PRIVATE AND CONFIDENTIAL

Certificate Practice Statement

Version 2.1.0

February 2021

Revision History

Version	Date	Comments	Performed by
1.0	2 July 1999	Document created	-
2.0	29 Jan 2001	The changes made to the CPS are: • Clause 2.1.2.3: Additional disclosure on the privileges given to the ORAs. • Clause 2.1.5.1: Clearer instructions for relying party to check on the validity of the Certificate before any reliance is made. • Clause 2.1.6.1: Amendment in the uptime to 99.7%. • Clause 2.1.6.2: Additional practice that Netrust will ensure that the downtime for the Directory will not exceed 30 mins • Clause 2.2.1.3: Additional information in loss limitation that for each class of Certificate, the liability cap is stipulated in the respective CP. • Clause 2.7.1.2: Additional clause for Netrust to submit the compliance audit report to CCA within 4 weeks of completion of the audit. • Clause 2.8.1.2: Additional clause that all subscriber-specific information must be authorized by the Subscriber. • Clause 4.2.3: Addition of Entrust Ver. 5 Certificates. • Clause 4.3.1: Additional procedures for certificate acceptance acknowledgement by the applicant. • Clause 4.4.1.1: Additional circumstances that would result in a revocation of the Certificate. • Clause 4.4.3.3: Additional procedures for revocation requester to include submission of supporting documents when requesting for revocation. • Clause 4.4.4.1: Change in the revocation request period to be immediate for all Certificates, including Entrust 5 Certificates.	Adrian Tan

		• Clause 4.4.4.2: Additional procedure for Netrust to notify the Subscriber on the date, time and reason why revocation was made. • Clause 4.4.5: Suspension procedures included • Clause 4.4.5.1: Circumstances for suspension included. • Clause 4.4.6 : Now applicable • Clause 4.4.6.1: Persons allowed to make suspension request included. • Clause 4.4.7: Now applicable • Clause 4.4.7.1: Procedures for suspension included. • Clause 4.4.7.2: Verification procedure for suspension included. • Clause 4.4.7.3: Documents for suspension included. • Clause 4.4.8.1: Suspension limit period has been set at one month from the date of receipt of the suspension request. • Clause 4.5.6.1: Inclusion of IDS and Network Monitoring Tools. • Clause 4.4.10.2: Ability to revoke and publish in the CRL upon request added. • Clause 7.1.6: Amendments in Certificate OID and types for Certificates in Entrust Ver. 5. • Clause 9.1.1: Inclusion of Controller of Certificate Authority of Singapore as one of the bodies to receive the circulation of the list of proposed changes to the CPS made.	
2.0.1	Mar 2001	Amendments to: • Clause 4.1.2: Added list of supporting documents needed for application of Corporate certificates • Clause 7.1.5: Updates to OIDs • Removal of Clause 4.1.3	Adrian Tan

2.0.2	Jan 2002	Amendments to: • Clause 4.2.3: Removal of reference to NetPass, WebServer, WebClient and Silver Class certificates. • Clause 4.4.4.1: Removal of reference to NetPass, WebServer, WebClient and Silver Class certificates. • Clause 7.1.5: Updates to OIDs	Adrian Tan
2.0.3	Mar 2002	Amendments to: • Clause 1.4.2.1: Update to contact details • Clause 5.1.2.3: Update of Data Center • Clause 5.1.3.2: Update of Data Center • Clause 5.1.4.1: Update of Data Center	Lim Hock Ern
2.0.4	Aug 2002	Amendment to: • Clause 6.1.2.2: Removal of statement indicating that private keys may be hand delivered or emailed to the rightful owner.	
2.0.5	Apr 2013	Amendments to: • Clause 1.4.2.1 and Glossary: Updated Company Address. • Clause 4.2.3: Updated Certificate Types to all Netrust Certificates, and added encrypted email as another mode of delivery of activation codes. • Clause 4.4.4.1: Updated certificate types to all Netrust Certificates. • Clause 6.7.2: Deleted Network Security Control device no longer in use and added HSM. • Clauses 7.1.1.1 and 7.2.1.1: Deleted reference to the outdated year for the Standards documents. • Clause 7.1.2.1: Updated the list of supported algorithms. • Clause 7.1.5: Remove old and add new list of Certificate Policy Object Identifiers (OID).	Sonjann Fortune Du
2.0.6	Jan 2015	Amendments to: • Clause 4.1.2: Updated Certificate Application Requirements • Clause 7.1.2.1: Updated RSA Key Size • Clause 4.8.1 Added Key Recovery / Renewal Process and Requirements	Sonjann Fortune Du

2.0.7	Dec 2016	Amendments to: • Clause 3.1.9.1 : Added Domain Name Validation for SSL Certificate • Clause 3.1.9.5 : Details of Domain Name Validation Check • Clause 4.1.2 : Added SSL Certificate Type • Clause 4.8.1 : Added SSL Certificate Type • Clause 5.1.2.3 Update of Data Centre • Clause 5.1.3.2 Update of Data Centre • Clause 5.1.4.1 Update of Data Centre • Clause 7.1.5: Added new list of Certificate Policy Object Identifier (OID), Adobe Certificate and Netrust SSL	Sonjann Fortune Du
2.0.8	Aug 2019	Amendments to: • Clause 4.1.2 Update of ID Document • Clause 4.1.2.1 Update of document storage • Clause 7.1.5: Removal of Certificate Policy (OID) - Netrust Grid-ID Certificate	Kirti Raj
2.0.9	Mar 2020	New Clause: • 8.0.1 Personal Data Protection Policy	Kirti Raj
2.1.0	Feb 2021	Amendments to: • Clause 3.1.9.1 Authentication of Individually Identity • Clause 4.1.2 Face-to-Face application • Clause 4.8.1 Key Recovery / Renewal Process • Clause 7.1.5: Added new Certificate Policy Object Identifier (OID) – Enterprise Email	Kirti Raj

Contents

1 INTRODUCTION

1.1 Overview

1.1.1 Netrust Pte Ltd (henceforth referred to as "Netrust") in its capacity as a Certification Authority (CA) acts as a trusted third party to confirm that a public key belongs to a named entity. Such confirmation is expressly represented by a Netrust X.509 Version 3 Certificate (henceforth termed Certificate) - An issued Certificate is a statement by the CA that the Certificate is associated with the person or equipment uniquely named within that Certificate.

1.1.2 To support its CA role, Netrust has established the Netrust Public Certification Services Framework (the "Netrust PCS") to issue, manage, revoke and renew Certificates in accordance with the practices set out in this Certification Practice Statement ("CPS"). The Netrust PCS is designed to support secure electronic commerce and other general security services.

1.1.3 The Netrust CPS is a detailed statement of the practices and operational procedures of Netrust. It supports multiple Certificate Policies ("CP") that are implemented by Netrust. A 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. A Relying Party should use the applicable CP to guide him in deciding whether or not to rely upon any such Certificates for his particular purpose or transaction.

1.1.4 Each CP relevant to a Certificate is represented in the Certificate by a unique, registered Object Identifier. Netrust may implement various CPs from time to time. The textual specification of the CPS and CPs may be found at the Netrust web site at http://www.netrust.net or at such other places as may be determined by Netrust.

1.1.5 The Netrust CPS is (i) intended to be applicable to and is a legally binding document between Netrust, its Organization Registration Authority (ORA), the Sponsor, the Subscriber, the Relying Party and each of their agents, employees and contractors; and (ii) intended to serve as notice to all parties within the context of the Netrust PCS and parties within the Netrust PCS are required to understand and consult this CPS at all times during the lifetime of the Certificate of the Subscriber.

1.2 Identification

1.2.1 Netrust Pte Ltd is assigned an Object Identifier (OID) 1.2.702.0.1002 (in ASN.13 format) in accordance with the ISO Assignment of OID Component Value.

1.3 Community and Applicability

1.3.1 Certification Authority

1.3.1.1 Netrust is the CA that will create and sign the Certificate. These Certificates shall bind the public key of each Subscriber to each Subscriber's Certificate generated. Netrust will publish Certificate status through Certificate Revocation Lists (CRLs) and enforce the particular CP for each Certificate issued.

1.3.1.2 Netrust may perform cross certification with other CAs within and/or outside the Netrust PCS. Cross certification is a process performed by Netrust where Netrust reviews all applicable documentation, practices and procedures of other CAs. The Relying Party must also review all the applicable documentation, practices and procedures of the other CA if the Relying Party chooses to rely on any certificates issued by such CA. The process of cross certification does not in any way equate to an endorsement or approval of the other CA by Netrust.

