NECTEC-GOC CA

Certificate Policy
and
Certificate Practice Statement

Version 1.3
Jan, 2014

National Electronics and Computer Technology Center,Thailand

Document History

Document Name	Document Version	Status	Date	By Whom	Review	Remarks
NECTEC-GOC CA CP/CPS	1.0	Created	15 Oct 2006	Suriya U-ruekolan, Sornthep Vannarat	NECTEC Grid PMA	Reviewed by APGrid PMA
NECTEC-GOC CA CP/CPS	1.1	Modified	6 Aug 2009	Suriya U-ruekolan, Sornthep Vannarat	NECTEC Grid PMA	Added Classic AP 4.2 profile OID
NECTEC-GOC CA CP/CPS	1.2	Modified	10 May 2010	Suriya U-ruekolan, Sornthep Vannarat	NECTEC Grid PMA	Updated CP/CPS to conform with RFC3647
NECTEC-GOC CA CP/CPS	1.3	Modified	2 Jan 2014	Suriya U-ruekolan, Sornthep Vannarat	NECTEC Grid PMA	Changed certificate and CRL signature algorithm from SHA-1 to SHA-2

Contents

1 Introduction

1.1 Overview

National Electronics and Computer Technology Center(NECTEC), Thailand operates a Certification Authority called NECTEC Grid Operation Center Certification Authority (NECTEC-GOC CA) for Grid PKI services. Structured according to RFC3647 [RFC3647] (obsolete RFC2527), this document describes policy and practices of NECTEC-GOC CA established by NECTEC-GOC PMA for the operations of the NECTEC-GOC CA. Not all sections of RFC3647 are used. Sections that are not included have a default value of No stipulation.

This document includes both the Certificate Policy and the Certification Practices Statement for the NECTEC-GOC CA. It is the intent of the NECTEC-GOC CA to issue user and host/services certificates for use in Grid projects. These certificates will be compatible with the Globus middleware that are used on these Grid projects.

The NECTEC-GOC CA is based on OpenCA Certificate Management System.

1.2 Document name and identification

NECTEC-GOC CA uses the following identifiers to identity this document and certificate policies.

- Document title: NECTEC-GOC CA Certificate Policy and Certificate Practice Statement
- Document version: 1.2
- OID: The following ASN.1 Object Identifier (OID) has been assigned to this document. This OID is constructed as shown in the Table 1:

Object	OID
IANA	1.3.6.1.4.1
National Electronics and Computer Technology Center(NECTEC)	1.3.6.1.4.1.25149
NECTEC Grid Operation Center (GOC)	1.3.6.1.4.1.25149.1
NECTEC-GOC CA	1.3.6.1.4.1.25149.1.1
CP/CPS	1.3.6.1.4.1.25149.1.1.1
Major Version	1.3.6.1.4.1.25149.1.1.1.1
Minor Version	1.3.6.1.4.1.25149.1.1.1.1.2

Table 1: OIDs of NECTEC-GOC

1.3 PKI participants

1.3.1 Organization

Figure 1 shows the organization of the NECTEC-GOC CA.

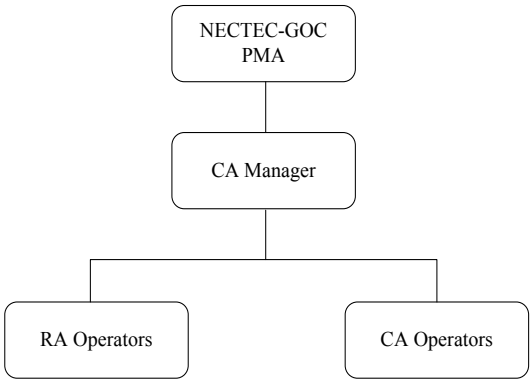

Figure 1: Organization of NECTEC-GOC CA

1.3.2 NECTEC-GOC Policy Management Authority

The decision related to the management of NECTEC-GOC CA will be performed by the coordinating committee called "NECTEC Grid Operation Center Policy Management Authority (NECTEC-GOC PMA)", which consists of representatives from Large Scale Simulation Laboratory, Network Technology Laboratory and Thai Computer Emergency Response Team of NECTEC. The NECTEC-GOC PMA is responsible for:

- Drafting and approving CP/CPS
- Taking countermeasure for the compromisation of the Certificate Authority(CA)'s private key
- Taking countermeasure in the case of emergencies
- Other important matters

1.3.3 CA Manager

The NECTEC-GOC CA Manager is responsible for:

- Administrating all tasks on the CA system including the management of CA private key

1.3.4 Certification Authorities

The NECTEC-GOC Certificate Authority (CA) is responsible for:

- Issuing certificates for users and hosts/services
- Managing CA and RA machines
- Maintaining the CA system
- Managing the CA's private key

The NECTEC-GOC CA does not issue certificates to subordinate certification authorities.

