

# NECTEC-GOC PKI Service

## Certificate Policy and Certificate Practice Statement

Ver. 1.0  
October, 2006



National Electronics and Computer Technology Center, Thailand

# Contents

<b>1</b>	<b>Introduction</b>	<b>5</b>
1.1	Overview	5
1.1.1	Type of Certificates	5
1.1.2	Related specification	5
1.2	Identification	5
1.3	Community and Applicability	5
1.3.1	Organization	5
1.3.2	End Entities	6
1.3.3	Applicability	7
1.4	Contact details	7
1.4.1	Specification administration organization	7
1.4.2	Contact information	7
1.4.3	Person determining CPS suitability for the policy	7
<b>2</b>	<b>General Provisions</b>	<b>7</b>
2.1	Obligations	7
2.1.1	CA Obligations	7
2.1.2	RA Obligations	8
2.1.3	RA Obligations Procedures	8
2.1.4	Subscriber Obligations	9
2.1.5	Relying Party Obligations	9
2.1.6	Repository Obligations	9
2.2	Liability	9
2.2.1	CA liability	9
2.2.2	RA liability	10
2.2.3	Certificate Users and host administrators liability	10
2.2.4	Relaying party liability	10
2.2.5	Repository liability	10
2.3	Financial responsibility	10
2.4	Interpretation and Enforcement	10
2.5	Fees	10
2.6	Publication and repository	10
2.6.1	Publication	10
2.6.2	Frequency of Publication	11
2.6.3	Access Controls	11
2.6.4	Repositories	11
2.7	Compliance Audit	11
2.8	Confidentiality	11
2.9	Intellectual Property Rights	11
<b>3</b>	<b>Identification and Authentication</b>	<b>11</b>
3.1	Initial Registration	11
3.1.1	Types of Names	11
3.1.2	Name Meanings	12
3.1.3	Rules for Interpreting Various Name Forms	12
3.1.4	Uniqueness of Names	12
3.1.5	Name Claim Dispute Resolution Procedure	12
3.1.6	Recognition, Authentication, and Role of Trademarks	12
3.1.7	Method to Prove Possession of Private Key	12
3.1.8	Authentication of Organization Identity	12
3.1.9	Authentication of Individual Identity	12
3.2	Routine Rekey	12
3.3	Rekey After Revocation	13

3.4	Revocation Request . . . . .	13
<b>4</b>	<b>Operational Requirements</b>	<b>13</b>
4.1	RA Operator Establishment . . . . .	13
4.2	Certificate Application . . . . .	13
4.3	Certificate Issuance . . . . .	13
4.4	Certificate Acceptance . . . . .	13
4.5	Certificate Suspension and Revocation . . . . .	13
4.5.1	Circumstances for Revocation . . . . .	13
4.5.2	Who Can Request Revocation . . . . .	14
4.5.3	Procedure for Revocation Request . . . . .	14
4.5.4	Revocation Request Grace Period . . . . .	14
4.5.5	Circumstances for Suspension . . . . .	14
4.5.6	Who Can Request Suspension . . . . .	14
4.5.7	Procedure for Suspension Request . . . . .	14
4.5.8	Limits on Suspension Period . . . . .	14
4.5.9	CRL Issuance Frequency . . . . .	14
4.5.10	CRL Checking Requirements for Relying Parties . . . . .	14
4.5.11	Online Revocation/Status Checking Availability . . . . .	14
4.5.12	Online Revocation Checking Requirements . . . . .	14
4.5.13	Other Forms of Revocation Advertisement Available . . . . .	15
4.5.14	Checking requirements for other forms of revocation advertisements . . . . .	15
4.6	Security Audit Procedures . . . . .	15
4.7	Records Archival . . . . .	15
4.7.1	Types of Event Audited . . . . .	15
4.7.2	Retention Period for Audit Logs . . . . .	16
4.7.3	Protection of Archive . . . . .	16
4.7.4	Time-Stamping Requirements . . . . .	16
4.7.5	Archive Collection System . . . . .	16
4.7.6	Procedures to Obtain and Verify Archive Information . . . . .	16
4.8	Key Changeover . . . . .	16
4.8.1	User certificate validity date . . . . .	16
4.8.2	CA certificate validity . . . . .	17
4.9	Compromise and Disaster Recovery . . . . .	17
4.10	CA Termination . . . . .	17
<b>5</b>	<b>Physical, Procedural and Personnel Security Controls</b>	<b>17</b>
5.1	Physical Security Controls . . . . .	17
5.1.1	Site Location . . . . .	17
5.1.2	Physical Access . . . . .	17
5.1.3	Power and Air Conditioning . . . . .	17
5.1.4	Water Exposure . . . . .	17
5.1.5	Fire Prevention and Protection . . . . .	17
5.1.6	Media Storage . . . . .	18
5.1.7	Waste Disposal . . . . .	18
5.1.8	Off-site Backup . . . . .	18
5.2	Procedural Controls . . . . .	18
5.2.1	Trusted Roles . . . . .	18
5.3	Personnel Security Controls . . . . .	18
5.3.1	Background Checks and Clearance . . . . .	18
5.3.2	Background Checks and Security . . . . .	18
5.3.3	Training Requirements and Procedures . . . . .	18
5.3.4	Training Period and Retraining Procedures . . . . .	18
5.3.5	Frequency and Sequence of Job Rotation . . . . .	18
5.3.6	Sanctions Against Personnel . . . . .	18