1.3.2 Organization Registration Authority (ORA)

1.3.2.1 The authorized Netrust ORA shall carry out registration procedures for Subscribers in specific communities. These registration procedures are required, designed and approved by Netrust in accordance with the applicable CP, this CPS and the applicable ORA Agreement. An ORA shall provide to Netrust the name, identification and contact information (including postal, electronic addresses and phone numbers) of each Subscriber to be certified. The ORA shall utilize such information provided by the Subscriber to create such Subscriber's Certificate. An ORA may employ agent(s) to perform the registration functions and in which case the ORA shall be directly accountable for the activities of the agent(s) and the functions that the agent performs on behalf of the ORA. The actions, inactions and/or omissions of each agent shall be deemed to be the actions, inactions and/or omissions of the ORA.

1.3.2.2 An ORA may elect to be a Sponsor if an ORA fulfills the requirements and definitions of Sponsor as set out below. In such an event, the ORA shall be known as a "Sponsor ORA".

1.3.2.3 An ORA performing the functions of an ORA without any payment obligations as required of a Sponsor shall be known as a "Non-Sponsor ORA".

1.3.2.4 The term ORA shall mean collectively the Sponsor and Non-Sponsor ORA.

1.3.3 Sponsor

1.3.3.1 Sponsor shall be the parties who will be responsible for all payment obligations in relation to each Subscriber's Certificate they decide to sponsor. They shall be entitled to revoke these Sponsored Subscriber's Certificate as set out in the applicable CP and in Clause 4.4 of this CPS at the discretion of the Sponsor.

1.3.4 Subscriber

1.3.4.1 Subscriber shall include individuals, partnerships, corporations, application servers or such other categories of person or entities who is a holder of any Netrust Certificate.

1.3.4.2 Subscribers are classified into two categories of either (a) Sponsored Subscriber whose payment obligations have been undertaken by the applicable Sponsor in relation to the applicable Certificate; or (b) Paying Subscriber who shall be the party paying for the Certificate.

1.3.4.3 The term Subscriber shall mean collectively the Sponsored Subscriber and Paying Subscriber.

1.3.5 Relying Party

1.3.5.1 A recipient of a Subscriber's Certificate in the Netrust PCS who acts in reliance on that Certificate is a Relying Party.

1.3.5.2 A Relying Party must also be a Subscriber in the Netrust PCS to be able to enjoy any of the benefits, including the indemnities provided by Netrust (if any), of the Netrust PCS as set out in the CPS or applicable CP.

1.3.6 Applicability

1.3.6.1 Netrust Certificates are intended to be used to support the following core security needs:

- Authentication - provides assurance of the identity of the Subscriber;

- Message Integrity - ensures that the content of a message is intact and has not been altered in any way between the time of sending and its receipt; and

- Digital Signature - assist any Relying Party in preventing a Subscriber from denying that such Subscriber has authorized any particular transaction if that Subscriber has digitally signed that transaction. However Netrust does not warrant non-repudiation of any electronic communication or transaction as non-repudiation is determined exclusively by law and the applicable dispute resolution mechanism.

1.3.6.2 In addition, Netrust Certificate may be used to support confidentiality. Confidentiality ensures that the information exchanged between the sender and the recipient stays private and is not disclosed to any unauthorized party. Netrust shall not be responsible or liable in relation to such confidentiality features and Netrust disclaims all direct and indirect damages, losses or liabilities that arises out of or pursuant to any such use.

1.3.6.3 Netrust currently supports distinct Certificate classes within the Netrust PCS. The extent and scope of use of each class of Certificate and the restrictions relating to each class of Certificate are determined and set out in the respective CP. Each Certificate class is described and is further set out in the respective CP. All ORAs, Sponsors, Subscribers and Relying Parties are required to be familiar with the terms, conditions, requirements, recommendations and provisions of the applicable CP.

1.3.6.4 Currently, Netrust Certificates can be used in various e-commerce applications as set out in the examples at the Netrust web site at http://www.netrust.net. Subscribers and Relying Parties must independently assess and determine the appropriateness of each class of Certificate for any particular purpose.

1.3.6.5 Netrust shall not be responsible for any liabilities howsoever arising from the use of any Certificate unless Netrust has expressly undertaken to assume such liabilities contained in this CPS.

1.4 Contact Details

1.4.1 Specification Administration Organization

1.4.1.1 This Netrust CPS is published and administered by Netrust Pte Ltd, Singapore.

1.4.2 Contact Person

1.4.2.1 The contact person is:

The Operations Manager
Netrust Pte Ltd
70 Bendemeer Road
#05-03, Luzerne Building
Singapore 339940
Telephone: 62121-388
Fax: 62121-366
E-mail: infoline@netrust.net

1.4.3 Person Determining CPS Suitability for the Policy

1.4.3.1 The person determining CPS suitability for any CP is the Operations Manager of Netrust.

2 GENERAL PROVISIONS

2.1 Obligations

2.1.1 CA Obligations

2.1.1.1 Notwithstanding any other provisions to the contrary contained in this CPS, Netrust's obligations is to ensure:

- That the public key algorithm employed and deployed by Netrust is not compromised;
- That the Netrust CA's private signing key will be reasonably secured and safeguarded within the Netrust PCS in accordance with standard industry practice.

2.1.1.2 The provisions set out above in Clause 2.1.1.1 above shall be Netrust's sole and absolute obligations in relation to its capacity as a CA and nothing contained herein this CPS shall be deemed to or be construed so as to imply that Netrust will be obliged to perform any other functions, or be obliged to ensure that any other matters are carried out by Netrust, its servants, employees or agents.

2.1.1.3 For purposes of clarity, this CPS sets out the procedures by which Netrust observes in the Netrust PCS and the technology under which Netrust deploys to observe such services but all such procedures shall not be deemed to be obligations of Netrust to perform, adhere or comply with but are merely procedures by which Netrust operates on in its PCS. The only obligation by which Netrust is obliged to perform, adhere or comply with is set out above in Clause 2.1.1.1 above.

2.1.1.4 Netrust shall not be liable for any loss, damage or penalty resulting from delays or failures in performance resulting from acts of God or other causes beyond its control. For purposes of clarity, such events shall include, but without limitation to, strikes, or other labour disputes, riots, civil disturbances, actions or in actions of suppliers, acts of God, war, fire, explosion, earthquake, flood or other catastrophes.

2.1.1.5 In any of the events mentioned in Clause 2.1.1.4 hereof, Netrust shall for the duration of such event be relieved of any and all obligations, responsibilities and duties under this Clause 2.1.1,this CPS and the applicable CP, as is affected by the event.

2.1.2 ORA Obligations

2.1.2.1 The ORA is required to and shall comply with all registration procedures and safeguards as may be determined by Netrust and as set out in this CPS or the applicable ORA Agreement or as may be subsequently amended by Netrust.

2.1.2.2 The ORA is required to adhere to and comply with the provisions contained in this CPS specifically including but not limited to the provisions set out in Clause 3 (Identification and Authentication) below.

2.1.2.3 The ORA is only allowed permission to issue Certificates to the Subscribers but will not be allowed to suspend or revoke any Certificates in any circumstances.

2.1.3 Sponsor Obligations

2.1.3.1 The Sponsor is required to and shall ensure that all payment obligations shall be complied with and shall ensure that all payments in relation to each of the Certificate issued to each of the Sponsor's Subscriber are fully and completely made to Netrust in such manner as may be determined by Netrust.

2.1.4 Subscriber Obligations

2.1.4.1 All Subscribers are required to comply strictly with the following procedures in relation to the application of Certificate and in their safekeeping and possession of their private keys:

- All statements or information provided by the Subscriber in the Certificate application forms must be complete, accurate, true and correct in all respects and could be verified by Netrust or the ORA.

- That all physical security measures as may be described in this CPS or as may be applicable or recommended by Netrust are observed and complied with and to ensure the adequate and secured protection of the Subscriber's private keys;

- That the Subscriber are familiar with the provisions of this CPS and the CP in relation to their Certificate and be familiar with and adhere to the restrictions applicable to the use of the Subscriber's Certificate; and

- That the Subscriber shall promptly notify Netrust, or its applicable Sponsor/Sponsor ORA as the case may be, immediately upon the occurrence of any event that would lead to the compromise, including but not limited to loss of, misplacement or exposure, of the Subscriber's private keys.

2.1.5 Relying Party Obligations

2.1.5.1 All Relying Parties are required to ensure that the following provisions are adhered to when relying on any of the Certificate:

- That the Relying Party are familiar with the provisions of this CPS and the CP in relation to the Subscriber's Certificate and be familiar with and comply with the purposes for which the Certificate are used. Relying Party must ensure that the Subscriber's Certificate is used for its intended use only.

- That the Relying Party, when relying on the Subscriber's Certificate, are required to check the status of that Certificate against appropriate and current CRL in accordance to the CRL practice and procedure in Clause 4.4.

