



1st APGrid PMA Meeting

29 Nov 2005

Jon Lau
National Grid Office
Singapore

Agenda

- Introduction to National Grid (NG)
- Commercial CA for NG Pilot Platform
- About Netrust
- Certificate Application Process
- Points to Note



National Grid

National Grid Vision

to facilitate the seamless use of an integrated cyber infrastructure in a secure, effective & efficient manner to advance scientific, engineering & biomedical R&D,

with the longer term goal of transforming the Singapore economy using grid

National Grid Steering Committee

Chairman

MTI
(A*STAR,
EDB, SPRING, RIS)

MINDEF
(DSTA, DSO)

MITA
(IDA, MDA)

MOH
(Hospitals)

MOE
(Schools,
NUS, NTU)

Industry
(Lilly, CPG,
ITSC, SITF, ...)

Working Groups

Security

Middleware & Architecture

Governance & Policy

Network

SIGs

System Administrators

Access Grid

PC Grid Computing

Physical Sciences

Life Sciences

Digital Media

Manufacturing

...

Virtual Grid Communities

**National Grid
Governance Council
(NGGC)**

Facilitates &
coordinates activities

**National Grid
Office
(NGO)**

**National Grid
Operations
Centre
(NGOC)**

**National Grid
Competency
Centre
(NGCC)**

Activities

- Formulate the framework & policies
- Plan & develop a secure platform
- Adopt common open standards
- Encourage the adoption of Grid Computing
- Demonstrate the commercial viability of compute-resource-on-tap
- Lay the foundation for a vibrant Grid Computing economy

National Grid Pilot Platform – Phase 1

- Objectives:
 - Build grid computing awareness
 - Foster collaboration
 - Interconnect main compute resources
- Scope:
 - Establish 1GE backbone
 - Establish rudimentary infrastructure for R&D in universities/research centres
 - Testbed distributed applications



Entity	OS	Platform
IHPC	AIX	IBM Regatta
One-North (BII & GIS)	Linux Solaris	Compaq Alpha Cluster Sun
NUS	Linux	Intel Xeon Cluster
NTU	Solaris Linux	Sun Fire Intel Pentium 4
SMA	Linux	Itanium 2

NGPP Certificate Authority

Commercial CA

- Objective:
 - To migrate from free digital certificates to commercial CA digital certificates so as:
 - Increased security robustness, in preparation for industry focus in NGPP2
 - Understand security procedures & issues pertaining to commercial CA certificate
- Tender awarded to Netrust Pte Ltd
 - Netrust is the only certified CA in Singapore
 - Netrust is able to accommodate flexibility in implementing digital certificates usable in Globus

Netrust Certificate Authority

- NGO has been officially acknowledged by Netrust as an Organizational Registration Authority (ORA)
 - Will ease NGPP sites in obtaining certificates – without ORA, need to obtain certificates from Netrust
 - NGO will perform the administrative processes only
- NGPP sites nominated representatives to receive digital certificates
- All existing NGPP sites have migrated their host certificates to Netrust certificates
- Continual effort to issue certificates for
 - New users of NGPP resources
 - Additional hosts added to NGPP
- **Temporary CA** will continue to exist to issue certificates for *testing* and *trials*.

About Netrust



Netrust



- Established in May 1997 as the **first Certification Authority (CA)** in **Southeast Asia**.
- Provides individuals, businesses and government organisations with a complete online identification and security infrastructure to enable secure electronic transactions via the Internet and other wireless media.
- In its **capacity as a CA**, Netrust acts as a trusted third party (TTP) that issues and manages digital certificates. Netrust maintains a Public Key Infrastructure (PKI) certification service and in its CA role creates and signs X.509 digital certificates which bind individuals, organisations and application servers with the particular public key of each subscriber.
- Netrust's digital certificates can be issued **globally** and provide complete online identification and security for secure electronic transactions. It supports the core security requirements of **Authentication, Authorization, Confidentiality, Data Integrity** and **Non-Repudiation**.

- ▶ Facts & Figures
- ▶ IDA Programmes
- ▶ Policy & Regulation

- ▶ Broadband
- ▶ Digital Exchange
- ▶ E-Business
- ▶ Manpower Development
- ▶ Technology Development
- ▶ Wireless

- ▶ About IDA
- ▶ Talk To Us
- ▶ Partner With Us
- ▶ Send This Page

- ▶ Privacy Statement
- ▶ Terms Of Use

[IDA Home](#) > [Policy & Regulation](#) > Licensed CAs in Singapore

Licensed CAs in Singapore

The following company has been granted a CA licence by the Controller of Certification Authorities:

[Netrust Pte Ltd](#)

10 Collyer Quay
Ocean Building #09-05/06
Singapore 049315
Tel: 62121388
Fax: 62121366

Logos For Licensed CAs

Licensed CAs may display the following logos during the conduct of their business as an indication that they have complied with the licensing criteria specified by the Controller of Certification Authorities.