5.3.7	Controls on Contracting Personnel . . . . .	18
5.3.8	Documentation Supplied to Personnel . . . . .	19
<b>6</b>	<b>Technical Security Controls</b>	<b>19</b>
6.1	Key Pair Generation and Installation . . . . .	19
6.1.1	Key Pair Generation . . . . .	19
6.1.2	Public Key Delivery to Certificate . . . . .	19
6.1.3	CA Public Key Delivery to Users . . . . .	19
6.1.4	Key Sizes Personal . . . . .	19
6.1.5	Public Key Parameters Generation . . . . .	19
6.1.6	Parameter Quality Checking . . . . .	19
6.1.7	Hardware/Software Key Generation . . . . .	19
6.1.8	End User Key Protection . . . . .	19
6.1.9	Key Usage Purposes . . . . .	19
6.2	Private Key Protection . . . . .	20
6.2.1	Standards for cryptographic module . . . . .	20
6.2.2	Private Key (n out of m) Multi-person Control . . . . .	20
6.2.3	Private Key Escrow . . . . .	20
6.2.4	Private Key Archival and Backup . . . . .	20
6.3	Other Aspects of Key Pair Management . . . . .	20
6.4	Activation Data . . . . .	20
6.5	Computer Security Controls . . . . .	20
6.5.1	Specific Computer Security Technical Requirements . . . . .	20
6.5.2	Computer Security Rating . . . . .	20
6.6	Life-Cycle Security Controls . . . . .	20
6.7	Network Security Controls . . . . .	20
6.8	Cryptographic Module Engineering Controls . . . . .	20
<b>7</b>	<b>Certificate and CRL Profiles</b>	<b>21</b>
7.1	Certificate Profile . . . . .	21
7.2	CRL Profile . . . . .	21
<b>8</b>	<b>Specification Administration</b>	<b>21</b>
8.1	Specification Change Procedures . . . . .	21
8.2	Publication and Notification Procedures . . . . .	21
8.3	CPS Approval Procedures . . . . .	21
	<b>Glossary</b>	<b>22</b>
	<b>Bibliography</b>	<b>24</b>

# 1 Introduction

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 RFC2527 [RFC2527], this document describes policy and practices of NECTEC-GOC PKI services. Not all sections of RFC2527 are used. Sections that are not included have a default value of No stipulation. This document describes the set of rules and procedures established by the NECTEC-GOC CA Policy management Authority for the operations of the NECTEC-GOC PKI service.

## 1.1 Overview

This document will include both the Certificate Policy and the Certification Practices Statement for the NECTEC-GOC CA. It is the intent of the NECTEC-GOC PKI to issue Identity and server certificates for use in Grids. These certificates are for NECTEC researchers and their colleagues. These certificates will be compatible with the Globus middleware that are used on these Grids. The NECTEC-GOC PKI is based on OpenCA Certificate Management System

### 1.1.1 Type of Certificates

NECTEC-GOC CA issues following types of certificates.

- Clients for identification
- Globus server

### 1.1.2 Related specification

None

## 1.2 Identification

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

Object	OID
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
Certification Practices Statements (CPS)	1.3.6.1.4.1.25149.1.1.1.X*
CA Certificate Policy	1.3.6.1.4.1.25149.1.1.2
Globus Server CP	1.3.6.1.4.1.25149.1.1.2.1.1
Globus Clients CP	1.3.6.1.4.1.25149.1.1.2.2.1