1.3.5 Registration Authorities

The NECTEC-GOC Registration Authority (RA) is responsible for:

- Accepting and verifies applicant's application forms
- Identifying the requester of certificates
- Checking the certificate signing request form
- Informing CA to issue certificates

1.3.6 Subscribers (End Entities)

NECTEC-GOC CA issues certificates for the following subjects:

- Host/service and users of domestic Grid-based Application/Projects

The term end entity is used to refer to the holder of private key. For a user certificate it will be the subscriber, and for a host or service certificate the end entity may be some process running on a machine. However, the application for a host/service certificate must be a person and, he/she must be responsible as the certificate end-entity. The subscriber/end-entity is required to:

- Read and adhere to the procedure published in this document
- Generate a key pair using a trustworthy method
- Take reasonable precautions to prevent any loss, disclosure or unauthorized use of private key associated with the certificate, including:
  - In case of user certificates
    - selecting a pass phrase of more than 12 characters
    - protecting the pass phrase from others
    - always using the pass phrase to encrypt the stored private key
    - never sharing the private key with other subscribers
  - In case of host/service certificates
    - storing the certificates encrypted whenever possible
    - providing the correct information and publication of the certificate
    - using the certificates for the permitted uses, only

1.3.7 Relying parties

The NECTEC-GOC CA's relying parties includes the following:

- Anyone who accepts IGTF CA distribution
- Anyone who accepts NECTEC-GOC CA's certificates

Relying parties are responsible for:

- Reading the procedures published by the NECTEC-GOC CA
- Using the certificates for permitted uses, only
- Notifying NECTEC-GOC CA of any relevant security incidents
- Verifying that the certificate is not on the CRL before validating a certificate

1.3.8 Other participants

No Stipulation.

1.4 Certificate usage

1.4.1 Appropriate certificate uses

Certificates from NECTEC-GOC CA are intended to be used for:

- Grid Authentication.

1.4.2 Prohibited certificate uses

Certificates issued by NECTEC-GOC CA must not be used for:

- Electronic commerce
- Transactions where applicable laws prohibit the use of digital signatures for such transactions or where otherwise prohibited by law

1.5 Policy administration

1.5.1 Organization administering the document

NECTEC-GOC PMA has the responsibility for administrating the NECTEC-GOC CA.

1.5.2 Contact person

Dr. Sornthep Vannarat and Mr. Suriya U-ruekolan
National Electronics and Computer Technology Center
Large Scale Simulation Research Laboratory
Grid Operation Center
112 Thailand Science Park, Phahon Yothin Rd., Klong 1, Klong Luang, Pathumthani
12120, THAILAND
Tel: (662) 564-6900 ext 2278 Fax: (662) 564-6776
Email: camanager@hpcc.nectec.or.th

1.5.3 Person determining CPS suitability for the policy

NECTEC-GOC PMA has the responsibility for determining CPS suitability for the policy.

1.5.4 CPS approval procedures

NECTEC-GOC CA is responsible for maintaining the CP/CPS. The modification must be authorized by the NECTEC-GOC PMA .

Whenever there is a minor change in the CP/CPS document, the O.I.D. of the document must change by incrementing the release number. This would include clarification of unclear meanings and alterations to procedures that have limited impacts.

Whenever there is a major or significant change in the CP/CPS document, it must be announced to and approved by the APGrid PMA before signing any certificates affected by that change.

Records will be maintained of changes against version and release numbers.

1.6 Definitions and acronyms

Definitions and acronyms are defined in Table 2

Acronyms	Fullname	Definition
CA	Certificate Authority	An entity which issues digital certificates for use by other parties. It is an example of a trusted third party. CAs are characteristic of many public key infrastructure (PKI) schemes.
CP	Certificate Policy	A named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements. For example, a particular certificate policy might indicate applicability of a type of certificate to the authentication of electronic data interchange transactions for the trading of goods within a given price range.
CPS	Certification Practice Statement	A statement of the practices, which a certification authority employs in issuing certificates.
CRL	Certificate Revocation List	A time stamped list identifying revoked certificates that is signed by a CA and made freely available in a public repository.
CRR	Certificate Revocation Request	A message sent from an applicant to a certificate authority in order to revoke for a digital identity certificate.
CSR	Certificate Signing Request	A message sent from an applicant to a certificate authority in order to apply for a digital identity certificate.
DN	Distinguished Name	A data set that identifies an Entity in the real world (such as a natural person) in the electronic context. (eg. CountryName=TH, OrganizationName=NECTEC, CommonName=Suriya)
EE	End-Entity	A certificate subject that does not sign certificates (i.e., user, host, and service certificates)
Entity		Any autonomous within the Electronic Signature Infrastructure. This may be a CA or an End-Entity.
PKC	Public Key Certificates	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.
PKI	Public Key Infrastructure	An arrangement that provides for trusted third party vetting of, and vouching for, user identities. It also allows binding of Public Keys to users.
RA	Registration Authority	An entity that is responsible for identification and authentication of certificate subjects but that does not sign or issue certificates (i.e., an RA is delegated certain tasks on behalf of a CA). The term Local Registration Authority (LRA) is used elsewhere for the same concept.
RP	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.
	Subscriber	In the case of certificates issued to resources (such as web servers), the person responsible for the certificate for that resource. For certificates issued to individuals, the certificate subject.