The licensing criteria are stipulated in the [Electronic Transactions Act 1998](#), [Electronic Transactions \(Certification Authorities\) Regulations 1999](#) and the [Security Guidelines for Certification Authorities](#).

Disclosure Records of Licensed CAs

Publicly accessible database on licensed CA disclosure records

[Netrust Disclosure](#)

[Back to Top](#)



- ▶ Facts & Figures
- ▶ IDA Programmes
- ▶ Policy & Regulation

- ▶ Broadband
- ▶ Digital Exchange
- ▶ E-Business
- ▶ Manpower Development
- ▶ Technology Development
- ▶ Wireless

- ▶ About IDA
- ▶ Talk To Us
- ▶ Partner With Us
- ▶ Send This Page

- ▶ Privacy Statement
- ▶ Terms Of Use

[IDA Home](#) > [Policy & Regulation](#) > Security Guidelines for Certification Authorities

Security Guidelines for Certification Authorities

Title	(in PDF)	Link
Security Guidelines for CAs (Version 2.0)	PDF	
BS 7799 Standard		Link

The BS7799 standard is a comprehensive set of controls comprising the best practices in information security. It is an internationally recognized generic information security standard.

The BS7799 comprises of two parts, namely:

- ◆ **BS 7799-1:2000** (Information Technology - Code of practice for information security management) and;
- ◆ **BS 7799-2:2002** (Information Security Management - Specification for information security management systems)

The BS7799 Standard is intended as a single point of reference for identifying a range of controls needed for most situations where information systems are used in industry and commerce. It establishes the basic framework for implementing adequate IT security that preserves and protects the quality of an organization's informational assets.

The "Security Guidelines for CAs" document defines the security guidelines for the management, systems and operations of a certification authority (licensed or potential licensee). It is intended for use by the management, security, technical and operational personnel of a certification authority.

Together, the documents provide the holistic security framework for managing and operating a CA and protecting its informational assets and general IT systems and operations at the same time.

Potential licensees and licensed CA's may obtain a copy of the BS7799 from its [official website](#).

BS7799

- **BS7799** is the **most widely recognised security standard in the world**. Although it was originally published in the mid-nineties, it was the re-vision of May 1999 which really put it on to the world stage. Ultimately, it evolved into **BS EN ISO17799** in December 2000.
- BS 7799 (ISO17799) is comprehensive in its coverage of security issues, containing a significant number of control requirements.
- Compliance with it is consequently a far from trivial task, even for the most security conscious of organizations.

Certificate Application Process

NGPP Host Certificate Registration/Issuance



- Registration process
 - Applicant/Administrator (nominated) submits required documents to NGO (personally) on behalf of organisation
 - Application form (duly signed)
 - Photocopy of NRIC/Passport/Employment Pass (clear)
 - Letter of Authorization from organisation to authorise **applicant to receive** the host certificate (duly signed by dept. head)
 - NGO submits required documents to Netrust
 - Netrust CA issues *enabling codes* (a.k.a. Authorisation Code & Reference Number)
 - CA forwards 1 set of code to the applicant via email
 - CA forwards Reference Number to NGO via email
 - NGO informs applicant via phone/SMS
 - Applicant log-on to Netrust interface to submit CSR and codes
 - CA signs certificate and returns to applicant

Netrust Digital Certificate Application Form Host Certificate

Instructions for form submission:

1. Please submit completed form to NGO.
2. Bring along:
 - i. Original and photocopied identification documents (e.g. NRIC/Passport) for verification.
 - ii. Letter of authorisation duly signed by person of acceptance to NGO.
 - iii. Certified true copy of Registry of Companies & Businesses (RCB) Certificate, if applicable.
 - iv. Proof of domain name ownership, if applicable.

Company Information

Company Name: _____
Business/Company Registration No: _____ Date of Registration: _____
Billing Address: _____
Postal Code: _____

Applicant Particulars

First Name: _____ Last Name: _____
NRIC/Passport/Foreign ID No.: _____ Gender: _____
Designation: _____ Email: _____
Tel No.: _____ Handphone No.: _____ Fax No.: _____

Application Server Details

FQDN: _____
Hardware Architecture (e.g. Xeon, Itanium2): _____
Operating System: _____

By signing below, I hereby acknowledge and accept the terms and conditions as stated in the Subscriber Agreement.

Signature: _____ Application Date: _____

Date:

To: National Grid Office
21 Heng Mui Keng Terrace
Singapore 119613
Fax: (65) 68721361

Cc: Netrust Pte Ltd
Customer Service Manager
10 Collyer Quay #09-05/06 Ocean Building
Singapore 049315

**RE: LETTER OF AUTHORISATION – NGPP (NETRUST) DIGITAL
CERTIFICATE**

This is to certify that <Applicant Name>, <NRIC/FIN/Passport no.>, is an employee of <Organisation Name>. He/She* has been authorised to apply and collect a NGPP (Netrust) Certificate on behalf of <Organisation Name> for the following host(s) that the host certificate(s) is/are being applied for:

1. <FQDN>
2. <FQDN>
- .
- .
- .