**Note:** \*X is for each major CPS version

Table 1-1 OIDs

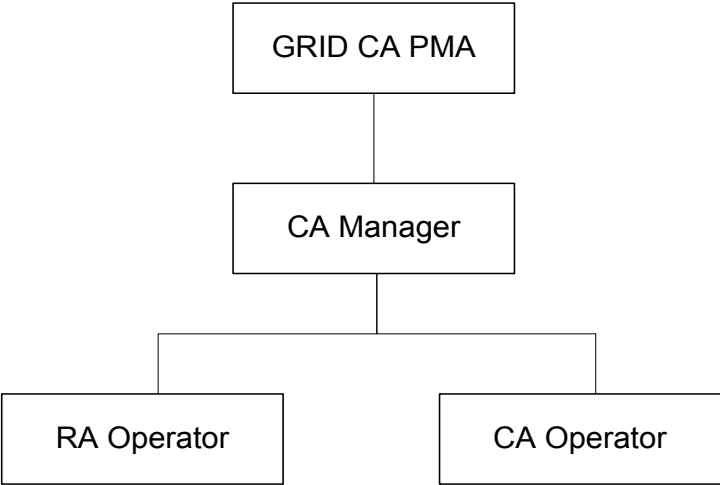
## 1.3 Community and Applicability

### 1.3.1 Organization

#### 1. Policy Management Authority

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

- Draft and approve CP/CPS,
  - Take countermeasure for compromise of the Certificate Authority(CA)'s private key,
  - Take countermeasure in emergencies,
  - Other important matters.
2. Operating Organization Figure 1-1 and Table 1-2 show organization and system configuration of the CA



**Figure 1-1 Organization and System Configuration**

<b>Role</b>	<b>Function</b>
GRID CA PMA	Policy Management Authority
CA Manager	Administrates all tasks on the CA system including the CA private key
RA Operator	<ul style="list-style-type: none"> <li>○ Accepts and verifies User Application form</li> <li>○ Checks Certificate Signing Request form</li> <li>○ Informs CA to issue certificate</li> </ul>
CA Operator	<ul style="list-style-type: none"> <li>○ Issues certificates</li> <li>○ Manages CA and RA servers</li> <li>○ Maintains the CA system</li> <li>○ Manages CA private key</li> </ul>

**Table 1-2 Organization of operating CA and roles**

**1.3.2 End Entities**

NECTEC-GOC CA issues certificates for the following subjects:

- Users of NECTEC.
- Users of domestic Grid-based Application/Projects.
- Collaborators related to NECTEC Grid Computing research.

### 1.3.3 Applicability

It is assumed that certificates issued by NECTEC-GOC CA have to be used in the following purposes and must not be used for any other purposes.

Type		Purpose
Client certificates		Client authentication under the Grid Computing environments (SSL)
Server certificates	Globus Server	Globus server authentication

Table 1-3 Certificates and its purpose

## 1.4 Contact details

### 1.4.1 Specification administration organization

The NECTEC GRID PMA has responsibility for administrating the NECTEC-GOC PKI services.

### 1.4.2 Contact information

Dr. Sornthep Vannarat and Mr. Suriya U-ruekolan  
National Electronics and Computer Technology Center  
Grid Operation Center  
112 Paholyotin Rd., Klong 1, Klong Luang, Pathumthani 12120, Thailand  
Tel: (662) 564-6900 ext 2278 Fax: (662) 564-6772  
Email: camanager@hpcc.nectec.or.th

### 1.4.3 Person determining CPS suitability for the policy

The NECTEC GRID PMA has responsibility for determining CPS suitability for the policy.

## 2 General Provisions

### 2.1 Obligations

#### 2.1.1 CA Obligations

- Accept certification requests from RA
- Notify the RA of certification request and accept authentication results from the RA
- Issue certificates based on the enrollment information forwarded from the RA
- Notify the subscriber of the issuing of the certificate
- Revoke the certificate based on the request forwarded from the RA
- Issue a Certificate Revocation List (CRL) timeliness [CPS 2.6.2 and 4.5.9]
- Authenticate entities requesting the revocation of a certificate, possibly by delegating this task to the RA
- Publish client certificate information and a CRL except in time of temporary suspension such as system maintenance or in other emergency case
- Identify which CP/CPS is used to issue certificates
- Keep audit logs of the certificate issuance process
- Always use a secure method, to communicate with RA Operator, such as signed and encrypted Email or face-to-face meeting

### 2.1.2 RA Obligations

- Ensure that reasonable care is taken to meet the requirements of this CPS
- Authorise applications only after a face to face meeting with applicant, only after the applicant has displayed appropriate photo ID and only after RA is reasonably sure that the applicant is an appropriate person to have a NECTEC-GOC certificate.
- Keep suitable records of applicant meetings
- Assist users with lodging applications and collecting certificates if necessary
- Accept authenticate requests from the NECTEC-GOC CA
- Validate the certificate request
- Notify the NECTEC-GOC CA when authentication is completed for a certification or revocation request
- Accept revocation requests
- Notify the NECTEC-GOC CA of all signing requests and revocation requests
- Will not approve a certificate with a lifetime greater than NECTEC-GOC CA lifetime
- Export the CSRs and CRRs
- Import the certificates and CRLs
- Keep audit logs of the certificate registration process
- Always use a secure method, to communicate with CA Operator, such as signed and encrypted Email or face-to-face meeting