Table 2: Definitions and Acronyms

2 PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 Repositories

NECTEC-GOC CA on-line repository is available at http://gridca.hpcc.nectec.or.th.

2.2 Publication of certification information

NECTEC-GOC CA publishes the following information through its on-line repository.

- NECTEC-GOC CA's root certificate
- NECTEC-GOC CA's signing policy
- NECTEC-GOC CA's root certificate fingerprint
- CRLs issued by NECTEC-GOC CA
- End entity certificates issued by the NECTEC-GOC CA
- All the CP/CPS under which valid certificates are issued
- Other information relevant to the NECTEC-GOC CA

2.3 Time or frequency of publication

All certificates and related data is available publicly on the NECTEC-GOC CA repository shortly after it is created, or added. Certificate Revocation Lists (CRL) will be published every 30 days, with a buffer of 7 days before the expiry of the previous CRL. A new CRL must be issued immediately after a certificate revocation.

2.4 Access controls on repositories

- The on-line repository is available on a substantially 24x7 basis, subjected to reasonable scheduled maintenance.
- The NECTEC-GOC CA does not impose any access control on the information described in section 2.2.

3 IDENTIFICATION AND AUTHENTICATION

3.1 Naming

3.1.1 Types of names

The subject name is an X.500 Distinguished Name (RFC2459). It may be one of the following:

- In case of user certificate, the subject name must include the name that person generally uses.
- In case of host/service certificate, the subject name must include the fully qualified domain name of the host.

Table 3 shows the attribute values for name. Common Name is decided based on the application information provided by subscribers when requesting certificates.

Attributes	Meaning	Value
commonName	Applicant's name	Based on application information
	Host name	FQDN (Based on application information)
organizationUnitname	Organization Unit Name	GOC
organizationName	Organization Name	NECTEC
CountryName	Country name	TH

Table 3: Attributes used in the certificate

3.1.2 Need for names to be meaningful

The Subject Name in a certificate MUST have a reasonable association with the end entity. 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.

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 assigned unique among certificates issued by the NECTEC-GOC CA.
- Applicants cannot have the same common name. Host will always have different fully qualified domain names. OpenCA prevents the issuing of a certificate if the DN will clash with an existing valid certificate. Certificates must apply to unique individuals or resources. Subscribers must not share certificates.
- In the case that the desired common name of the applicant is repeated, the applicant must provide the extension to the common name. The RA and CA operator may reject an extension provided by an applicant if the extension is considered inappropriate. In the case that an extension is rejected, the applicant can purpose alternative extensions.
  - Impolite extensions are not allowed.
  - If the extension refers to an organization, the organization must be related to the end entity.
  - The extension must not lead to social conflicts.

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

NECTEC-GOC CA confirms the possession of a private key by verification of the CSR signature.

3.2.2 Authentication of organization identity

All certificates issued must be associated with an organization that is, in turn, associated with a Grid Project. For this purpose, only organizations personally known to be associated with a Grid Project by the CA Manager and / or the RA operator will be considered.

3.2.3 Authentication of individual identity

- User certificate: A person who requests a user certificate will be identified by in person interview with the RA operator. The applicant's photo ID must be presented at the interview.
- Host or Service certificate: The request must be submitted by a valid subscriber of NECTEC-GOC CA. That person must be the owner of domain/services or has been authorized by such owner to operate Grid services on such domain. Proof of such authorization, such as by an official letter or by setting a certain information in the DNS record of that domain, must be provided. The RA operator will approve name of requestor, FQDN and email in CSR which must match with in the application form. The certificate signing request must signing with a requestor's valid certificate.

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

Rekey before expiration can be accomplished by sending a rekey request based on a new public key. The RA operator will send renewal reminders at least a month before the expiration. The certificate of subscriber must not be re-keyed consecutively for more than 5 years. Authentication of person requesting rekeying must be performed by face to face meeting with RA operator at least every 5 years. After certificate expiration, rekeying of certificate follows the same rules as an initial registration.

3.3.2 Identification and authentication for re-key after revocation

The same procedure as for requesting a new certificate will be applied.

3.4 Identification and authentication for revocation request

For circumstance of revocation request in section 4.9.1 no authorization is necessary. However, the RA and CA operator shall take appropriate measures to verify the circumstance. For circumstance of revocation request in section 4.9.1.2, the certificate holder must submit a revocation request to an RA operator via email signed with a valid and trusted certificate.

4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 Certificate Application

Enrollment process is as follows:

- The applicant must have a face to face meeting with an RA operator and hand in the application form and CSR at the meeting time.
- The RA operator checks whether the email specified in the application form matches that in the CSR. The certificate will be delivered via this email address.

- The RA operator will sign the CSR and store it in a USB flash drive, then pass the flash drive and the application form to the CA operator, by hand.
- The CA operator verifies the CSR and the application form, and informs the result to the RA operator, who will inform the result to the applicant.
- If the CSR and the application form are valid, the CA operator will begin the certificate generation. Otherwise, the applicant will be instructed to correct the problems before making another request.

