



# Thailand Grid Certificate Authority

*Suriya U-ruekolan*

*Computing Research and  
Development Division,  
NECTEC Thailand*

# Outline

---

- **NECTEC Grid Infrastructure**
- **About APGrid PMA**
- **Thailand Grid Certificate Authority**
- **Future Work**

# About NECTEC

- **National Electronics and Computer Technology Center**
- **Government Research Institute**
- **Under National Science and Technology Development Agency (NSTDA) , Ministry of Science and Technology**
- **Missions:**
  - Research, development, design, and engineering of Electronics and ICT technologies
  - Technology transfer to industries
  - Human resources development for Electronics and ICT technologies
  - Technology-related infrastructure and policy development

# NECTEC Grid Infrastructure

- **Main Cluster Computer**

- 33 nodes Rocks Cluster
- 3.2 TB storage
- ~200 GFlops



- **Grid supporting system**

- MDS (GT4 starting in Jan 2006)
- Resource Broker (Starting in Apr 2006)
- *Thailand Grid CA System (Started in July 2005)*

# About APGrid PMA

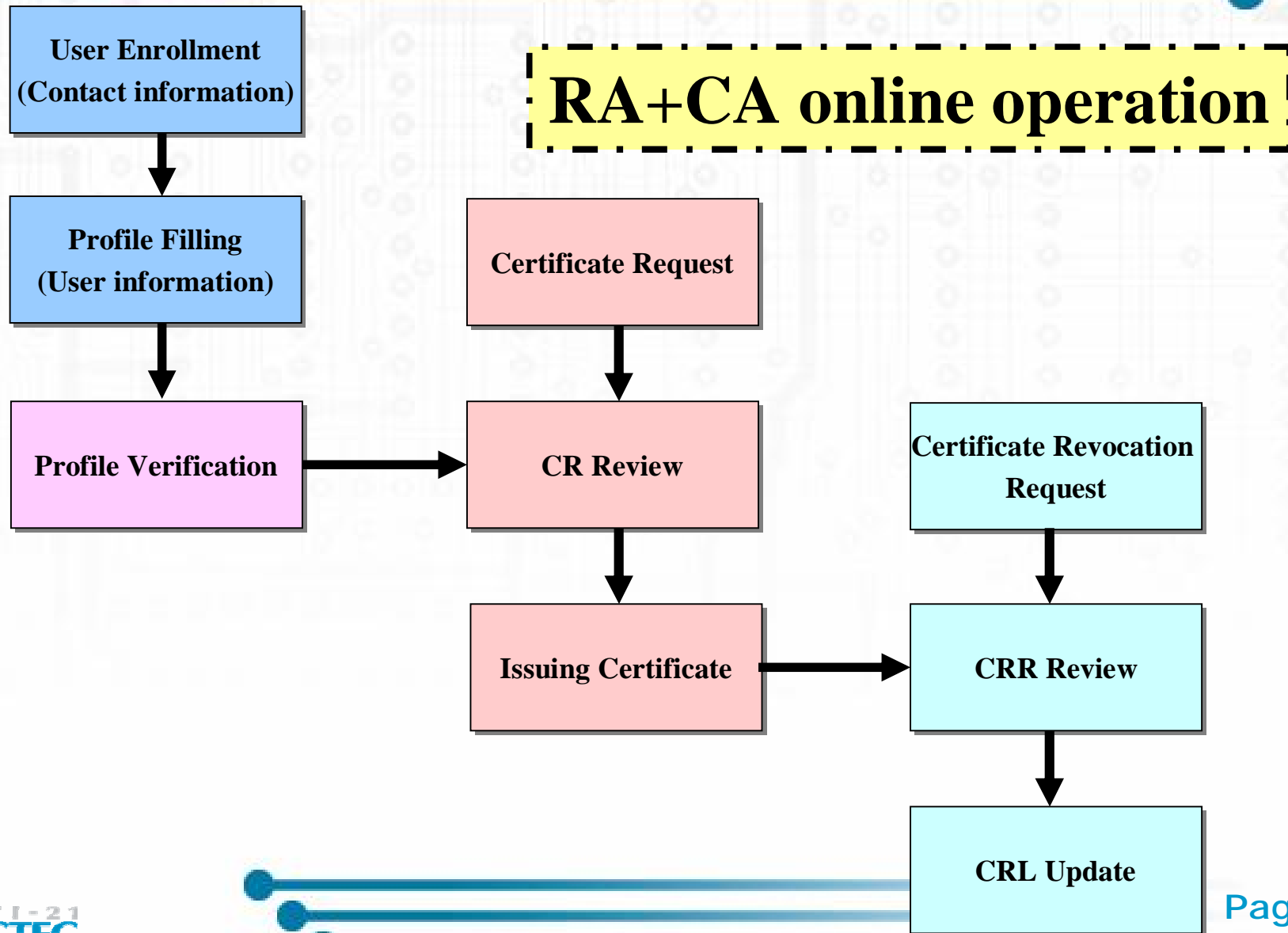
- **Supports Grid communities in Asia Pacific to implement a common trust domain across organizations.**
- **Coordinates Public Key Infrastructure for use with Grid authentication**
- **NECTEC joined APGrid PMA in 2005**