### 2.1.3 RA Obligations Procedures

RA Operator are required to check the photo ID, in person, of a applicant before approving a request. The procedures for approval are:

1. The applicant meets the RA Operator at an agreed upon time in person, and presents the RA Operator with the serial number of his/her request, and photo ID to prove his/her identity.
2. The RA Operator logs in to the RA website at <https://gridca.hpcc.nectec.or.th/ra>, 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.
3. The RA Operator checks that the applicant's name is identical to the name on the certificate, and that his/her photo ID is valid.
4. The RA Operator may also choose to ask the applicant to verify their PIN via the "verify PIN" button at the bottom of the page.
5. The RA Operator then checks that the certificate lifetime is no more than 13 months (or n/a, which is effectively the same), and that the organization unit field is correct for the user RA Operator List. If these or anything else are incorrect on the application, the RA Operator can correct them.
6. If the RA Operator is satisfied with the application, then an appropriate certificate will be generated, otherwise the RA Operator must reject application.
7. The approved request will then be signed by the Certificate Authority, this is generally done at the end of each business day. The user should then follow the instructions on the NECTEC-GOC CA website for collecting his/her certificate. The RA Operator isn't required to do anything further.

## Note

1. RA Operator may not nominate a substitute or ‘stand in’ RA Operator to perform their duty in the their absense. If necessary, another person can be appointed an RA Operator (subject to normal RA Operator appointment process) and act in their own right.
2. RA Operator must meet, face to face, in person with the applicant. Phone calls, video conferences, Access Grid Sessions are not appropriate approval forums.
3. RA Operator must always err on the safe side, that is, if there is any doubt about an approval process it must be rejected.
4. Occasionally the restrictions placed on the approval process will cause unwelcome delays in processing a certificate application. This cannot be avoided.

### 2.1.4 Subscriber Obligations

- Acknowledge, read and adhere to the rules, policies and limitations as per the CPS.
- Not falsify personal information
- Protect private key in the manner described in [CPS 6.1.8].
- Notify NECTEC-GOC CA staff if the private key is suspected of compromise.

### 2.1.5 Relying Party Obligations

- To allow use of certificates for only the purposes that they are issued for.
- To collect and observe revocation and suspension lists.
- Acknowledgment of liability caps and limitations.

### 2.1.6 Repository Obligations

- To publish certificates, revocation and suspension lists in a timely manner.
- To ensure appropriate records are retained as described elsewhere in this document.
- The NECTEC-GOC PKI repository will run on a best-effort basis, with an intended availability of 24x7.

## 2.2 Liability

### 2.2.1 CA liability

NECTEC-GOC CA has liability:

- To perform practices on the procedures based on this document and have authenticity for issued certificates. NECTEC-GOC CA does not have liability for modification of certificates by the malicious person or compromise of signature algorithm such as discovery attack.
- To perform practices based on this document adequately so that the private key is not compromised by theft or lost.
- The certification service is run with a reasonable level of security, but it is provided on a best-effort basis. It does not warrant its procedures and it will take no responsibility for problems arising from its operation, or for the use made of the certificates it provides.
- No financial liability with respect to use or management of any issued certificates.

### **2.2.2 RA liability**

NECTEC-GOC RA has a liability:

- To perform practices based on the document to protect unauthorized access or modification to confidential information contained in enrollment requests.
- Take restrict precautions to prevent any loss, disclosure or unauthorized access the subscriber's individual information.

### **2.2.3 Certificate Users and host administrators liability**

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

### **2.2.4 Relaying party liability**

No Stipulation

### **2.2.5 Repository liability**

NECTEC-GOC PKI repository has a liability

- To response to retrieve requests within operating time defined in this document.
- Not to have a liability that the stored CRL is not the newest one at the time of the retrieval request.

## **2.3 Financial responsibility**

No Stipulation.

## **2.4 Interpretation and Enforcement**

No Stipulation.

