NETRUST PTE LTD ("NETRUST") CERTIFICATE POLICY
NETRUST GRID-ID CERTIFICATE
(POLICY OID: 1.2.702.0.1002.6.7 & IGTF AP Classic OID: 1.2.840.113612.5.2.2.1)

1. Introduction

The Certificate Policy (CP) is a named set of rules that indicate the applicability of a certificate to a particular community and/or class of applications with common security requirements and is further supported by the Netrust Certification Practice Statement ("CPS").

When Netrust issues a certificate, it is making a statement that the certificate is associated with the person, organisation or equipment uniquely named within that certificate. The process of issuance of any class of certificates is guided by the relevant CP and the CPS. The Applicant's organisation should assess his own requirements when relying on a particular Netrust Certificate, taking into consideration the CP applicable to that Netrust Certificate, together with the CPS.

This CP is applicable to the class of Netrust GRID-ID Certificate ("NGIC").

2. Certificate Profile

NGIC issued under this CP shall contain the following information. Additional information may be included as necessary.

Field	Content
1. Issuer Distinguished Name	The Issuer Distinguished Name should contain the following fields.
1.1. Organisational Unit (OU)	Netrust Certificate Authority
1.2. Organisation (O)	Netrust Pte Ltd
1.3. Country (C)	SG
2. Validity	
2.1. Valid From	e.g. Wednesday, July 01, 2009 00:00:01AM
2.2. Valid To	13 Months e.g. Sunday, Aug 01, 2010 00:00:01AM
3. Subject	The Subject Distinguished Name should contain the following fields.
3.1. Serial Number (2.5.4.5)	a. Organisations that are registered with a registration body: (ISA code of country + '-' + Unique Entity Number+ ':' + E or W + ':' + 0) e.g. SG-199702368H:E:0 for organisations that are registered with ACRA (Unique Entity Number aka UEN) SG-ACP133126:E:0 for law firms that are registered with The Law Society of Singapore. SG-0166/2002:E:0 for organisations that are registered with Registry of Societies

	b. Organisations that are not registered with a registration body: (ISA code of country + '-' + Abbreviated organization name + ':' + E or W + ':' + 0) e.g. MY-Universiti of Malaya:W:0 for 'Universiti of Malaya' c. Individuals/Users: (ISA code of country + '-' + NRIC or Passport No. or FIN No.) or (Employee No.) + ':' + E or W + ':' + 0) E.g. SG-S1234567A:E:0
3.2. Common Name (CN)	Designation and/or Department or Company Name (for Organisation only) or Name of person (for Individuals)
3.3. Organisational Unit (OU)	Company or Society or Organisation Name
3.4. Organisational Unit (OU)	Netrust CA 2-1 (Corporate)
3.5. Organisation (O)	Netrust Pte Ltd
3.6. Country (C)	SG
4. Key Usage	Digital Signature, Key Encipherment
5. Certificate Policies	This extension gives reference to the certificate policy under which this certificate is issued.
5.1. Policy Identifier	1.2.702.0.1002.6.7 1.2.840.113612.5.2.2.1 (AP Classic)

3. Characteristics

A. Registration

Registration of the NGIC will be based on the Applicant's organisation submitting an application form, properly filled and signed, to the Organisation Registration Authority ("ORA"). The form must include the Netrust Subscriber Agreement. The Applicant's organisation must also submit Proof of Right by sending suitable documentation. The table below list documents, which can be submitted.

Organisation Type	Submit
A company, corporation, partnership, or proprietorship	The company registration document, or a copy of article of incorporation or partnership stamped by the relevant authority
A government department or agency	An original letter of authorisation signed by the department head on appropriate letterhead. The letter must include contact information for the department and for the signer's immediate superior.

A non-government organisation (NGO)	An original letter of authorisation signed by the Chief Executive, Chairman, or Managing Director of the NGO on appropriate letterhead
A type of organisation not listed here	Please contact Netrust to determine suitable documentation

B. **Issuance**

Issuance of the NGIC will be based on the ORA providing a set of unique registration information to allow the Applicant's organisation to generate a set of unique keys and Certificate in accordance with Clause 4.2 of the CPS.

Acceptance of the NGIC will be based on the ORA implicitly accepting a profile that contains the Applicant's organisation's private signing key and decryption key, public verification and encryption certificates and the Netrust CA public verification certificate.

C. **Storage & Escrow**

The Applicant's organisation's private keys associated with the NGIC must be stored in an appropriate medium – on disk or crypto tokens. The Applicant's organisation must be aware that private keys stored on a less secure medium may not provide the desired level of assurance.

With the NGIC, the Netrust Public Certification Services Framework only has provision to perform key escrow for private encryption key.

4. Applicability and Suitability

NGIC is firstly intended for use within the International Grid Trust Federation (IGTF) community to provide credentials requiring strong authentication, message integrity and digital signing. NGIC is in compliance with the Authentication Profile requirements of IGTF. The **IGTF AP Classic OID** is added for this specific purpose. The NGIC is suitable for supporting the deployment of large scale distributed computing grids on a production scale, across organisations, across countries, and across continents, for the advancement of science and engineering.

NGIC is also intended for the support of strong authentication, message integrity and digital signing requirements of commercial GRID infrastructure and applications.

5. Loss and Replacement

In the event of loss of the NGIC token, the Subscriber must personally report to Netrust or Sponsor ORA. The replacement process will be similar to the initial registration process.

6. Validity and Expiry

NGIC will have a validity of 13 months in accordance to the IGTF-AP-Guidelines.

7. Renewal

Upon expiry, the Applicant's organisation will have to obtain a new set of keys (re-keying) and certificate through the defined renewal process.

8. Obligations

The Netrust CPS sets out the obligations to be performed by Netrust, the Organisation Registration Authorities, the Sponsors, the Applicant's organisations and the Relying Parties and all such provisions must be read and understood by all parties and shall be deemed to be incorporated herein by reference.

9. Disclaimers

9.1 Netrust shall not be liable for any loss or damage whatsoever, including but not limited to direct, compensatory, indirect, special, consequential, exemplary or incidental damages incurred by any person howsoever arising directly or indirectly, including but not limited to contract, tort and any other form of liability claims, in connection with the use or reliance on any certificates by any parties. Unless otherwise expressly stated in this CP, Netrust does not warrant that any materials, documents, software, products or any certificates supplied or provided by Netrust will be error-free and all statements, conditions or warranties, express or implied, statutory or otherwise, as to the quality, merchantability, or suitability or fitness for any particular purpose of any such materials, documents, software, products or any certificates thereto is hereby excluded.

9.2 In the event that any limitation or provision contained in this Agreement is held to be invalid for any reason and Netrust becomes liable for loss or damage that would otherwise have been excluded hereunder or excludable in law, Netrust's total liability shall be limited to the aggregate amount of its liability under any insurance policies that it subscribes to for each certificate as set out below and as may be further and/or subsequently amended by Netrust.

Certificate Class	**Liability Cap**
NGIC	Singapore Dollars Fifty Thousand (S$50,000.00) Only

THIS CP MUST BE READ IN CONJUNCTION WITH THE NETRUST CPS AT http://www.netrust.net