Certificate application process is as follows:

- The RA operator uploads the CSR in to the certificate request web interface.
- The RA operator logs in to the RA website, and follows the menu tabs to the Active CSRs → new and clicks Search. The RA operator uses the applicant's serial number to find the request.
- The RA operator checks that the applicant's name is identical to the name on the certificate.
- The RA operator then checks that the certificate lifetime is not more than 13 months (or n/a, which shall be replaced by 13 months), and that the organization unit field is correct. If these or anything else are incorrect, the RA operator can correct them.
- If the RA operator is satisfied with the application, then the CSR will be sent to the CA operator, otherwise the RA operator must reject application.
- The approved request will then be signed by the CA operator, this is generally done at the end of each business day. The subscriber should then follow the instructions on the NECTEC-GOC CA website for collecting his/her certificate. The RA operator is not required to do anything further.
- Subscriber can generate the CSR using either the Globus certificate request tools, or OpenSSL tools.

4.2 Certificate application processing

4.2.1 Performing identification and authentication functions

NECTEC-GOC CA ensures the followings in the enrollment process and the certificate application process: In the enrollment process:

- The application form and the CSR are correct.
- The RA examines the subscriber in a face to face meeting.

In the certificate application process:

- The certificate request is done in accordance with the process in this document especially in the section 4.1.
- The CSR has the correct format.
- The key length of the certificate request meets the requirement.
- The applicant of host/service certificate has the authority to do so.

4.2.2 Approval or rejection of certificate applications

- The issuance of a certificate by the CA indicates a complete and final approval of the certificate application by the CA.
- If any conditions specified in section 4.2.1 are not satisfied, the certificate application is rejected and the CA notifies to the subscriber the reasons of the rejection.

4.2.3 Time to process certificate applications

The RA operator should process the certificate application within 3 business days from the acceptance of the certificate request.

4.3 Certificate issuance

- The CA operator received the CSR, signed by the RA's digital signature, which is kept in a USB flash drive.
- The CA operator validates the RA digital signature on the CSR.
- The CA operator issues the certificate containing the public key with the CA signature and keeps the certificate in a USB flash drive and directly delivers to the RA operator .
- The RA operator uploads the certificate to the certificate request web interface.
- The RA operator notifies the subscriber with the instructions on how to download the certificate from the on-line public web server.
- The subscriber downloads his/her certificate.

4.4 Certificate acceptance

- If a certificate becomes unacceptable to a subscriber, the subscriber can revoke it.

4.4.1 Publication of the certificate by the CA

NECTEC-GOC CA publishes the certificate at the on-line certificate repository by the RA operator .

4.4.2 Notification of certificate issuance by the CA to other entities

The CA operator stores the certificate on a USB flash drive and sends to the RA operator by hand for publishing the certificate on web server.

4.5 Key pair and certificate usage

4.5.1 Subscriber private key and certificate usage

- The certificate issued by this CA should not be used for any objectives other than those explicitly written in this document.
- NECTEC-GOC CA does not warrant any usages other than those explicitly written in this document.
- A subscriber's certificate must not be shared by multiple people.
- A host certificate must be linked to a single network entity.
- The subscriber must manage his/her certificates and private keys securely. To protect the private key the subscriber must encrypt his private key with a pass phrase. The pass phrase must be more than 12 characters long.

4.6 Certificate renewal

4.6.1 Circumstances for certificate renewal

NECTEC-GOC CA does not support the key renewal.

4.6.2 Who may request renewal

Nobody can request renewal of certificates.

4.6.3 Processing certificate renewal requests

No stipulation.

4.6.4 Notification of new certificate issuance to subscriber

No stipulation.

4.6.5 Conduct constituting acceptance of a renewal certificate

No stipulation.

4.6.6 Publication of the renewal certificate by the CA

No stipulation.

4.6.7 Notification of certificate issuance by the CA to other entities

No stipulation.

4.7 Certificate re-key

4.7.1 Circumstance for certificate re-key

Generally, certificate re-key can or must take place in cases such as:

- After a certificate is revoked for the reasons of private key compromise.
- After a certificate and its key pair have expired.
- 30 days prior to the expiration of the end entities certificate.

4.7.2 Who may request certification of a new public key

A subscriber who meets the condition in section 4.7.1 can request for rekey.

4.7.3 Processing certificate re-keying requests

- If certificate is revoked for reasons that private key is compromised. The compromised certificate must be revoked and the certificate subscriber should follow the enrollment process described in section 4.1
- If certificate and its key pair have expired, the subscriber of the certificate must follow the enrollment process described in section 4.1
- If there are only no more than 30 days prior to the expiration of the end entities certificate, the certificate subscriber must follow the following procedure:
  - The subscriber, who has a valid certificate, must fill the renew application form and send to RA operator via email or fax. The subscriber needs not to participate in the face to face meeting with RA operator.
  - The subscribe should request for the rekey using the online request form and sign the CSR by the valid certificate issued by NECTEC-GOC CA, only. After that the subscriber should send a CSR with the valid signature to RA operator via email: rastaff@hpcc.nectec.or.th.
  - In the email, the subscriber has to mention the current certificate serial number and the newly rekey CSR number.
  - NECTEC-GOC CA does not permit a certificate signing request with the previously used key. The new certificate request must use a new key, which is not the same key that was used in previous certificate.