- That the Relying Party, when checking on the Subscriber's Certificate, are required to check on the validity of the Certificate before any reliance is made in relation to the Certificate.

2.1.5.2 All Relying Parties acknowledge that by relying on the Certificate, the Relying Party acknowledge that they are aware of the provisions herein contained in this CPS especially the provisions in relation to the disclaimers and limitation of liabilities as set out herein below in Clause 2.2 and 2.3.

2.1.6 Directory Obligations

2.1.6.1 Netrust publishes Subscriber's Certificates and CRLs in the Netrust Directory. This Directory is made available on the Internet and provides for 24 hours daily operations with 99.7% up-time in one calendar year.

2.1.6.2 Netrust will ensure within reasonable control that the downtime for the Directory will not exceed 30 minutes at any one time.

2.2 Liability

2.2.1 CA Liability

2.2.1.1 Warranties and Limitations on Warranties

NETRUST MAKES NO OTHER WARRANTIES EXPRESS OR IMPLIED AND HAVE NO FURTHER OBLIGATIONS UNDER THIS CPS AND EXCEPT AS EXPRESSLY PROVIDED IN THE FOREGOING, NETRUST DISCLAIMS ALL WARRANTIES AND OBLIGATIONS OF ANY TYPE, INCLUDING, BY WAY OF EXAMPLE AND NOT OF LIMITATION; (i) ANY WARRANTY OF MERCHANTABILITY; (ii) ANY WARRANTY OF FITNESS FOR A PARTICULAR PURPOSE; (iii) THAT THE USE OF THE CERTIFICATE OR ANY SOFTWARE PROVIDED AND/OR SUPPLIED HEREUNDER AND/OR PURSUANT TO THIS CPS WILL NOT INFRINGE ANY PATENT, COPYRIGHT OR TRADEMARK OR OTHER PROPRIETARY RIGHTS OF OTHERS; (iv) AND ANY WARRANTY OF THE ACCURACY OF INFORMATION PROVIDED, AND FURTHER DISCLAIM ANY AND ALL LIABILITY FOR NEGLIGENCE AND LACK OF REASONABLE CARE.

Netrust does not warrant the accuracy, authenticity, reliability, completeness, currentness, merchantability or fitness of purpose in relation to any information contained in Certificate or otherwise compiled, published or disseminated by or on behalf of Netrust and Netrust disclaims all liabilities for representations of information contained in a Certificate, and Netrust does not warrant "nonrepudiation" of signature on any electronic communication or transaction (as mentioned above in Clause 1.3.6 above).

2.2.1.2 Kinds of Damages Covered

Netrust shall not be liable for any loss or damage whatsoever or howsoever caused arising directly or indirectly in connection with the use or reliance on any Certificate by any parties.

Notwithstanding any other provisions to the contrary, Netrust is to and/or has expressly excluded liability for all indirect, special, incidental and consequential loss or damage, howsoever caused including without limitation, negligence, default or any acts of Netrust, its employees, agents, contractors, representatives, including but not limited to loss or damage to other equipment or property or for loss of profit, business, revenue, goodwill or anticipated savings pursuant to the use or reliance of any Certificate or any other transactions, services offered or contemplated by this CPS even if Netrust has been advised of the possibility of such damages. No action arising pursuant to the use or reliance of any Certificate, regardless of form, may be brought by any parties more than one (1) year after such cause of action has arisen.

2.2.1.3 Loss Limitations

Subject to the provisions of this clause, in the event that (i) any limitation or provision contained in this Agreement is held to be invalid for any reason; and (ii) Netrust breaches any of its obligations pursuant to Clause 2.1 above, and Netrust becomes liable for loss or damage that would otherwise have been excluded hereunder or excludable in law, (a) 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 currently at the level set out below for each Certificate within each of its class or such other applicable liability cap for such Certificate as may be further and/or subsequently amended by Netrust; and (b) Netrust shall only be liable for any such loss or damages if such loss or damage arose or is incurred during the paid subscription period.

This limitation on damages applies to loss and damages of all types, including but not limited to direct, compensatory, indirect, special, consequential, exemplary or incidental damages incurred by any person, including without limitation a Subscriber, an applicant, a recipient or a Relying Party that are

caused by reliance on or use of a Certificate Netrust issues, manages, uses, or revokes or such a Certificate that expires. This limitation on damages applies as well to liability under contract, tort and any other form of liability claim. The liability cap on each Certificate shall be the same regardless of the number of digital signatures, transactions or claims related to such Certificate. For each class of Certificate, the liability cap is stipulated in its respective CP. In the event that the liability cap is exceeded, the available liability cap shall be apportioned first to the earliest claims to achieve final dispute resolution, unless otherwise ordered by a court of competent jurisdiction. In no event shall Netrust be obligated to pay more than the aggregate liability cap for each Certificate, regardless of the method of apportionment among claimants to the amount of the liability cap.

2.2.1.4 Other Exclusions

Netrust's PCS are not designed, intended or authorized for use or resale as control equipment in hazardous circumstances or for uses requiring fail-safe performance such as the operation of nuclear facilities, aircraft navigation or communication systems, air traffic control systems or weapons control systems, where failure could lead directly to death, personal injury or severe environmental damage.

2.2.2 ORA Liability

2.2.2.1 The liabilities of the ORA are addressed in the appropriate and applicable ORA Agreement entered into between the applicable ORA and Netrust.

2.3 Financial Responsibility

2.3.1 Indemnification by Relying Party and Subscriber

2.3.1.1 Netrust shall be entitled to be indemnified from and against any and all loss, damage or liability and legal fees and costs incurred by Netrust in the event of or as a result of any act or default by any Relying Party making use of or relying on the Certificate or their agents and employees.

2.3.1.2 Without limiting other Subscriber obligations stated in this CPS, Subscribers are liable for any misrepresentations they make in Certificate or in their applications for Certificate to third parties who having verified one or more digital signatures with the Certificate, reasonably rely on the representations contained therein.

2.3.1.3 BY ACCEPTING A CERTIFICATE, THE SUBSCRIBER AGREES TO INDEMNIFY AND HOLD NETRUST, ITS ORA, THEIR AGENTS AND CONTRACTORS HARMLESS FROM ANY ACTS OR OMISSIONS RESULTING IN LIABILITY, ANY LOSS OR DAMAGE AND ANY SUITS AND EXPENSES OF ANY KIND, INCLUDING REASONABLE LEGAL FEES, THAT NETRUST, ITS ORA, THEIR AGENTS AND CONTRACTORS MAY INCUR, THAT ARE CAUSED BY THE USE OR PUBLICATION OF A CERTIFICATE AND THAT ARISES FROM (i) FALSEHOOD OR MISREPRESENTATION OF FACT BY THE SUBSCRIBER (OR A PERSON ACTING UPON INSTRUCTIONS FROM ANYONE AUTHORISED BY THE SUBSCRIBER); (ii) FAILURE BY THE SUBSCRIBER TO DISCLOSE A MATERIAL FACT, IF THE MISREPRESENTATION OR OMISSION WAS MADE NEGLIGENTLY OR WITH INTENT TO DECEIVE NETRUST, ITS ORA, THEIR AGENTS AND CONTRACTORS OR ANY PERSON RECEIVING OR RELYING ON THE CERTIFICATE, OR (iii) FAILURE TO PROTECT THE SUBSCRIBER'S PRIVATE KEY, TO USE A TRUSTWORTHY SYSTEM, OR TO OTHERWISE TAKE THE PRECAUTIONS NECESSARY TO PREVENT THE COMPROMISE, LOSS, DISCLOSURE, MODIFICATION OR UNAUTHORISED USE OF THE SUBSCRIBER'S PRIVATE KEY.

2.3.1.4 When a Certificate is issued by the request of a Subscriber's agent, both the agent and the Subscriber shall jointly and severally indemnify Netrust, its ORA, their agents and contractors pursuant

to this CPS. The Subscriber has a continuing duty to notify the issuer of any misrepresentations and omissions made by an agent.

2.3.2 Fiduciary Relationships

2.3.2.1 Netrust and ORA are not the agents, fiduciaries, trustees or other representatives of Subscriber or Relying Party. The relationship between Netrust and Subscriber and that between Netrust and Relying Party are not that of agent and principal. Neither Subscriber nor Relying Party have any authority to bind Netrust, by contract or otherwise, to any obligation. Netrust does not make any representations to the contrary, either expressly, implicitly, by appearance or otherwise.

2.3.3 Administrative Processes

2.3.3.1 Administrative procedures (such as accounts and annual report) maybe published yearly in accordance with the laws of the Republic of Singapore.