# About Thailand Grid CA

- **A project designed to set up a CA for Thailand Grid resources**
- **Two Phases:**
  - Experimental Phase (Use for NECTEC Grid Community only)
  - Production Phase (Use for Thailand Grid Community)
- **Thailand Grid CA operates under APGrid PMA's policy**

# Experimental Phase



# Hardware & Software Stack

## RA+CA Online operator

Content Management System  
(Public Interface)

DBMS

PHP

OpenSSL Library

LINUX OS (Slackware)

HARDWARE

P4 3.0GHz RAM 512 MB Storage 120GB SATA RAID1



# Experimental CA Public Interface



## NECTEC-GRID Certificate Authority

Home

### Main Menu

Home  
Contact Us

### Publication

CA Certificate / CRL  
PKCS12 to PEM

### Related links

HPCC wiki

### Login Form

Username

Password

Remember me

Login

Forgotten your password?  
No account yet? Register

Welcome to NECTEC-GRID Certificate Authority

NECTEC-GRID Certificate Authority provides X,509 certificates to support GRID Computing Research and Development.



We issue :

- Grid Computing Certificates
- Access Grid Certificates

NECTEC-GRID Certificate Authority is operated by Computing Research and Development Division, National Electronics and Computer Technology Center.

<http://rdcca.hpcc.nectec.or.th>

Last Updated ( Thursday, 30 March 2006 )

### Main Menu

Home  
Contact Us

### Publication

CA Certificate / CRL  
PKCS12 to PEM

### Related links

HPCC wiki

### Login Form

Username

Password

Remember me

Login

The NECTEC-GRID root certificate, CRL and GRID SSL environment can be downloaded from the links in the table below.

NECTEC-GRID Root CA	PEM format	DER format	CRT format	163dae9d.0
Signing Policy	NECTEC GRID Signing Policy			
Certificate Revocation List	PEM format	CRL format	163dae9d.0	
FingerPrint SHA-1	5e:66:74:25:2e:1e:b8:7e:53:67:b8:56:37:ff:e5:82:fb:b5:77:ee			
FingerPrint MD5	c8:01:b9:5ecc:7:58:e3:d6:6e:7d:face0cf1d0:b1:e6			

**Public interface for CA repository**

# Production Phase

- **Open CA is used for implementing full CA functionality:**
  - Public interface (enrollment , repository)
  - RA
  - CA
- **Installation Environments**
  - Two dedicated servers:
    - Public interface and RA server:
      - Fedora Core 4 OS
      - RA requires SSL
    - CA server (offline):
      - Fedora Core 4 OS
      - CA requires SSL

# Production Phase Operator

Repository, CA, CRL

Public Interface

RA Server (online)

Manually

CA Server (Standalone)

HTTP/SSL

End-entity

3. Approve CSR and user identity

- Approve request  
- revocation and public CRL

4. Issued certificate

- Revocation certificate
- Update CRL

Offline

(Not Network)

1. Send request via application form or email

2. Generate CSR and enroll to RA by paste it in public interface

# Certificate Authority

- **Single CA issuing end-entity certificate for:**
  - Users in Thailand Grid Community
  - Thailand Grid Community hosts and services
  - Private-key (2048bits) stored in the CA server hard-disk
  - The server is off-line and accessing to the server room is restricted
  - Backup symmetric encryption passphrase known only to two staff members
  - Subject format:  
C=TH , O=NECTEC, OU=NECTEC-GOC, CN=NECTEC GRID CA

# Registration Authority

- **Approve user's identity (application form or face-to-face meeting)**
- **Send user enrollment request to the CA correctly**
- **Send user revocation request to the CA quickly.**

# End-entity certificates

- **Thailand Grid Community user certificates are used for dynamic delegation through proxy-certificate issuance.**

- Subject format:

- C=TH, O=NECTEC, OU=NECTEC-GOC, CN= <Full user name>

- **Thailand Grid Community host/LDAP certificates are used in client to host mutual authentication.**

- Subject format:

- C=TH, O=NECTEC, OU=NECTEC-GOC, CN= host/<FQDN>

- C=TH, O=NECTEC, OU=NECTEC-GOC, CN= ldap/<FQDN>

# Enrollment user certificates

- **Thailand Grid CA user certificate enrollment:**
  - User generates key-pair and CSR (PKCS#10) using grid-cert-request on globus toolkit
  - User sends application form to RA
  - User sends CSR via a public interface
  - RA operator goes through the validation process
  - CA operator issues the certificate

# Enrollment host certificates

- **Thailand Grid CA host certificates enrollment:**
  - Grid system administrator generate key-pair and CSR using grid-cert-request tool on globus toolkit
  - Grid system administrator sends CSR via paste it in enrollment form in the public interface
  - RA Operator goes through the validation process
  - CA Operator issues the certificate



# Revocation and CRL's

- **PIN-based revocation in the public interface requested by user, approved by the RA operator and performed by the CA operator**
- **Direct revocation requested and approved by the RA operator and performed by the CA operator**
- **CRL's are issued with 30 days validity period whenever a certificate is revoked or one day before the current CRL expiration**

# Public Interface

- **The public interface serves as a repository via HTTP for the following data:**
  - End-entity certificates
  - CRL's
  - CP/CPS
  - CA Certificate, Signing policy and grid-mapfile

# Future Work

---

- **Write CP/CPS documents**
- **Creation of production RA and CA in NECTEC RDC**
- **Testing certificates on Thailand Grid Community environment**

**Thanks**