## **2.5 Fees**

No Stipulation

## **2.6 Publication and repository**

### **2.6.1 Publication**

Following information will be published on the NECTEC-GOC PKI repository operated by NECTEC-GOC

- Client certificate information used for Grid map file
- A CRL issued by NECTEC-GOC CA
- The CAs certificate
- The CAs certificates fingerprint
- The CAs signing policy file
- A copy of this policy

- The current CPS document and a list of suggested organization names.
- Other information deemed relevant to the NECTEC-GOC PKI

### **2.6.2 Frequency of Publication**

All certificates and related data is available publicly on the NECTEC-GOC website shortly after it is created, or added. Certificate Revocation Lists will be published every 30 days, with a buffer of 7 days before the expiry of the previous CRL [CPS 4.5.9]. A new CRL must be issued immediately after a revocation.

### **2.6.3 Access Controls**

Access to the web interface is free to anyone. Access to the RA interface is limited via X.509 based login to users with the role of RA Operator. Access to the CA machine and interface is physically restricted to the CA operator. The online components of the Authority are available 24x7 on a best effort basis.

### **2.6.4 Repositories**

Information specified in this document [CPS 2.6.1] is stored in the NECTEC-GOC PKI repository and accessible from ThaiSarn network.

## **2.7 Compliance Audit**

The CA will undergo an internal audit from time to time to ensure compliance with this document and general security rules. The CA expects to be audited, probably annually, by representatives of the APGrid PMA.

## **2.8 Confidentiality**

No personal information will be publicly available, other than names. Other information, such as phone numbers, email addresses and physical addresses will be stored privately, and will only be accessible to RA Operators and CA Operators for use in contacting end users about certificate status.

## **2.9 Intellectual Property Rights**

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

# **3 Identification and Authentication**

## **3.1 Initial Registration**

### **3.1.1 Types of Names**

The subject name is an X.500 Distinguished Name, it may be one of the following :

- Person - must include the organization name and the name of the subject that closely relates to the name that person generally uses.
- Host - Must include the fully qualified domain name of the host.

### 3.1.2 Name Meanings

Table 3-1 shows attribute values for name. Common Name is decided based on the data specified in the enrollment information.

Attributes	Meaning	Value
commonName	User name(clients certificate)	
	Host name(server certificate)	host/FQDN
organizationUnitname		GOC
organizationName		NECTEC
CountryName	Country name	TH

**Table 3-1 Attributes used in the certificate**

### 3.1.3 Rules for Interpreting Various Name Forms

Identification will be according to the rule in the previous section [CPS 3.1.2]

### 3.1.4 Uniqueness of Names

Distinguished Names must be unique. User cannot have the same common name. Host will always have different fully qualified domain names. OpenCA prevents the issuing of a certificates if the DN will clash with an existing valid certificate. Certificates must apply to unique individuals or resources. Users must not share certificates.

### 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

There is no requirement for users to prove possession of private keys, it is implicit in the Grid system.

### 3.1.8 Authentication of Organization Identity

All Certificates issued must be associated with an organization that is, in turn, associated with the NECTEC Grid Project. For this purpose, only organizations personally known to be associated with the NECTEC Grid by the CA Manager and / or the RA Operator will be considered. See [CPS 4.1] "RA Operator Establishment"

### 3.1.9 Authentication of Individual Identity

Certificates will be issued only to members of the NECTEC Grid project or people associated in some way with the NECTEC Grid project, subject to the CA Manager's approval. The process used to establish an individual's identity and their appropriateness to have a certificate is detailed in [CPS 2.1.2].

## 3.2 Routine Rekey

Rekey (or renewal) before expiration can be accomplished by sending a rekey request based on a new public key. The NECTEC-GOC CA will send renewal reminders at least a month before expiration. Rekey after expiration follows the same authentication procedure as a new certificate.

### **3.3 Rekey After Revocation**

This procedure is the same as for requesting a new certificate.

### **3.4 Revocation Request**

End entities must submit a revocation request to RA Operator via email and signed with a valid and trusted certificate. Revocation request is confirmed that user and organization is authenticated by certificates issued based on this CPS.

## **4 Operational Requirements**

### **4.1 RA Operator Establishment**

NECTEC-GOC CA Manager appoints a person at each participating institute or physical location to accept the role of an RA Operator. This person is personally known to the Manager or is personally introduced to him by another person who personally knows the potential RA Operator and is trusted by the Manager. Once the potential RA Operator's identity is established and an appropriate personal certificate is issued, the RA Operator is permitted to vouch for people at his/her institute or physical location. When an RA Operator countersigns a certificate application, it is done over a HTTPS connection using the RA Operator own certificate enabled browser. A RA Operator cannot countersign an application using another person's browser. The procedures to be followed by a RA Operator are listed in [CPS 2.1.2] RA Operator obligations. A written agreement with each RA Operator stating that they will follow those procedures must be made.

