographic keys are locally generated by their application during the requesting process.

6.1.2. Private key delivery to subscriber

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

6.1.3. Public key delivery to certificate issuer

End entity will upload its CSR include its public key at the time of enrollment procedure.

6.1.4. CA public key delivery to relying parties

CA certificate will be published on the NCHC CA repository.

6.1.5. Key sizes

- The minimum key length for user/host/service certificate is 1024 bits (RSA).
- NCHC CA key length is 2048 bits (RSA)

6.1.6. Public key parameters generation and quality checking

No stipulation

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

- NCHC CA private key is the only key used for signing CRLs and Certificates for user/host/service.
- 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 Protection and Cryptographic Module Engineering

6.2.1. Cryptographic module standards and controls

NCHC CA do not use any hardware security module.

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

Not supported.

6.2.3. Private key escrow

No stipulation.

6.2.4. Private key backup

The NCHC CA private key backup is performed by CA Manager and the copies of backup key is kept in offline media respectively in a safe place where access is controlled.

6.2.5. Private key archival

No stipulation.

6.2.6. Private key transfer into or from a cryptographic module

No stipulation.

6.2.7. Private key storage on cryptographic module

No stipulation.

6.2.8. Method of activating private key

- NCHC CA private key must be protected by a pass phrase of at least 15 characters when the CA private key is generated
- It must be done by the CA Manager or CA Operator with getting the CA Manager agreement.
- The pass phrase is known by only the CA Managers or specific persons.

6.2.9. Method of deactivating private key

The CA private key will be deactivated by the CA Manager.

6.2.10. Method of destroying private key

No stipulation.

6.2.11. Cryptographic Module Rating

No stipulation.

6.3. Other Aspects of Key Pair Management

6.3.1. Public key archival

The CA shall retain all significant public key certificates it generates.

6.3.2. Certificate operational periods and key pair usage periods

- The validity of each user/host/service certificate and key pair is 1 year.
- The validity of CA certificate and key pair is 10 years.

6.4. Activation Data

see session 6.2.8.

6.5. Computer Security Controls

6.5.1. Specific computer security technical requirements

- CA operating systems are maintained at a high level of security by applying all the relevant patches.
- All related CA machine are used for dedicated purpose respectively.

6.5.2. Computer security rating

No stipulation.

6.6. Life Cycle Security Controls

No stipulation.

6.7. Network Security Controls

- The CA signing server is kept off-line.
- The CA web server is protected by a firewall.
- Appropriate software upgrade/patch of the CA web server is performed every 6 month or

immediately if it is required.

6.8. Time-stamping

No stipulation.

7. Certificate and CRL Profiles

7.1. Certificate Profile

7.1.1. Version number(s)

X.509 v3.

7.1.2. Certificate extensions Â¶

- **CA Certificate:**

name	value
X509v3 Basic Constraints	critical, CA:TRUE
X509v3 Key Usage	critical, Certificate Sign (keyCertSign), CRL Sign (cRLSign)
X509v3 Subject Key Identifier	[the unique Key ID]
X509v3 Authority Key Identifier	keyid DirName serial
X509v3 Subject Alternative Name	email:nchcca@nchc.org.tw, URI:http://ca.goc.nchc.org.tw/
X509v3 Issuer Alternative Name	email:nchcca@nchc.org.tw, URI:http://ca.goc.nchc.org.tw/
Certificate Policies	1.3.6.1.4.1.23308.1.1.2.0
X509v3 CRL Distribution Points	URI:http://ca.goc.nchc.org.tw/nchcca/CRL/

- **User Certificates:**

name	value
X509v3 Basic	critical

Constraints	CA:FALSE
X509v3 Key Usage	critical, Digital Signature (digitalSignature), Non Repudiation (nonRepudiation), Key Encipherment (keyEncipherment), Data Encipherment (dataEncipherment) Key Agreement (keyAgreement)
X509v3 Extended Key Usage	TLS Web Client Authentication(clientAuth)
X509v3 Subject Key Identifier	[the unique Key ID]
X509v3 Authority Key Identifier	keyid DirName serial
X509v3 Issuer Alternative Name	email:nchcca@nchc.org.tw, URI:http://ca.goc.nchc.org.tw/
X509v3 Certificate Policies	1.3.6.1.4.1.23308.1.1.2.0
X509v3 CRL Distribution Points	URI:http://ca.goc.nchc.org.tw/nchcca/CRL/

- **Host Certificates:**

name	**value**
X509v3 Basic Constraints	critical CA:FALSE
X509v3 Key Usage	critical, Digital Signature (digitalSignature), Non Repudiation (nonRepudiation), Key Encipherment (keyEncipherment), Data Encipherment (dataEncipherment) ,Key Agreement (keyAgreement)
X509v3 Extended Key Usage	TLS Web Server Authentication(serverAuth), TLS Web Client Authentication(clientAuth)
X509v3 Subject Key Identifier	[the unique Key ID]
X509v3 Authority Key Identifier	keyid DirName serial
X509v3 Issuer Alternative Name	email:nchcca@nchc.org.tw, URI:http://ca.goc.nchc.org.tw/