2.4 Interpretation and Enforcement

In the event of any conflict or inconsistencies between this CPS and other rules, guidelines or contracts, the provisions herein this CPS shall prevail over such other rules, guidelines or contracts, except as to other contracts either (i) predating the first public release of the CPS; or (ii) expressly superseding this CPS for which such contract shall govern as to the parties thereto and except to the extent that the provisions of this CPS are prohibited by law.

2.4.1 Governing Law

2.4.1.1 This CPS shall be governed by and construed in all respects in accordance with the laws of the Republic of Singapore.

2.4.2 Severability, Survival, Merger, Notice

2.4.2.1 In the event that any or any part of the terms, conditions or provisions contained in this CPS are determined invalid, unlawful or unenforceable to any extent such term, condition or provision shall be severed from the remaining terms, conditions and provisions which shall continue to be valid and enforceable to the fullest extent permitted by the Governing Law.

2.4.2.2 This CPS shall supersede any and all previous negotiations, agreements, memoranda and commitments in relation to the subject matter. Netrust shall be entitled to amend, modify and change any of the terms, conditions or provisions herein contained at any time and without prior notice to any parties. Netrust shall be entitled to place and/or publish amendments in the Netrust repository either (i) in the form of an amended version of the CPS; (ii) in the Netrust website at http://www.netrust.net; (iii) in such other manner as may be determined by Netrust. All amendments, modification and changes shall, unless otherwise expressly stated in such amendments, modification and changes be effective immediately upon placement and/or publication. The subscriber's decision not to request revocation of his Certificate within fifteen (15) days following such placement and/or publication shall constitute agreement to the amendments, modification and changes.

2.4.2.3 Netrust's failure or forbearance to enforce any right or claim against any party arising hereunder shall not be deemed to be a waiver by Netrust to such right or claim. Any of Netrust's waiver of a breach of any provision of this CPS shall not operate or be construed as a waiver of any subsequent breach or breaches of the same or any other provision.

2.4.2.4 Any notice required or permitted to be given to a Subscriber shall be in writing and shall in the case of a recipient being (i) a company be sent to its registered office from time to time; (ii) an individual be sent to its address as set out in its application. Any such notice shall be delivered personally or sent in a letter by the recorded delivery service and shall be deemed to have been served if by personal delivery when delivered and if by recorded delivery 48 hours after posting. If Netrust so elects, Netrust shall be entitled to send any such notice to the Subscriber via electronic mail ("e-mail") to the e-mail address designated by the Subscriber at the time of application for the Certificate.

2.4.2.5 Any notice required or permitted to be given to Netrust shall be in writing and shall be sent to its registered office from time to time. Any such notice shall be delivered personally or sent in a letter by the recorded delivery service and shall be deemed to have been served if by personal delivery when delivered and if by recorded delivery 24 hours after receipt by Netrust. Any such notice may be sent to Netrust via electronic mail ("e-mail") and such notices shall only be deemed to be valid if such e-mail notices are confirmed in writing by the Subscriber to Netrust within 24 hours of the receipt of the e-mail notice by Netrust.

2.4.2.6 Each of the Certificate and all the terms and provisions of this CPS are personal to each of the Subscriber and the Subscriber shall not assign their Certificate to any other parties.

2.4.2.7 The headings contained in this CPS are inserted for convenience of reference only and are not intended to be part of or to affect the meaning or interpretation of any of the terms, conditions or provisions of this CPS.

2.4.2.8 Export of certain software used in conjunction with Netrust's PCS may require the approval of appropriate Netrust and/or government authorities. All parties shall conform to applicable export laws and regulations as may or may not have been advised by Netrust.

2.4.3 Dispute Resolution Procedures

2.4.3.1 All questions or differences whatsoever which may at any time hereafter arise hereto touching or concerning the CPS or its construction or effect or as to the rights, duties or liabilities of the parties hereunder under or by virtue of this CPS or otherwise as to any other matter connected with or arising out of or in relation to the subject matter of this CPS shall if such questions disputes or differences cannot be amicably resolved by the parties, be referred to arbitration in Singapore in accordance with the Arbitration Rules of the Singapore International Arbitration Centre ("SIAC Rules") for the time being in force which rules are deemed to be incorporated by reference into this CPS. The arbitrators' decision shall be final and binding upon the parties and shall provide the sole and exclusive remedies of the parties. All arbitration proceedings shall be in the English language and judgment upon the award so rendered may be entered in any court having jurisdiction or application may be made to such court for a judicial acceptance of the award or orders of enforcement.

2.5 Fees

2.5.1 Netrust charges Subscribers and all such other parties for their use of Netrust's PCS and all Subscribers and all such other parties shall be obliged to pay to Netrust such charges in accordance with its Schedule of Fees and at such times as may be prescribed by Netrust.

2.5.2 All fees are subject to change seven (7) days following their posting in the Netrust web site at http://www.netrust.net or as may be notified by Netrust in any other manner. The fees Netrust charges include:

2.5.2.1 Certificate Subscription or Renewal Fees - refer to Netrust for Schedule of Fees.

2.5.2.2 Certificate Revocation Fees - refer to Netrust for Schedule of Fees.

2.5.2.3 Fees for Other Services such as Policy Information - Schedule of Fees to be determined.

2.5.2.4 Refund Policy - Netrust has a policy where no monies will be refunded under any circumstances whatsoever.

2.6 Publication and Directory

2.6.1 Publication of CA Information

2.6.1.1 Netrust publishes Netrust related information on its web site.

2.6.2 Frequency of Publication

2.6.2.1 Information, once published on the Netrust web site, will remain accessible on the web site until a new version is made available. It is the sole discretion of Netrust to make available older versions of publications on the web site.

2.6.2.2 Netrust, where appropriate may implement access control to certain Netrust-related publication as may be determined by Netrust such that only Subscribers to the Netrust PCS are granted the privilege to read these publications.

2.6.2.3 Netrust also implements access control and/or security measures such that only authorized Netrust personnel can write or modify the online version of the Netrust publications.

2.6.3 Directory

2.6.3.1 Subject to the provisions of Clause 2.1.1 above, Netrust shall:

- Publish a copy of the Subscriber Certificate upon the Subscriber's acceptance of the Certificate, and revocation data in such manner and at such times as it deems fit but sufficiently such that Relying Party will be able to access such information in the Netrust Directory;

- Make reasonable efforts to publish any changes, amendments and modifications to any published information in the Netrust Directory and shall endeavour to keep all published information in such Directory updated.

2.7 Compliance Audit

2.7.1 Frequency of Netrust Compliance Audit

2.7.1.1 Netrust will conduct a compliance audit of all its procedures and practices as set out here in this CPS and the appropriate CP at such frequency as may be determined by Netrust or as may be required under the Governing Law.

2.7.1.2 Netrust will submit the compliance audit report to the Controller of Certificate Authority in Singapore within four weeks of the completion of the audit.

2.7.2 Identity/Qualifications of Auditors

2.7.2.1 An auditor performing the Netrust compliance audit will have such qualifications and experience that conforms to the Governing Law and industry practice including the following qualifications:

- Be a licensed certified public accountant (CPA) or a commercial licensed evaluation facilities (CLEFs), as may be applicable and required by the Governing Law and industry practice, in good standing.
- Has knowledge of trusted computer information systems, telecommunications networking environments, PKI technology, standards and practices.
- Has knowledge of professional audit techniques to test the systems.

2.7.3 Auditor's Relationship to Audited Party

2.7.3.1 The auditor appointed by Netrust or the regulatory government body must be an entity independent of any control of Netrust.

2.7.4 Topics Covered by Audit

2.7.4.1 The Netrust compliance audit will establish that:

- All requirements of the CP supported by Netrust are sufficiently addressed in this CPS including the technical, procedural and personnel policies and practices of Netrust.
- Netrust implements those technical, procedural and personnel policies and practices.

2.7.5 Actions Taken as a Result of Deficiency

2.7.5.1 If irregularities are found, Netrust will prepare a report as to any action it will take in response to the audit report. Based on the severity of the irregularities, Netrust will carry out corrections of problems in a most expeditious manner and in accordance with generally accepted international practice and the Governing Law.

2.7.6 Communications of Results

2.7.6.1 The Netrust compliance audit results will not be made public unless required by law. Where appropriate, the method and detail of notification of audit results to Netrust partners (i.e. Sponsor, ORA) will be defined within respective agreements between Netrust and the other party.

2.8 Confidentiality

2.8.1 Types of Information to be Kept Confidential

2.8.1.1 The types of information Netrust will keep confidential include agreements, correspondence and business arrangement with its Sponsor, ORA, and Subscriber. These information are considered sensitive and shall not be disclosed without prior consent of the other respective party, unless required by law.

2.8.1.2 Any disclosure of subscriber-specific information by Netrust or ORA must be authorized by the Subscriber as defined in 1.3.4.