### **4.2 Certificate Application**

Grid users will generate a certificate signing request on a system under their own control using either the Globus certificate request tools, or OpenSSL tools. The request is uploaded over https to the OpenCA web interface. Once the request is submitted, their identity will be verified by face to face meeting with a RA Operator, who will verify them using photo ID, and take a record of their request approval. The RA Operator will then electronically counter sign the application over a secure connection.

### **4.3 Certificate Issuance**

Approved certificate requests will be signed at the end of each business day, and the signed certificates will be made available online shortly afterwards. Emails will be sent to new certificate holders, if they have supplied an email address.

### **4.4 Certificate Acceptance**

NECTEC-GOC CA does not confirm acceptance before publishing new certificates. If its necessary to reject a certificate application, the responsible administrator will advise the unsuccessful candidate and will, wherever possible, advise them of the reason as to why the application was rejected.

### **4.5 Certificate Suspension and Revocation**

#### **4.5.1 Circumstances for Revocation**

A certificate will be revoked when the information it contains is suspected to be incorrect or compromised.

- 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.

- CA private key is suspected to be compromised.
- The subscriber leaves his/her organization.

#### **4.5.2 Who Can Request Revocation**

Any certificate holder, the NECTEC-GOC CA Manager and NECTEC-GOC RA can request revocation.

#### **4.5.3 Procedure for Revocation Request**

A certificate revocation can be requested as outlined in [CPS 3.4]. In case of the RA can independently confirm that the certificate has been compromised or misused, the RA notify the CA to revoke the certificate, even if the request comes from an unauthenticated source and/or the holder of the certificate is unreachable. In case of the revocation request is signed by the owners certificate, the RA can authenticate the request and notify the CA to revoke the certificate. In all other cases the RA should authenticate the revocation request and try to contact the subscriber by the phone or email before revoking the certificate. If the revoked certificate is a CA certificate the CA shall inform the subscribers and cross-certifying CAs in addition and shall terminate the certificate and CRLs distribution service for certificates/CRLs which have been issued using the compromised private key..

#### **4.5.4 Revocation Request Grace Period**

There is no explicit grace period, although the revoked certificate may continue to work on any particular server up until the next certificate revocation list is activated.

#### **4.5.5 Circumstances for Suspension**

No Stipulation.

#### **4.5.6 Who Can Request Suspension**

No Stipulation.

#### **4.5.7 Procedure for Suspension Request**

No Stipulation.

#### **4.5.8 Limits on Suspension Period**

No Stipulation.

#### **4.5.9 CRL Issuance Frequency**

Certificate Revocation Lists will be published every 30 days, with a buffer of 7 days before the expiry of the previous CRL [CPS 2.6.2].

#### **4.5.10 CRL Checking Requirements for Relying Parties**

Servers relying on NECTEC-GOC CA Certificates are required to update their CRL every day or more frequently.

#### **4.5.11 Online Revocation/Status Checking Availability**

No stipulation.

#### **4.5.12 Online Revocation Checking Requirements**

No stipulation.

#### **4.5.13 Other Forms of Revocation Advertisement Available**

No stipulation.

#### **4.5.14 Checking requirements for other forms of revocation advertisements**

No stipulation.

### **4.6 Security Audit Procedures**

A person within the NECTEC-GOC system team but not a CA Operator is appointed to watch the Online machine's security logs and to advise when its necessary to update security sensitive components. Access to the security logs is granted to this person in a way that does not allow them control of OpenCA itself. The CA expects to be audited as per [CPS 2.7].

### **4.7 Records Archival**

All records will be backed up to CD or DVD every month as part of the backup process. The entire image of the machine will be backed up including the databases. No separate backup of individual records takes place. As a log rotate system will eventually flush interesting records (such as boot and shutdown messages) one backup CD or DVD will be retained for each month indefinitely. This means that three and sometimes four CDs or DVDs may be discarded each month (to prevent the archive becoming too large), these disks must be physically destroyed.

#### **4.7.1 Types of Event Audited**

The following events will be logged:

##### **CA system logs**

- Access and operation logs to the CA daemon process
- Error logs for accesses and operations to the CA daemon process
- Operation logs of 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 machine and the RA server
- login/logout logs of the CA and the RA server
- other logs archived by Linux operation of the CA and the RA server  
( secure/cronlog/maillog/messages/syslog/errorlog )

### Logs of physical access to the CA machines

- Paper sheets which record all events about the access to the CA machines. The events include the names of CA operators, date and time of entering/leaving the CA room, and the purpose of the access to the machines.
- Access logs to the CA machines those are recorded by the Security Officers of NECTEC-GOC CA.

**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
- for each approved request, how the request was approved
- for each rejected request, how the request was rejected
- official documents if they are used for identification of entities
- All versions of the CP/CPS
- All Audit reports

#### 4.7.2 Retention Period for Audit Logs

The minimum retention period is three years.