X509v3 Certificate Policies	1.3.6.1.4.1.23308.1.1.2.0
X509v3 CRL Distribution Points	URI:http://ca.goc.nchc.org.tw/nchcca/CRL/

7.1.3. Algorithm object identifiers

Signature Algorithm: **sha1WithRSAEncryption(2048 bits)**

7.1.4. Name forms

name	**value**
Issuer	C=TW, O=NCHC, OU=GOC, CN=NCHC CA
User DN	C=TW, O=[applicant's organization], OU=[applicant's organization unit], CN=[the name of applicant with serial]
Host DN	C=TW, O=[applicant's organization], OU=[applicant's organization unit], CN=[FQDN of the hostname]
Service DN	C=TW, O=[applicant's organization], OU=[applicant's organization unit], CN=[the name of service with serial]

7.1.5. Name constraints

Subject DN can contain the following characters:

Alphabetic characters: **a-z, A-Z**
Numerical character: **0-9**
Special character: **-(dash), _(underscore), .(full stop)**

No other characters are not allowed for the subject name.

7.1.6 Certificate policy object identifier

X509v3 Certificate Policies: Policy: **1.3.6.1.4.1.23308.1.1.2.0**

7.1.7 Usage of policy constraints extensions

No stipulation.

7.1.8 Policy qualifier syntax and semantics

No stipulation.

7.1.9. Processing semantics for the critical Certificate Policies extension

No stipulation.

7.2. CRL Profile

CRLs are signed by the NCHC CA private key and are published in a web page.

7.2.1. Version number(s)

X.509 v2.

7.2.2. CRL and CRL entry extensions

Message digest algorithm of the CRL: **SHA-1**

7.3. OCSP Profile

7.3.1. Version number(s)

No stipulation.

7.3.2. OCSP extensions

No stipulation.

8. Compliance Audit and Other Assessment

8.1. Frequency of Entity Compliance Assessment

The NCHC CA will accept external Compliance Audit.

In addition, the NCHC CA performs operational self-assessment at least once per year.

8.2. Identity/Qualifications of Assessor

NCHC CA can be audited by the APGrid PMA (Asia Pacific Grid Policy Management Authority).

8.3. Assessor's relationship to assessed entity

NCHC CA can be audited by the APGrid PMA.

8.4. Topics Covered by Assessment

The audit will focus on whether the NCHC CA certification duties are compliant to this CPS. The NCHC CA is expected to operate according to the minimum CA requirements specified by the APGrid PMA.

8.5. 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.

8.6. Communications of Results

The result of the audit will be made available to the members of APGrid PMA. The NCHC PMA can decide whether the results of the audit will release to the public.

9. Other Business and Legal Matters

9.1. Fees

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

9.2. Financial Responsibility

No financial responsibility is accepted.

9.3 Confidentiality of Business Information

9.3.1 Scope of confidential information

Except the information specified in section 5.2.1, 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.

9.3.2 Information not within the scope of confidential information

Information specified in section 5.2.1 is not confidential information in this system.

9.3.3 Responsibility to protect confidential information

No stipulation.

9.4. Privacy of Personal Information

Subscribers shall supply these information in enrollment form and we do not provide this information to other organizations :

- Name, Gender
- Country
- Organization Name, Organization Unit Name
- Position
- Email, Telephone
- WorkID, NationalID

9.5. Intellectual Property Rights

All certificate related data issued by NCHC CA is not under any copyright or intellectual property protection.

9.6. Representations and Warranties

No stipulation.

9.7. Disclaimers of Warranties

No stipulation.

9.8. Limitations of Liability

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 RA Operators of the operating organization.
- Issue license IDs to the RA Operators.
- 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.

9.9. Indemnities

No stipulation.

9.10. Term and Termination

9.10.1. Term

This CP/CPS is valid and enforceable from the time of accreditation by APGrid PMA.

9.10.2. Termination

This CP/CPS terminates in the following cases:

- CA certificate expires
- CA terminates its service
- A new version of CP/CPS is accredited

9.10.3. Effect of termination and survival

No stipulation.

9.11. Individual notices and communications with participants

No stipulation.

9.12. Amendments

- This document and any older versions are available in repository given in section 2.1.
- All major changes related to policy, technology or security must be approved by APGrid PMA.
- Revision is made by NCHC PMA and approved by APGird PMA.
- Minor changes related to editorial problems can be made without approved by APGrid 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.

9.13. Dispute Resolution Procedures

No stipulation.

9.14. 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.

9.15. Compliance with Applicable Law

No stipulation.

9.16. Miscellaneous Provisions

No stipulation.

9.17. Other Provisions

No stipulation.