2.8.1.3 The Subscriber's private keys are to be kept secret by the Subscriber. Disclosure of these keys by the Subscriber is at Subscriber's own risk.

2.8.1.4 Audit results and information are considered sensitive and will not be disclosed to anyone other than Netrust authorized and trusted personnel. These information will not be used for any purpose other than audit purposes or where required by law.

2.8.1.5 Information pertaining to Netrust CA operations shall only be disclosed to Netrust authorized personnel on a need-to-know basis.

2.8.1.6 Netrust is not and shall not be obliged to disclose any information pertaining to management of Subscriber's Certificates unless expressly required by law.

2.8.2 Types of Information Not Considered Confidential

2.8.2.1 Notwithstanding any other provisions to the contrary all information revealed to Netrust and the ORA in the application forms are considered and shall be deemed to be not of a confidential nature and Netrust and its ORA shall be allowed to make use of all such information in such manner as would be required by Netrust and/or the ORA in the conduct of Netrust's or the ORA's business, including without limitation the right to disseminate the aforesaid information to any third party.

2.8.2.2 The types of information that are not considered confidential includes information related to Subscriber's Certificate. Personal or corporate information that appear in public directories or web sites are also not considered confidential.

2.8.3 Disclosure of Certificate Revocation/Suspension Information

2.8.3.1 Netrust publishes the Certificate revocation information in the Netrust Directory.

2.8.4 Release to Law Enforcement Officials

2.8.4.1 In the event that Netrust is required under any provision of any rules, regulations or statutory provisions or by any order of court to release any information that is deemed to be or construed to be of a confidential nature under this CPS, Netrust shall be at liberty to release all such information required to be disclosed under any provision of any said rules, regulations or statutory provisions or by any order of court without any liabilities and any such release shall not be construed as or be deemed to be a breach of any obligations or requirements of confidentiality.

2.8.5 Release as Part of Civil Discovery

2.8.5.1 In the event that Netrust is required, pursuant to any suit or legal proceedings initiated by itself or otherwise, under any provision of any rules, regulations or statutory provisions or by any order of court to release any information that is deemed to be or construed to be of a confidential nature under this CPS, Netrust shall be at liberty to release all such information required to be disclosed under any provision of any said rules, regulations or statutory provisions or by any order of court without any liabilities and any such release shall not be construed as or be deemed to be a breach of any obligations or requirements of confidentiality.

2.8.6 Disclosure Upon Owner's Request

2.8.6.1 In the event that the owner of any confidential information requests that Netrust reveal or disclose any confidential information owned by the said owner for any reasons whatsoever, Netrust shall only do so if it forms the opinion that the release of any such information will not result in the

incurrence of any liability on any other party and Netrust shall not be liable for any damages or losses arising out of any such revelation or disclosure of such confidential information and the owner of the confidential information shall indemnify Netrust for any and all liabilities, damages, losses or any and all such liabilities arising out of or pursuant to any such revelation or disclosure of such confidential information.

2.8.7 Other Information Release Circumstances

2.8.7.1 Any and all such other information may be released by Netrust upon such times and under such circumstances as Netrust may at its sole option determine.

2.9 Intellectual Property Rights

2.9.1 Netrust shall retain sole and exclusive ownership of all right, title and/or interest in and to the Certificate and all software supplied by Netrust. Netrust shall be entitled to continue using the Certificate and all software supplied in whatever form, manner or model it so elects.

2.9.2 All parties are to acknowledge that any and all of the copyrights, trademarks and other intellectual property rights used or embodied in or in connection with any and all Certificate issued and all software supplied by Netrust pursuant to this CPS, including all documentation and manuals relating thereto, is and shall remain the property of Netrust and the parties shall not during or at any time after the revocation, expiry or suspension of any of their Certificate in any way question or dispute the ownership or any other such rights of Netrust.

2.9.3 The parties also acknowledge that such trademarks, copyrights and other rights in the Certificate belongs to Netrust and/or that Netrust has the authority to use all such trademarks, copyrights and all such other rights and shall not be used by the parties unless with the express written consent of Netrust. Upon the termination, revocation, or expiry of any Certificate, the parties shall forthwith discontinue such use, without receipt of compensation for such discontinuation and the parties shall deliver unto Netrust any and all copies of the Certificate and software supplied by Netrust that it has in its possession or shall at the request of Netrust destroy any and all copies of the Certificate and software supplied by Netrust that it has in its possession and shall render unto Netrust a certification that the parties has so duly done so.

2.9.4 The parties shall not, during or after the expiry, revocation, or termination of any Certificate, without the prior written consent of Netrust, use or adopt any name, trade name, trading style or commercial designation that includes or is similar to or may be mistaken for the whole or any part of any trademark, trade name, trading style or commercial designation used by Netrust.

3 IDENTIFICATION AND AUTHENTICATION

3.1 Initial Registration

3.1.1 Types of Names

3.1.1.1 Each Subscriber will be represented by a clearly distinguishable and unique X.509 Distinguished Name (DN) in the Certificate subject name field and in accordance with PKIX Part 1.

3.1.1.2 Each Entity may use an alternative name via the Subject Alternate Name field, which will be in accordance with PKIX Part 1.

3.1.1.3 The DN may be in the form of a X.509 printable String or in such other form but will not be blank.

3.1.2 Need for Names to be Meaningful

3.1.2.1 The contents of each Certificate Subject and Issuer name fields may have an association with the authenticated name of the Subscriber.

3.1.2.2 In the case of individuals Relative Distinguished Name (RDN) should be a combination of first name, surname, and optionally initials.

3.1.2.3 This RDN may also include an organizational position or role.

3.1.2.4 In the case of other entities the RDN shall reflect the authenticated legal name of the Subscriber.

3.1.2.5 If a Certificate refers to a role or position, the Certificate may also contain the identity of the person who holds that role or position.

3.1.3 Rules for Interpreting Various Name Forms (Not applicable)

3.1.4 Uniqueness of Names

3.1.4.1 DN must be unique for all Subscribers of the Netrust PCS. Netrust adopts the Unique Identifier such that Subscribers with identical names can be supported in the Netrust PCS.

3.1.5 Name Claim Dispute Resolution Procedure

3.1.5.1 In the event of any disputes concerning name claim issues, Netrust reserves the right to make all decisions and shall be the final arbiter of all such claims in relation to Subscriber names in all assigned Certificate. A party requesting a Certificate must demonstrate its right to use a particular name. Netrust will have the right to reject any name in its sole and absolute discretion.

3.1.6 Recognition, authentication and role of trademarks

3.1.6.1 The use of trademarks will be reserved to registered trademark holders and proper documentary proof of such ownership must be produced to Netrust.

3.1.7 Method to prove possession of subscriber's private key

3.1.7.1 The Netrust PCS provides a set of Setup Information for the Subscriber at the initial stage of registration. This Setup Information is subsequently used by the Subscriber to confirm with Netrust PCS that he/she is the rightful owner of the private key(s). The Setup Information, typically, is distributed to the owner via an out-of-band manner securely.

3.1.8 Authentication of Organization Identity

3.1.8.1 An application for an organization/organization representative/application server to be a Subscriber must be made by an individual authorized to act on behalf of the prospective Subscriber. Netrust or the applicable ORA will perform the face-to-face authentication of the Subscriber.

3.1.8.2 Identification and authentication of the prospective Subscriber must be through one of the following means:

- Netrust or the ORA must examine copies of documentation, duly certified by such persons recognized by Netrust, providing evidence of the existence of the organization;

- If Netrust or the ORA has previously established the identity of an individual, then Netrust or the ORA shall be entitled to rely on such initial verification and utilize this privately shared information.

3.1.8.3 Netrust or the ORA will also verify the identity and authority, including any and all letters of authorization, of the individual acting on behalf of the prospective Subscriber and their authority to receive the keys on behalf of that organization.

3.1.8.4 Netrust or the ORA will keep a record of the Subscriber's information as detailed in the Subscriber's application form.

3.1.9 Authentication of Individual Identity

3.1.9.1 The process of identification of a Subscriber will differ based on the class of Certificate that the Subscriber is applying for and may be via either (a) e-mail validity; (b) reliable information database (c) face-to-face verification either digitally or physically (d) domain name and ownership validation. The applicable CP sets out the process of identification for each class of Certificate. An application for a Certificate must be made (i) personally by an individual, (ii) by the duly authorized representative of the Subscriber (ORA).

3.1.9.2 For e-mail validation, identification and authentication of the individual will be done by checking and verifying that the e-mail address of the Subscriber does in fact exist.

3.1.9.3 For reliable information database, identification and authentication of the individual will be done by checking and verifying an existing database in which such necessary particulars of the individual has been stored. Such a database may be a third party database of an existing Netrust database.