4.7.4 Notification of new certificate issuance to subscriber

Covered in section 4.1.

4.7.5 Conduct constituting acceptance of a re-keyed certificate

Covered in section 4.1.

4.7.6 Publication of the re-keyed certificate by the CA

Covered in section 4.4.1.

4.7.7 Notification of certificate issuance by the CA to other entities

Covered in section 4.4.2.

4.8 Certificate modification

NECTEC-GOC CA does not support certificate modification.

4.9 Certificate revocation and suspension

4.9.1 Circumstances for revocation

The subscribers must inform any changes that may affect the status of the certificate to RA and CA operators via telephone, email or face to face meeting. The subscribers must request revocation of its certificate as soon as possible, but within one working day after detection of:

4.9.1.1 A certificate is suspected to revocation circumstances in the following

- The subscribers private key is lost or suspected to be compromised.
- The information in the subscribers certificate is suspected to be inaccurate.
- The subscriber violates his/her obligations.
- The CA private key is suspected to be compromised.
- The subscriber leaves his/her organization.
- In case of host/service certificates, the corresponding host/service is retired.

4.9.1.2 A certificate holder can request the revocation of his/her certificates, without any reason.

4.9.2 Who can request revocation

Anybody can request revocation.

4.9.3 Procedure for revocation request

A revocation request can be submitted to a RA and CA operators according to the contact information published on the repository. The RA or CA operators will take appropriate measure to verify the circumstances and to authenticate the identity of the requestor, before taking any action.

4.9.4 Revocation request grace period

- The CA operator will process revocation as soon as it receives the revocation request and the request is approved.
- The revocation information will be published to the on-line repository.
- A revocation notification is sent to the subscriber via email.

4.9.5 Time within which CA must process the revocation request

The CA should process the certificate revocation request within one working day after receiving 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 of the current CRL.

4.9.8 Maximum latency for CRLs (if applicable)

- CRLs must be published in the repository immediately after generation.
- The maximum latency between the generation of CRLs and posting of the CRLs to the repository is 30 minutes.

4.9.9 On-line revocation/status checking availability

NECTEC-GOC CA system does not provide any on-line status checking facility.

4.9.10 On-line revocation checking requirements

NECTEC-GOC CA system does not provide any on-line status checking facility.

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

No stipulation.

4.9.14 Who can request suspension

No stipulation.

4.9.15 Procedure for suspension request

No stipulation.

4.9.16 Limits on suspension period

No stipulation.

4.10 Certificate status services

4.11 End of subscription

If a subscriber of NECTEC-GOC CA ends the subscription to the CA services:

- The subscriber must not use any certificates issued by NECTEC-GOC CA.
- The CA must revoke all certificates issued for the subscriber.

4.12 Key escrow and recovery

No stipulation.

5 FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

5.1 Physical controls

5.1.1 Site location and construction

NECTEC-GOC CA is located safely at National Electronics and Computer Technology Center,Thailand.

5.1.2 Physical access

The room, in which the CA operates are locked during CA operations. The CA machine, a computer notebook, is stored in a safe deposit box. The safe deposit box is protected by a six-digit digital code. The battery used in the safe deposit box will be replaced every 365 days or sooner by NECTEC-GOC CA staff.

5.1.3 Power and air conditioning

The room is supplied with enough electrical power, including automatic emergency power generator for the case of power outage. It also maintains adequate circulation for staff and equipment running by setting of air conditioners.

5.1.4 Water exposures

Due to the location of the NECTEC-GOC CA facilities, floods are not expected.

5.1.5 Fire prevention and protection

The building is fire-resistant and the room is equipped with smoke detectors for fire prevention.

5.1.6 Media storage

NECTEC-GOC CA key and backup copies of CA related information is securely kept in a USB flash drive which is stored in a safe deposit box.

5.1.7 Waste disposal

The CA shall ensure that all media containing sensitive information is sanitized, to remove information such that data recovery is not possible, or destroyed before release for disposal. CA personnel shall account for the destruction of sensitive information.

5.1.8 Off-site backup

No off-site backups are currently performed by NECTEC-GOC CA.

5.2 Procedural controls

5.2.1 Trusted roles

Role	Function
GRID CA PMA	Policy Management Authority
CA Manager	Administrates all tasks on the CA system including the management of CA private key
RA operator	◦ Accepts and verifies application forms ◦ Checks Certificate Signing Request forms ◦ Informs CA to issue certificates
CA operator	◦ Issues certificates ◦ Manages the CA and RA machines ◦ Maintains the CA system ◦ Manages the CA private key

Table 4: Trusted Role and Function of NECTEC-GOC CA

5.2.2 Number of persons required per task

For operation of NECTEC-GOC CA, the numbers of persons required for the roles are:

- CA Manager: 1 person.
- Certificate Authority Operator: 1 person or more for backing-up each other.
- Registration Authority Operator: 1 person or more for each RA site.