<signature>

Yours sincerely,
<Name of authorising officer>
<Designation of authorising officer>

NGPP User Certificate Registration/Issuance



- Registration process
 - User submits required documents to NGO (personally)
 - Application form (duly signed)
 - Photocopy of NRIC/Passport/Employment Pass (clear)
 - Letter of Authorization from organisation to certify that the **applicant is an employee of the organisation**
 - NGO submits required documents to Netrust
 - Netrust CA issues *enabling codes* (a.k.a. Authorisation Code & Reference Number)
 - CA forwards reference code to applicant via email
 - CA forwards authorisation code to applicant via pin-mailer
 - Applicant generates his/her own CSR and log-on to Netrust interface to submit CSR and codes
 - CA signs certificate and returns to applicant

Netrust Digital Certificate Application Form User Certificate

Instructions for form submission:

1. Please submit completed form to NGO.
2. Bring along:
 - i. Original and photocopied identification documents (e.g. NRIC/Passport) for verification.
 - ii. Letter of authorisation duly signed by person of acceptance to NGO.
 - iii. Certified true copy of Registry of Companies & Businesses (RCB) Certificate, if applicable.

Personal Particulars

First Name: _____ Last Name: _____
(according to NRIC)

NRIC/Passport/Foreign ID No.: _____ Gender: _____

Mother's Maiden Name: _____ (for emergency identification)

Home No.: _____ Pager No.: _____ Handphone No.: _____

Home Address: _____

Professional Details

Organisation: _____

Department: _____ Appointment/Designation: _____

Billing Address: _____

Postal Code: _____ Office No.: _____ Fax No.: _____

Email Address: _____

By signing below, I hereby acknowledge and accept the terms and conditions as stated in the Subscriber Agreement.

Signature: _____ Application Date: _____

For Official Use Only

Verifying Officer: _____ Date Verified: _____

Date:

To: National Grid Office
21 Heng Mui Keng Terrace
Singapore 119613
Fax: (65) 68721361

Cc: Netrust Pte Ltd
Customer Service Manager
10 Collyer Quay #09-05/06 Ocean Building
Singapore 049315

**RE: LETTER OF AUTHORISATION – NGPP (NETRUST) DIGITAL
CERTIFICATE**

This is to certify that <Applicant Name>, <NRIC/FIN/Passport no.>, is an employee of <Organisation name>. He/She* has been authorised to apply and collect a (NGPP) Netrust Certificate.

<signature>

Yours sincerely,
<Name of authorising officer>
<Designation of authorising officer>

Certificate Lifetime & Revocation List (CRL)

- Netrust certificates have a life of 5 years (flexible)
 - Considerations: cost, user generation experience, size of CRL
- Netrust generates a new CRL every 24 hours
- The CRL can be downloaded from <http://netrustconnector.netrust.net/netrust.crl>

Host Cert Info

- Issuer: C=SG, O=Netrust Certificate Authority 1, OU=Netrust CA1

Validity

Not Before: Jun 6 01:19:13 2005 GMT

Not After : Apr 19 16:00:00 2010 GMT

Subject: C=SG, O=Netrust Certificate Authority 1, OU=Netrust CA1 (Server), OU=National Grid Pilot Platform, CN=machine.ngpp.ngp.org.sg

User Cert Info

- Issuer: C=SG, O=Netrust Certificate Authority 1, OU=Netrust CA1

Validity

Not Before: Aug 5 07:39:04 2005 GMT

Not After : Apr 25 16:00:00 2010 GMT

Subject:

C=SG, O=Netrust Certificate Authority 1,
OU=Netrust CA1 (Corporate), OU=National Grid
Pilot Platform, OU=National Grid Singapore,
CN=TAN Ah Seng + serialNumber=SG-
A1234567N:W:1,

Points to Note

Certificates Issued

- Issued todate:
 - 16 User Certificates
 - 27 Host Certificates
 - None revoked (as yet)
- To organisations in Singapore:
 - Bioinformatics Institute
 - Institute for High Performance Computing
 - Nanyang Technological University
 - National Grid Singapore
 - National University of Singapore
- Updated list of issued certificates obtainable from Netrust

Issues Faces/Lessons Learnt

- Documentation procedures – unclear photocopies of NRIC, illegible handwriting, & missing letter of authorizations
- Retrieval of Certificates – wrong steps
- Justification on relationship to Parent organization to use its domain name (IHPC, Nanyang Campus Grid, & SMA)
 - E.g. www.sma.nus.edu.sg, www.ihpc.nus.edu.sg

Considerations

- Cost of certificate
- Type of certificates
 - Ownership: Organisation Certificate, User Certificate
 - Regeneration when keys are wrongly entered
- Relaying authorisation code
 - NGO relays using SMS
 - Other ways?

End

jonlau@ngp.org.sg

www.ngpp.ngp.org.sg