#### 4.7.3 Protection of Archive

The archive is stored in a large secure safe in the NECTEC server room. This safe is accessible to only the NECTEC-GOC CA system administrator. The machine room security is described in [CPS 5.1]

#### 4.7.4 Time-Stamping Requirements

All archived logs and documents are time stamped.

#### 4.7.5 Archive Collection System

No stipulation.

#### 4.7.6 Procedures to Obtain and Verify Archive Information

No stipulation.

### 4.8 Key Changeover

#### 4.8.1 User certificate validity date

Each User certificates have to be re-issued in following validity term.

Type		Validity
Client certificate		13 months
Server certificate	Globus server	13 months

Table 4-1 user certificate validity

#### 4.8.2 CA certificate validity

CA will stop to sign new user certificates by its private key before it is shorter than user certificates. CA certificate validity is 10 years

Type	Validity
NECTEC Grid Operation Center Certificate Authority	10 years

Table 4-2 CA certificate validity

#### 4.9 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.

#### 4.10 CA Termination

In the event that the CA operates until the end of its certificate lifespan, it will be removed from service. All users and relying services will be notified well before this happens. Appropriate bodies may be notified and given the opportunity to access archives and records that might be necessary to establish an on going service.

### 5 Physical, Procedural and Personnel Security Controls

#### 5.1 Physical Security Controls

CA operations are performed in a server room that can be locked and in which no unauthorized persons are allowed during the operation. The CA machine is kept in a secured safe deposit box, stored in the server room. Only specific NECTEC-GOC CA system staff will have access to it physically. The CA machine is not connected to any network of any sort. Unauthorized users do not have access to the CA machine.

##### 5.1.1 Site Location

The 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 box. The safe deposit box is protected by a six-digit digital code. The battery used in the safe box will be replaced every 90 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 circumstances for staff and equipment running by setting of air conditioner.

##### 5.1.4 Water Exposure

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

##### 5.1.5 Fire Prevention and Protection

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

### **5.1.6 Media Storage**

Data is stored on local hard drives. Backups are stored on CDs or DVDs as per [CPS 4.7.3].

### **5.1.7 Waste Disposal**

No pass phrases or private keys will be recorded on paper apart from one copy in the safe deposit box [CPS 4.7.3]. Any media that has been used for backups or archives must be thoroughly cleaned and destroyed before being disposed of.

### **5.1.8 Off-site Backup**

No off-site backups are currently performed.

## **5.2 Procedural Controls**

Procedures will be tested by NECTEC-GOC staff to ensure correct operation as part of internal audit as mentioned in [CPS 2.7]

### **5.2.1 Trusted Roles**

One nominated NECTEC system administrators operate the CA. He know the CA Pass phrase. No other person will know his/her pass phrase although the NECTEC system administrator can find out what it is from the archive [CPS 4.7.3] if deemed necessary.

## **5.3 Personnel Security Controls**

Personnel are checked using identity cards before getting access to the building. Logs are retained of all entries.

### **5.3.1 Background Checks and Clearance**

CA personnel are recruited from the National Electronics and Computer Technology Center.

### **5.3.2 Background Checks and Security**

No other personnel are authorized to access NECTEC-GOC CA facilities without the physical presence of CA personnel.

### **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 NECTEC-GOC CA provides internal instruction manual for personnel.

## **6 Technical Security Controls**

The CA Key is 2048 or greater bits. The CA Key is protected by a pass phrase of 15 characters or longer. See above [CPS 4.7.3] and [CPS 5.2.1] for details of backup storage of the CA key.

### **6.1 Key Pair Generation and Installation**

#### **6.1.1 Key Pair Generation**

CA Key pair is generated by NECTEC-GOC CA operator. A Grid user and server may generate a key pair using a tool, such as "grid-cert-req", which is module from Globus Toolkit and no network transfer of private keys is required to get a certificate.

#### **6.1.2 Public Key Delivery to Certificate**

Certificate Signing Requests are submitted online using the HTTPS web interface.

#### **6.1.3 CA Public Key Delivery to Users**

The CA certificate is available online using the HTTPS web interface.

#### **6.1.4 Key Sizes Personal**

The size of personal and host keys is 1024 bits. Key Lifetime Personal keys have a life of 13 months. Host keys have a life of 13 months. The CA itself has a life of 10 years.

#### **6.1.5 Public Key Parameters Generation**

Key generation parameters are controlled by Grid configuration files. The files are provided by CA operator, and can be downloaded from the repository.