5.2.3 Identification and authentication for each role

In NECTEC-GOC CA, on-line and/or off-line system will identify and authenticate the operator.

5.3 Personnel controls

NECTEC-GOC CA will maintain list and perform CA and RA staff audit at least once per year. All access to the servers and applications that comprise the NECTEC-GOC CA is limited to NECTEC-GOC CA staff.

5.3.1 Qualifications, experience, and clearance requirements

The CA shall ensure that all staff performing CA and RA functions possess the necessary knowledge, experience and qualifications to perform their duties.

5.3.2 Background check procedures

CA personnel must be a formal member of National Electronics and Computer Technology Center (NECTEC).

5.3.3 Training requirements

The CA shall ensure that all personnel receive appropriate training. Such training shall address relevant topics such as security requirements, operational responsibilities and associated procedures.

5.3.4 Retraining frequency and requirements

The CA shall review and update its training program at least once a year to accommodate changes in the CA system.

5.3.5 Job rotation frequency and sequence

No stipulation.

5.3.6 Sanctions for unauthorized actions

In the event of actual or suspected unauthorized actions by a person performing duties with respect to the operation of the CA or an RA, the CA shall suspend his or her access to the CA system.

5.3.7 Independent contractor requirements

The CA shall ensure that contract personnel satisfy the same personnel security requirements with respect to appointment, training and background checks as those applicable to CA employees.

5.3.8 Documentation supplied to personnel

The CA shall provide this CP/CPS, relevant provisions of the CPS, as well as any specific statutes, policies or contracts relevant to their positions to CA personnel, RAs and Client Responsible Individuals.

5.4 Audit logging procedures

5.4.1 Types of events recorded

CA system logs

- Operation logs of the CA daemon process
- Error logs for accesses and operations to the CA daemon process

RA system logs

- Access and operation logs to the RA daemon process
- Error logs for accesses and operations to the RA daemon process
- Logs of issued certificates
- All issued CRLs
- The date of issuance of CRLs
- All CSRs and CRRs

Linux system logs

- shutdown/boot/reboot logs of the CA and the RA machine
- login/logout logs of the CA and the RA machine
- other logs archived by Linux operation of the CA and the RA machine
  (secure/cronlog/maillog/messages/syslog/errorlog)

Logs of physical access to the CA machine

- Paper sheets which record all events about the access to the CA machine. The event information includes the name of CA operator, date and time of entering/leaving the CA room, and the purpose of the access to the machine.
- Access logs of the CA machine are recorded by the CA operator.

Emails All emails received by the NECTEC-GOC RA and CA regarding.

- Application
- Technical support request and response will be logged.

Other documents

- A list of email addresses of end entities
- All issued certificates
- The application form and photo ID of the applicant are archived in a safe deposit box. In case of repeated identity vetting via face to face meeting, the CA operator sends back the initial copy to the RA operator.
- Official documents if they are used for identification of entities
- All versions of the CP/CPS
- All Audit reports

5.4.2 Frequency of processing log

The CA shall ensure that all significant events are explained in an audit log summary and that CA personnel review audit logs quarterly. Such reviews involve verifying that the log has not been tampered with, and the inspecting all log entries.

5.4.3 Retention period for audit log

The minimum retention period is three years.

5.4.4 Protection of audit log

The archive is stored in a safe deposit box in the NECTEC server room. This safe deposit box is accessible to the NECTEC-GOC CA system administrator, only. The machine room security is described in section 5.1.

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

Records of all the types of events listed in section 5.4.1 are archived.

5.5.2 Retention period for archive

Certificates and CRLs generated by the CA, must be retained for at least 2 years after their expirations, and the minimum retention period is 3 years. The subscriber identity information will be retained for 5 years.

5.5.3 Protection of archive

System logs and email archives are protected by the authorization mechanism provided by Unix operating system. Only the owners of the system logs are able to modify the logs. System logs and email archives are periodically back up to offline media e.g., USB flash drive or CD/DVD, which is stored in the safe deposit box.

5.5.4 Archive backup procedures

A second copy of all materials retained or backed up must be stored in readonly media like CD/DVD. 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

All archived logs and documents are 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

When the CA's cryptographic data needs to be changed (e.g. CA key expiration), from the time of distribution of new cryptographic data, only the new CA certificate will be used for certificate signing purposes.

- From that time, the old CA certificate will not be used for certificate signing purposes.
- The overlap of the old and new CA certificate must be at least the longest time an end-entity certificate can be valid (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.

5.7 Compromise and disaster recovery

In the event of CA private key compromise, all certificates will be revoked, and the CA removed from service. In the event of disaster, the CA will be restored to full function from backups. If the backups are destroyed as well, the existing certificates can keep functioning until CRLs expire, but no new certificates can be issued, and therefore the CA must be replaced.

5.8 CA or RA termination

Before NECTEC-GOC CA terminates its services it will:

- Make publicly available information of its termination.
- Stop issuing certificates and CRL.
- Destroy its private key and all copies.