3.1.9.4 For face-to-face, identification and authentication of the individual must be through one of the following means:

- Netrust or the ORA will compare the identity of the individual with two pieces of identification (photocopies and originals). The identification document must be a government-issued identification either physical document or via MyInfo SingPass; or

- If Netrust or ORA has previously established the identity of an individual, then Netrust or ORA shall be entitled to rely on such initial verification and utilize this privately shared information.

3.1.9.5 Domain name and ownership validation verification involves checking the Applicant/Entity is a registered holder or has exclusive control of the domain name to be included in the certificate name in which the following will be checked

- Verify the Applicant's legal existence and identity
- Verify the Applicant's physical existence (business presence at a physical address)
- Verify the Applicant's operational existence or business registration (business activity)

3.1.9.6 Netrust or the ORA will record the Subscriber's information as detailed in the Subscriber's application form.

3.2 Routine Renewal

3.2.1 One month prior to the expiry of each Certificate, Netrust will send a subscription renewal notice, and any applicable set-up information, to the applicable Paying Subscriber or Sponsor. Renewal notices may be sent by Netrust via mail or e-mail in accordance with the provisions of Clause 2.4.2.5 above.

3.2.2 The Paying Subscriber or Sponsor may choose to renew the subscription period by the payment of the requisite subscription or renewal fees to Netrust.

3.2.3 Only (i) the Paying Subscriber, (ii) Sponsor; or (iii) any other parties duly authorized by either the Paying Subscriber or the Sponsor, may renew the applicable subscription.

3.3 Renewal after Revocation

3.3.1 In the event of any suspected key compromise, the Certificate issued must be revoked. It is the responsibility of that Subscriber to notify Netrust or the relevant ORA who issued the Certificate immediately upon such suspicion. The process of renewals carried out by Netrust or the relevant ORA after such revocation will be in the same manner as the initial registration. Any change in any information contained in a Certificate will have to be re-certified by Netrust or the relevant ORA before any Certificate is issued.

3.4 Revocation Request

3.4.1 Netrust or its ORA will verify any request for revocation for a Certificate. The procedures for processing any revocation request and the means by which its validity is established will be stipulated in Clause 4.4.2.

3.4.2 All revocation requests will be logged by Netrust or its ORA as the case may be.

4 OPERATIONAL REQUIREMENTS

4.1 Certificate Application

4.1.1 Netrust PCS supports both face-to-face and online Certificate applications. The application process differs for different Netrust Certificate classes, and it adheres and conforms to the procedures as set out by the respective CP.

4.1.2 For face-to-face application which requires verification either digitally or physically, Netrust requires the applicant to:

- Submit by way of email, an application form properly filled and signed. The form must include the Netrust Subscriber Agreement.

- Provide identification supporting documents such as:

Subscriber Category	ID Document
Personal • Singaporean • Singapore Permanent Resident (PR) • Other Foreigners	 • NRIC (pink) • NRIC (blue) • SingPass - MyInfo • Government issued identity (e.g. Employment Pass) or Passport
Corporate Individual	Letter of authorization, applicant's governing bodies' consent (if applicable) and applicant's identification document as stated above including such other types of documents as may be required by Netrust from time to time. (Netrust will verify the Company's Proof of Existence)
Organization	Letter of authorization detailing the appointment for which the certificate is to be issued and the current holder of that appointment and applicant's identification document as stated above including such other types of documents as may be required by Netrust from time to time. (Netrust will verify the Company's Proof of Existence)
Application Server	Same as above and ownership of server domain name, where applicable
Secure Socket Layer Certificate (SSL)	Same as above and ownership of domain name except that a face to face verification is not required after all checks and validations are completed

4.1.2.1 Completed application forms and photocopies of relevant supporting documents are stored in an encrypted server and archived for a period of seven years or until such time when the applicant's subscription with Netrust is invalidated, whichever is longer.

4.1.2.2 Netrust or its ORA are responsible to ensure that the verification of the applicant's identity is duly performed. The verifier's name, designation, signature and date of which the verification is performed are recorded for accountability and audit purpose.

4.2 Certificate Issuance

4.2.1 During the Certificate issuance process, the applicant will be issued with a digital certificate or through a set of secret codes used to generate on their end or enrolled in a cryptographic device

4.2.2 Netrust or its ORA issues the set of unique codes to the applicant only if the following conditions are met:

Respective Certificate application procedures as stated above are adhered to;

- Payment is made by Paying Subscriber himself or made by the respective Sponsor of the Sponsored Subscriber; and
- Netrust or its ORA approves the application.

4.2.3 The method of issuing the set of unique codes differs for different Netrust Certificate classes, and it adheres and conforms to the procedures as set out below:

- For all Netrust Certificates, the codes are issued to the applicant in a secure manner, e.g. printed in pin mailer, hand-delivered to the applicant in person, or sent via encrypted email.
- For Test Certificates, no codes will be issued. Test Certificates are issued directly to the applicant.

4.2.4 Upon receipt of the set of unique codes, the applicant may proceed to perform Certificate generation. The Certificate generation process uses Netrust authorized software and it involves the following steps:

- Netrust authorized software generates the Subscriber's signing key pair and sends a public verification key to the Netrust CM for certification. This is communicated securely via the Internet using the shared secret, i.e. the set unique codes previously issued to the applicant. Alternatively, Netrust PCS also supports PKCS#10 Certificate requests standards.
- Netrust CM validates the authenticity of the certification request and upon validation, creates the Subscriber's verification Certificate.
- Where applicable, Netrust CM creates the Subscriber's encryption key pair and encryption Certificate.

4.3 Certificate Acceptance

Netrust PCS supports various Certificate acceptance processes for different Netrust Certificate classes, and it adheres and conforms to the procedures as set out by the respective CP.

4.3.1 Procedures for Certificate Acceptance

Netrust requires that all Certificate acceptances to be formally acknowledged by the Subscriber on the agreement after the CA or ORA has issued the Certificate.

4.4 Certificate Revocation

4.4.1 Circumstances for Revocation

4.4.1.1 A Certificate must be revoked in any of the following circumstances (including but not limited to):

- The key pairs are replaced by a new set.
- The private key corresponding to the public key in that Certificate has been compromised.
- There is an affiliation change where information in the Certificate has changed.
- There is a cessation of operation where that Certificate is no longer needed for its original purpose.
- The payment for Certificate renewal is not received.
- The Subscriber has breached or failed to meet his obligations under this CPS, or any other agreement, regulation or law that may be in force.
- The Subscriber does not belong to the community of which he is a member of that is subject to the certificate policy. (e.g. due to death or termination of employment)
- A revocation request is made by the Subscriber.
- Netrust is of the opinion that the Certificate was not issued in accordance to the CPS.
- The certification key of Netrust has been compromised or cessation of Netrust's operations as a certificate authority.
- Any other circumstances as may be determined by Netrust from time to time or in accordance with any requirements, rules or regulations of the governing law.

4.4.1.2 Netrust is under no obligations to disclose the reason for revocation.

4.4.2 Who Can Request Revocation

4.4.2.1 The revocation request can only be made by:

- The Paying Subscriber whose name the Certificate has been issued in.
- The Sponsor or Sponsor ORA.
- The duly authorized representative of the Subscriber.
- Authorized personnel of Netrust or Non-Sponsor ORA when the Paying or Sponsored Subscriber has breached the agreement, regulation or law that may be in force.

4.4.3 Procedure for Revocation Request

4.4.3.1 The Netrust PCS supports different procedures for revocation request in accordance with the procedures as set out in the "Loss and Replacement" provisions in the respective CP. These include:

- Revocation request is made in person

- Revocation request is made via fax/email or phone where stringent checks are incorporated to ensure the requester is indeed the authorized personnel as stated in 4.4.2. 4.4.3.2 Netrust or its ORA who execute the revocation requests must ensure that the verification of the requester's identity and authority are duly performed. The verifier's name, designation, signature and date of which the verification and revocation are performed are recorded for accountability and audit purpose.

4.4.3.3 Netrust requires that the revocation requester submit a “Netrust Certificate Management Request Form” in addition with the supporting documents as defined in 4.1.2 in order for Netrust or its ORA to verify and execute the revocation request.

4.4.4 Revocation Request Grace Period

4.4.4.1 Netrust PCS provides various revocation request Grace Period in accordance with the procedures as follows. These include:

- For all Netrust Certificates, the revocation action must be initiated immediately within 24 hours receipt of the revocation request received on a business day and updated to the CRL immediately upon request of the Subscriber**.** All other revocations will be initiated within forty-eight hours upon receipt of the revocation request.

- For Test Certificates, the revocation action must be initiated within forty-eight hours of receipt of the revocation request.

4.4.4.2 Subject to the provisions of Clause 2.4.2.4 above, Netrust will notify the Subscriber of the revocation action via fax, email or phone within forty-eight hours of such revocation in a notice including details like date, time and reason for revocation.