#### **6.1.6 Parameter Quality Checking**

No stipulation

#### **6.1.7 Hardware/Software Key Generation**

Software key generation is used in NECTEC-GOC .

#### **6.1.8 End User Key Protection**

End users must protect their private key with a pass phrase at least 12 characters long. A pass phrase of at least 12 characters long must also be applied to the users browser master password. Under no circumstances should an end user share their private key with another user or any other person. The CA cannot enforce these rules apart from making them plain to end users and advising them that CA services could be withdrawn if they are identified as not complying.

#### **6.1.9 Key Usage Purposes**

User keys are intended for generating proxy certificates and identifying browser users. They may be used for other standard certificate applications as well.

## **6.2 Private Key Protection**

### **6.2.1 Standards for cryptographic module**

No Stipulation

### **6.2.2 Private Key (n out of m) Multi-person Control**

No Stipulation

### **6.2.3 Private Key Escrow**

No Stipulation

### **6.2.4 Private Key Archival and Backup**

The Certificate Authority private key backup is stored on a CD or USB disk located as described in [CPS 4.7.3].

## **6.3 Other Aspects of Key Pair Management**

- 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 15 characters passphrase created by NECTEC-GOC CA operator.

## **6.5 Computer Security Controls**

### **6.5.1 Specific Computer Security Technical Requirements**

NECTEC-GOC CA regularly apply security patches to ensure the security of publicly accessible servers.

### **6.5.2 Computer Security Rating**

No Stipulation

## **6.6 Life-Cycle Security Controls**

No Stipulation

## **6.7 Network Security Controls**

The NECTEC-GOC CA machine is unconnected to any network, and is therefore secured from network based attack. The RA machine is protected in the normal manner, that is maintained with current OS patches and observed closely.

## **6.8 Cryptographic Module Engineering Controls**

No Stipulation

## **7 Certificate and CRL Profiles**

### **7.1 Certificate Profile**

Certificate profile is described in a separate document, “NECTEC-GOC CA Certificate and CRL Profile version 1.0”. The document is available on the NECTEC-GOC CA repository.

### **7.2 CRL Profile**

CRL profile is described in a separate document, “NECTEC-GOC CA Certificate and CRL Profile version 1.0”. The document is available on the NECTEC-GOC CA repository.

## **8 Specification Administration**

### **8.1 Specification Change Procedures**

Changes may be made to the CPS Document, subject to provisions in “CPS Approval Procedures”, [CPS 8.3] without individual user notification. Users may read the current CPS at any time and reasonable attempts will be made to notify users of changes that affect them.

### **8.2 Publication and Notification Procedures**

For minor editorial changes, revision to this CPS will be announced on the NECTEC-GOC CA repository. Substantial changes will be notified by E-mails to all relevant NECTEC-GOC CA’s participants. These changes will also be announced on the NECTEC-GOC CA repository.

### **8.3 CPS Approval Procedures**

Changes to the CPS must be approved by NECTEC GRID PMA before the document is changed.

Changes that make no alteration to meaning can be made without releasing a new version. This would normally be limited to spelling corrections and similar. A record of such changes should be made in the document header.

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 impact.

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

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

# Glossary

## Activation Data

Data values, other than keys, that are required to operate cryptographic modules and that need to be protected (e.g., a PIN, a passphrase, or a manually-held key share).

## CA certificate

A certificate for one CAs public key issued by another CA.

## Certificate Authority

Certificate Authority (CA) is 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 (CP) is 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 (CPS) is a statement of the practices, which a certification authority employs in issuing certificates.

## CRL

Certificate Revocation List (CRL) is 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 (CRR) is a message sent from an applicant to a certificate authority in order to revoke for a digital identity certificate.

## CSR

Certificate Signing Request (CSR) is a message sent from an applicant to a certificate authority in order to apply for a digital identity certificate.

## DN

Distinguished Name (DN) is a data set that identifies an Entity in the real world (such as a natural person) in the electronic context. (eg. CountryName=TH, State=Pathumthani, OrganizationName=NECTEC, CommonName=Suriya)

## End-Entity

End Entity (EE) is a certificate subject that does not sign certificates (i.e., person, 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 is 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 (PKI) is 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 (RA) is 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**

Relying Party is 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, same as certificate subject.

## Bibliography

1. Internet X.509 Public Key Infrastructure Certificate and CRL Profile. <http://www.ietf.org/rfc/rfc2459.txt>
2. Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework. <http://www.ietf.org/rfc/rfc2527.txt>
3. AIST GRID PKI Service Certificate Policy and Certificate Practice Statements Ver.1.1.1, June 15,2005
4. APAC-GRID Certificate Policy and Certificate Practice Statement Ver.1.2, May 1,2006