6 TECHNICAL SECURITY CONTROLS

6.1 Key pair generation and installation

6.1.1 Key pair generation

- The CA key pair is generated by the CA operator on the signing machine which is not connected to any kind of network.
- End entities cryptographic keys are locally generated by the Globus certificate request tools, or OpenSSL tools during the requesting process.
- NECTEC-GOC CA does not generate private keys for end entities.

6.1.2 Private key delivery to subscriber

The NECTEC-GOC CA does not generate end entities private keys hence does not deliver private keys.

6.1.3 Public key delivery to certificate issuer

End entities will send its public key included in CSR at the time of certificate signing request.

6.1.4 CA public key delivery to relying parties

CA certificate will be published on the NECTEC-GOC CA web repository.

6.1.5 Key sizes

- The minimum key length for the user or host/service certificate is 1024 bits.
- The CA key length is 2048 bits.

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)

NECTEC-GOC CA private key is the only key used for signing CRLs and Certificates for subscribers, host and services. The Certificate key Usage field must be used in accordance with the "Internet X.509 Public Key Infrastructure Certificate and CRL profile" [RFC 2459].

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic module standards and controls

NECTEC-GOC CA do not use any hardware security module.

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

In NECTEC-GOC CA system, (n out of m) multi-person control is not supported. The passphrase for accessing to CA's private key is known to 2 persons, namely, the CA manager and the CA operator .

6.2.3 Private key escrow

Not supported.

6.2.4 Private key backup

The NECTEC-GOC CA private key backup is performed by the CA operator and the backup key is kept encrypted in a USB flash drive which is stored in the safe deposit box described in section 5.1.2.

6.2.5 Private key archival

See section 5.5.

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

See section 6.4.

6.2.9 Method of deactivating private key

No stipulation.

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 retains all public key certificates it generated.

6.3.2 Certificate operational periods and key pair usage periods

- The lifetime of NECTEC-GOC CA certificate is 10 years.
- The lifetime of user certificate is 13 months.
- The lifetime of host certificate is 13 months.

6.4 Activation data

- The NECTEC-GOC CA's private key is protected by a pass phrase over 15 characters.
- A copy of pass phrase is kept in a sealed envelop, which is kept in a safe place where access is controlled.
- The sealed envelop is kept separated from the private key.

6.5 Computer security controls

6.5.1 Specific computer security technical requirements

- The CA machine operating systems are maintained at a high level of security by applying all the relevant patches.
- Both CA and RA machine are dedicated machines used for the specified purposes, only.

6.5.2 Computer security rating

No stipulation.

6.6 Life cycle technical controls

No stipulation.

6.7 Life cycle security controls

No stipulation.

6.8 Network security controls

- The CA machine is a dedicated machine and is completely offline.
- The RA machine is protected by a firewall.
- The RA machine is a dedicated machine and no network service other than RA web server runs on it.
- Appropriate software upgrade/patch of the RA machine is performed immediately, when security vunerability has been reported and such upgrade/patch is available.

6.9 Time-stamping

No stipulation.

7 CERTIFICATE, CRL, AND OCSP PROFILES

7.1 Certificate profile

7.1.1 Version number(s)

X.509 v3.

7.1.2 Certificate extensions

CA Certificate:

- X509v3 Basic Contraints: critical, CA:TRUE
- X509v3 Key Usage: critical, digitalSignature, crlSign, keyCertSign
- X509v3 Subject Key Identifier: [the unique key ID]
- X509v3 Authority Key Identifier: keyid

User Certificates:

- X509v3 Basic Contraints: critical, CA:FALSE
- X509v3 Key Usage: critical, nonRepudiation, digitalSignature, keyEncipherment, dataEncipherment
- X509v3 Extended Key Usage: clientAuth
- X509v3 Issuer Alternative Name: email:camanager@hpcc.nectec.or.th
- X509v3 CRL Distribution Points: URI:http://gridca.hpcc.nectec.or.th/pub/crl/cacrl.crl
- X509v3 Subject Alternative Name: email: <user email address>
- CertificatePolicies: policyIdentifier: 1.3.6.1.4.1.25149.1.1.1.1.2, policyIdentifier: 1.2.840.113612.5.2.2.1 , CPS: <URI of the NECTEC-GOC CA CP/CPS>

Host Certificates:

- X509v3 Basic Contraints: critical, CA:FALSE
- X509v3 Key Usage: critical, digitalSignature, keyEncipherment, dataEncipherment
- X509v3 Extended Key Usage: serverAuth
- X509v3 Issuer Alternative Name: email:camanager@hpcc.nectec.or.th
- X509v3 CRL Distribution Points: URI:http://gridca.hpcc.nectec.or.th/pub/crl/cacrl.crl
- X509v3 Subject Alternative Name: DNS:<FQDN of the host>, email: <user email address>
- CertificatePolicies: policyIdentifier: 1.3.6.1.4.1.25149.1.1.1.1.2, policyIdentifier: 1.2.840.113612.5.2.2.1 , CPS: <URI of the NECTEC-GOC CA CP/CPS>

7.1.3 Algorithm object identifiers

CA Certificate:

- Signature Algorithm: sha1WithRSAEncryption (2048 bits)

User and Host Certificates:

- Signature Algorithm: sha256WithRSAEncryption (1024 bits)

7.1.4 Name forms

Issuer: C=TH, O=NECTEC, OU=GOC, CN=NECTEC GOC CA

User DN: C=TH, O=NECTEC, OU=GOC, CN=[the name of applicant]

Host DN: C=TH, O=NECTEC, OU=GOC, CN=[FQDN of the hostname]

7.1.5 Name constraints

Subject DN can contain the following characters:

- Alphabetic character: a-z, A-Z
- Numerical character: 0-9
- Special character: -(dash), _ (underscore)

7.1.6 Certificate policy object identifier

See in section 1.2.