4.4.5 Circumstances for Suspension

4.4.5.1 A certificate can be suspended based on the following reasons:

- The Certificate does not contain valid information.

- The Certificate during issuance was provided with misleading and untrue information.

- The private key corresponding to the public key in that Certificate is suspected of being compromised.

- The payment for Certificate renewal is not received within thirty (30) days after the expiry of the Certificate.

4.4.6 Who Can Request Suspension

4.4.6.1 The suspension request can only be made by:

- The Paying Subscriber whose name the Certificate has been issued in.

- The Sponsor or Sponsor ORA.

- The duly authorized representative of the Subscriber.

- Authorized personnel of Netrust or Non-Sponsor ORA when the Paying or Sponsored Subscriber has breached the agreement, regulation or law that may be in force.

4.4.7 Procedure for Suspension Request

4.4.7.1 The Netrust PCS supports different procedures for suspension request in accordance to the procedures as set out in the "Loss and Replacement" provisions in the respective CP. These include:

- Suspension request is made in person
- Suspension request is made via fax or phone where stringent checks are incorporated to ensure the requester is indeed the authorized personnel as stated in 4.4.6.

4.4.7.2 Netrust or its ORA who execute the suspension requests must ensure that the verification of the requester's identity and authority are duly performed. The verifier's name, designation, signature and date of which the verification and suspension are performed are recorded for accountability and audit purpose.

4.4.7.3 Netrust requires that the suspension requestor submit a “Netrust Certificate Management Request Form” in addition with the supporting documents as defined in 4.1.2 in order for Netrust or its ORA to verify and execute the suspension request.

4.4.8 Limits on Suspension Period

4.4.8.1 The suspension period will be one month from the receipt of the suspension request. Any further extension of this limit will be subjected to Netrust's discretion.

4.4.9 CRL Issuance Frequency

4.4.9.1 Netrust updates and publishes the Certificate Revocation List (CRL) every forty-eight hours. It is the responsibility of the Relying Party to ensure that the Certificate in use is validated against the updated CRL published by Netrust.

4.4.10 CRL Checking Requirements

4.4.10.1 The Relying Party is strongly advised to (i) check the status of Certificate against the up-todate CRL published by Netrust prior to their use; (ii) verify the authenticity and integrity of the CRL to ensure that it is issued and digitally signed by Netrust CA.

4.4.10.2 Netrust updates and publishes the Certificate Revocation List (CRL) every forty-eight hours upon any revocation requests made. It is the sole responsibility of the Relying Party to ensure that the Certificate in use is validated against the updated CRL published by Netrust.

4.4.11 On-line Revocation/Status Checking Availability (Not applicable)

4.4.12 On-line Revocation Checking Requirements (Not applicable)

4.4.13 Other Forms of Revocation Advertisements Available (Not applicable)

4.4.14 Checking Requirements for Other Forms of Revocation Advertisements (Not applicable)

4.4.15 Special Requirements Key Compromise

4.4.15.1 All revocation requests are processed in accordance with the operational requirements as stated in Clauses 4.4.1 through 4.4.4. There is no special requirement needed when the Certificate is revoked due to key compromise.

4.5 Security Audit Procedures

4.5.1 Types of event recorded

4.5.1.1 Netrust maintains audit logs for all system related matters. The logs, whether manual or electronic, will contain the date and time of the event, and the identity of the entity which caused the event.

4.5.1.2 Netrust also maintains audit logs for non-system related matters, e.g. physical access logs, personnel changes.

4.5.2 Frequency of Processing Log

4.5.2.1 Netrust reviews audit logs at least once every week and actions taken from these reviews are documented for accountability and audit purposes.

4.5.3 Retention Period for Audit Log

4.5.3.1 Netrust retains its audit logs on-site for at least two months and subsequently archives them off-site for a minimum of seven years.

4.5.4 Protection of Audit Log

4.5.4.1 Netrust implements strict access controls to ensure that only Netrust authorized personnel can access these audit logs. These logs are protected from unauthorized viewing, modification and deletion.

4.5.5 Audit Log Backup Procedures

4.5.5.1 Netrust ensures that all audit logs and audit summaries are backed up in accordance to Netrust backup standards and procedures. These include daily, weekly, monthly and yearly backup, as well as on-site and off-site backup facilities.

4.5.6 Audit Collection System (Internal vs External)

4.5.6.1 The Netrust CPS audit collection systems include:

- The Certificate management system
- The Certificate directory system
- The remote access system
- The firewall system
- The Intrusion Detection System (IDS)
- Network Monitoring Tools

4.5.6.2 Netrust is constantly reviewing other system management and auditing tools. Where appropriate, these systems will be implemented to support the audit requirements.

4.5.7 Notification to Event-Causing Subject

4.5.7.1 The decision to notify the event-causing subject is at the sole discretion of Netrust. Netrust is not obliged to notify the person or system or application if they caused an event that was logged by the Netrust PCS audit systems.

4.5.8 Vulnerability assessments

4.5.8.1 Netrust will conduct a system audit to monitor systems vulnerability at such periods as may be determined by Netrust. Where necessary, vulnerability assessments will be performed and reviewed based on the audit results/recommendation.

4.6 Records Archival

4.6.1 Types of Events Recorded

4.6.1.1 Netrust will archive the CA databases that consist of Certificate and CRLs it issues and the Subscriber's encryption private key at such periods as may be determined by Netrust. It will also archive audit logs and information used for identification and authentication purpose.

4.6.2 Retention Period for Archive

4.6.2.1 The retention period of archive in Netrust PCS is typically seven years unless otherwise stated.

4.6.3 Protection of Archive

4.6.3.1 The archives are protected at a level of physical security where only authorized personnel can access them. They are also protected from environmental threats such as temperature, humidity and magnetism.

4.6.4 Archive Backup Procedures

4.6.4.1 Currently, all archived materials are stored at off-site locations with similar protection stated in Clause 4.6.3.

4.6.5 Requirement for Time-Stamping of Records

4.6.5.1 All archived materials stated in Clause 4.6.1 shall be time-stamped unless otherwise stated.

4.6.6 Archive Collection System (Internal or External)

4.6.6.1 The archive collection system in Netrust PCS is manually performed.

4.6.7 Procedures to Obtain and Verify Archive Information

4.6.7.1 Netrust will verify the integrity of archived information on a yearly basis. Detailed procedures are being documented in the Netrust Standards and Procedures Specifications.

4.7 Key Changeover

4.7.1 Automated key changeover is permitted in Netrust PCS. A Subscriber or a Sponsor may apply to initiate this process.

4.8 Key Recovery / Key Renewal

4.8.1 Key Recovery or certificate recovery is required if the certificate password was locked or has expired. The Subscriber or ORA is required to furnish the following documents and Netrust will require a face-to-face verification either digitally or physically.

Certificate Type	Required Documents
Net ID Certificates ➢ Personal ➢ Corporate	• Users NRIC / Passport / Government issued ID for Foreigners • Change Management Request Form • Letter of authorization if by way of proxy
• Organization ID Certificate • Server Certificate • SSL Certificate	• Letter of Authorization from the company • Authorized Person's NRIC / Passport / Government issued ID for Foreigners • Change Management Request Form

4.9 Compromise and Disaster Recovery

4.9.1 Computing Resources, Software, and/or Data Corruption

4.9.1.1 This provision will be outlined in the Netrust Disaster Recovery Plan.

4.9.2 Entity Public Key is Revoked

4.9.2.1 In the event that the Netrust CA Certificate is revoked, Netrust shall take such steps to notify all Subscriber of such revocation in accordance with the notice provisions (Clause 2.4.2.4) of this CPS.

4.9.3 Entity Key is Compromised

4.9.3.1 In the event that the Netrust CA private key is revoked, Netrust shall perform disaster recovery procedures as set out in the Netrust Disaster Recovery Plan.

4.9.4 Secure Facility After a Natural or Other Type of Disaster

4.9.4.1 This provision will be outlined in Netrust Disaster Recovery Plan.

4.10 CA Termination

4.10.1 In the event that Netrust intends to discontinue its operations, Netrust will give the ORA, Sponsor and Subscriber a minimum of three months written notice before terminating its operations and will follow procedures in compliance with all applicable laws.

4.10.2 Netrust will make arrangements for its records and Certificate to be archived in a manner prescribed by the applicable laws of the Republic of Singapore.