7.1.7 Usage of Policy Constraints extension

No stipulation.

7.1.8 Policy qualifiers syntax and semantics

No stipulation.

7.1.9 Processing semantics for the critical Certificate Policies extension

No stipulation.

7.2 CRL profile

CRLs are signed by the NECTEC-GOC CA private key and are published in the NECTEC-GOC CA web repository.

7.2.1 Version number(s)

X.509 v2.

7.2.2 CRL and CRL entry extensions

Message digest algorithm of the CRL: sha256WithRSAEncryption.

7.3 OCSP profile

7.3.1 Version number(s)

No stipulation.

7.3.2 OCSP extensions

No stipulation.

8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS

8.1 Frequency or circumstances of assessment

The NECTEC-GOC CA will accept external Compliance Audit. In addition, the NECTEC-GOC CA performs operational self-assessment of CA/RA staff at least once per year.

8.2 Identity/qualifications of assessor

NECTEC-GOC CA can be audited by personnel from institutes, which are members of APGrid PMA.

8.3 Assessor's relationship to assessed entity

NECTEC-GOC CA can be audited by the APGrid PMA.

8.4 Topics covered by assessment

Audit items will be selected based on the minimum CA requirements and documents enacted by the APGrid PMA.

8.5 Actions taken as a result of deficiency

NECTEC-GOC CA has the responsibility for the action taken as a result of deficiency. When NECTEC-GOC CA receives an audit report from the auditor, it will send a report on actions to the auditor within two weeks. The report must describe actions taken as a result of deficiency and their timetable.

8.6 Communication of results

The result of the audit will be made available to APGrid PMA in which the NECTEC-GOC CA participates. NECTEC-GOC CA may make the results of the audit publicly available.

9 OTHER BUSINESS AND LEGAL MATTERS

9.1 Fees

No fees are charged for any service provided by NECTEC-GOC CA.

9.2 Financial responsibility

No stipulation.

9.3 Confidentiality of business information

- NECTEC-GOC CA collects subscriber's full names and email addresses. Some of this information is used to construct unique, meaningful subject names in the issued certificates.
- Information included in issued certificates and CRLs is not considered confidential.
- NECTEC-GOC CA does not collect any kind of confidential information.
- The key pairs are generated and managed by the subscribers and are the sole responsibility of the subscribers.

9.4 Privacy of personal information

The subscriber's private information collected for registration are:

- Name of subscriber
- ID CARD number
- Country
- Organization Name

- Position
- Telephone
- Email

We do not provide this information to other organizations.

9.5 Intellectual property rights

All certificate related data issued by NECTEC-GOC 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

- NECTEC-GOC CA makes no guarantee about the security or suitability of service that is identified by a NECTEC-GOC CA certificate.
- The certification service is run with a reasonable level of security, but it is provided on a best effort, only, basis.
- It does not warrant its procedures and it will take no responsibility for problems arising from its operations, or for the use of the certificates it provides.

9.9 Indemnities

No stipulation.

9.10 Term and termination

9.10.1 Term

This CP/CPS is valid as long as it is published on the web repository and the old version of CP/CPS has been removed.

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 accreditated.

9.10.3 Effect of termination and survival

No stipulation.

9.11 Individual notices and communications with participants

No stipulation.

9.12 Amendments

- Users will not be warned in advance of changes to the NECTEC-GOC CA's CP/CPS.
- Minor editorial changes to this document can be made without approval by the APGridPMA.
- Major changes such as changes in policy or technical security controls need to be approved by the APGrid PMA. New OID will be assigned to the revised document for such major changes.
- For minor editorial changes, revision to this document will be announced on the NECTEC-GOC CA repository. Substantial changes will be notified by Emails to all relevant relying parties, all cross-certifying CAs, and the PMAs in which the NECTEC-GOC CA participates.

9.13 Dispute resolution provisions

No stipulation.

9.14 Governing law

No stipulation.

9.15 Compliance with applicable law

No stipulation.

9.16 Miscellaneous provisions

No stipulation.

9.17 Other provisions

No stipulation.

10 Bibliography

1. Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile. http://www.ietf.org/rfc/rfc3280.txt
2. Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework. http://www.ietf.org/rfc/rfc3647.txt
3. Korea Institute of Science and Technology Information (KISTI) Certificate Policy and Certification Practice Statement,OID: 1.3.6.1.4.1.14305.1.1.1.2.0, Version 2.0, July 2007.