5 PHYSICAL, PROCEDURAL & PERSONNEL SECURITY CONTROLS

5.1 Physical Controls

5.1.1 Site Location and Construction

5.1.1.1 Netrust PCS is currently housed in a secure data centre with four layers of protection to control physical access to the Netrust Operation Centre (NOC). These include:

a. The need to exchange either a Visitor/Contractor Pass with identification document at the reception of the data centre.

b. Restricted door access at the entrance of Data Centre.

c. Restricted trapped-door access to enter the Data Centre where the NOC is located. The NOC is a separate room in the data centre and data centre staff, who are on 24hrs * 7 days shift will ensure that only Netrust staff can access the room.

d. Biometrics technology has also been deployed to control the physical access to the NOC.

5.1.1.2 A manual log-file system is adopted to track the access to the NOC. Based on the above restriction, the person is required to sign-in/out at the Reception, the entrance to Data Centre and finally at the NOC. They are required to state the date/time and purpose of visit. In addition, movements of all Netrust authorized staff or its agents are to be accompanied by data centre personnel when in the restricted zone. A list of Netrust authorized personnel is provided to the data centre to ensure that only authorized Netrust staff are allowed to gain access to the NOC. Other Netrust's visitors, contractors and/or vendors to access the NOC need to be escorted by an authorized Netrust staff.

5.1.1.3 All Netrust ORA sites must also be protected to ensure only authorized staff has access to the ORA System. Netrust Administrators are responsible for the protection of the Netrust administrator profile. All these requirements and guidelines are set out in the applicable ORA Agreement.

5.1.1.4 The Netrust Subscriber must take full responsibility to ensure that their workstations and Netrust profile password are protected against unauthorized access and/or disclosure.

5.1.2 Power and Air Conditioning

5.1.2.1 Netrust CA Systems are adequately protected against power fluctuations or total loss of power by an uninterruptible power supply (UPS).

5.1.2.2 Netrust CA Systems are also adequately protected with air conditioning and cooling systems.

5.1.2.3 Netrust leverages on the Data Centre operations and procedures to cater for the above.

5.1.3 Water Exposures

5.1.3.1 Netrust CA Systems are adequately protected against water exposures.

5.1.3.2 Similarly, Netrust leverages on the Data Centre operations and procedures to meet such requirements.

5.1.4 Fire Prevention and Protection

5.1.4.1 Netrust CA Systems are adequately protected against fire. Netrust leverages on the Data Centre operations and procedures to cater for such protection.

5.1.5 Media Storage

5.1.5.1 The media storage used in the Netrust CA Systems are adequately protected against environment threats such as temperature, humidity and magnetism. The specific requirements are specified in Netrust Standards and Procedures Specification.

5.1.6 Waste Disposal

5.1.6.1 Netrust will perform data destruction once the CA-related data are no longer needed and/or the archival period has expired. Netrust will ensure the respective media that stores these information are properly sanitized or destroyed before it is release for disposal.

5.1.6.2 All disposal exercises will be recorded for audit purposes and shall be subject to such independent criterion as may be required pursuant to the applicable laws of the Republic of Singapore.

5.1.7 Off-Site Backup

5.1.7.1 Netrust provides off-site support for storage media back-up. Other off-site arrangement for business resumption will be specified in the Netrust Disaster Recovery Plan.

5.1.7.2 The security requirements for the off-site backup are similar to those that are practiced in Netrust premise, and they are in accordance to Netrust backup standards and procedures.

5.2 Procedural Controls

5.2.1 Trusted roles

5.2.1.1 Netrust establishes trusted roles to perform the critical CA function. These include:

- CA Security Officer(s) (minimum of 3)
  - implement the CA policies;
  - incorporate new Security Officers;
  - manage the CA Administrators;
  - verify audit logs, CP and CPS Compliance; and - is the manager of the System.
- Admin (CS)
  - manage the Subscriber registration process; and
  - create, delete, renew and/or revoke Subscriber Certificate.
- Admin (Engineer)
  - configure and maintain the CA system hardware and software; - administer the commencement and cessation of CA services; and - manage CA operators.
  - perform day-to-day monitoring of the CA Systems.
  - carry out activities such as collection of logs and backup
- Auditor
  - check logs

5.2.1.2 The appointment of these trusted roles is to ensure segregation of duties such that no one person can maliciously use the CA system without detection. Each of the trusted roles is limited to the actions they are required to perform in fulfilling their responsibilities.

5.2.1.3 Netrust will provide recommendations and guidelines to its ORA to carry out their responsibility as the remote CA Administrators. Where appropriate, the ORA will ensure separation of duties such that not all administrative functions are performed by one individual only.

5.2.2 Number of Persons Required Per Task

5.2.2.1 Netrust must ensure that no single individual may gain access to Subscriber private keys stored by the Netrust CA.

5.2.2.2 At a minimum two individuals, preferably using a split knowledge technique such as twin passwords to perform any key recovery operation.

5.2.2.3 All other duties associated with Netrust CA roles may be performed by an individual operating alone.

5.2.3 Identification and Authentication for Each Role

5.2.3.1 All Netrust trusted roles are verified and authenticated before they are issued an account or certificate to carry out their duties.

5.2.3.2 All Netrust trusted roles are to ensure that:

- The account or certificate issued directly attributed to an individual or an organization.
- The account or certificate issued is not shared.
- Restriction to actions authorized for the role is through the use of the account and/or certificate, Netrust software and procedural controls.

5.3 Personnel Controls

5.3.1 Background, Qualifications, Experience, and Clearance Requirements

5.3.1.1 The qualifications and experience of CA trusted personnel is in accordance to the job responsibility assigned to them. Netrust provides comprehensive training with respect to the duties they have to perform. (Netrust may issue such certificates as may be determined by Netrust to such personnel on the completion of the training)

5.3.1.2 Netrust will implement appropriate background checks for its key CA trusted personnel. The ORA are recommended to conduct such checks for their administrators.

5.3.1.3 Netrust establishes procedural controls such that the CA trusted personnel are bound by statute or contract not to disclose sensitive Netrust PCS information.

5.3.2 Background Check Procedures

5.3.2.1 Employees of Netrust are required to declare that they are not undischarged bankrupts, nor involved in any arrangement with any creditors or convicted of any offence in Singapore. Failure to comply will lead to disciplinary action taken by Netrust.

5.2.3.2 Employees of Netrust are also required to notify Netrust in the event that they are involved or may be involved in any prosecution. Failure to comply will lead to disciplinary action taken by Netrust.

5.3.3 Training Requirements

5.3.3.1 Netrust ensures that comprehensive training to respective Netrust trusted roles are provided in areas of:

- Netrust security principles and mechanism
- Netrust CA software version in use
- Netrust CA operating systems and network implementation
- Operational duties
- Netrust policies, standards and procedures
- Governing regulations and rules, where appropriate
- Netrust may issue certificates thereafter the completion of training

5.3.4 Retraining Frequency and Requirements

5.3.4.1 The re-training frequency is subject to the frequency of changes in the Netrust CA Systems.

5.3.4.2 The training requirements are in accordance to those specified in Clause 5.3.3.

5.3.5 Job Rotation Frequency and Sequence (Not Applicable)

5.3.6 Sanctions for Unauthorized Actions

5.3.6.1 Netrust will suspend the trusted personnel access to the Netrust PCS, in the event that he is suspected, or has performed unauthorized actions such as unauthorized use of authority and unauthorized use of the Netrust CA Systems or operations.

5.3.6.2 The suspension will be immediate upon detection and the period of suspension will be subject to investigation reports.

5.3.7 Contracting Personnel Requirements

5.3.7.1 Netrust does not employ contract personnel to perform the trusted roles in Netrust PCS.

5.3.7.2 In the event where Netrust authorized vendors and/or contractors need to access the Netrust CA system, authorized Netrust personnel must escort them at all time. All actions performed by these contracting personnel will be recorded and logged for accountability and audit purposes.

5.3.8 Documentation Supplied to Personnel

5.3.8.1 Pertaining to the training listed in Clause 5.3.3, respective documentation will be made available to Netrust personnel, where relevant.

6 TECHNICAL SECURITY CONTROLS

6.1 Key Pair Generation and Installation

6.1.1 Key pair generation

6.1.1.1 The Netrust CA owns a set of signing key pair. The key pair is generated using the respective Netrust controlled key generation software.

6.1.1.2 Each Subscriber will have control over the generation of his/her own Digital signature and Encryption key pairs using application provided by Netrust.

6.1.1.3 The key pair generation for Subscriber are in accordance with the applicable Netrust CP. The Netrust PCS allows the Subscriber to have control of the generation of his signing key pair.

6.1.2 Private Key Delivery to Entity

6.1.2.1 The Netrust CA private key is generated at system initialization stage. There is no requirement to deliver this key as this key remains in the Netrust CA System.

6.1.2.2 Netrust PCS supports the requirements where the private key is delivered to the Administrator or Subscriber in a secure on-line transaction.

6.1.3 Public Key Delivery to Certificate Issuer

6.1.3.1 The Netrust CA Certificate is self-signed and this is performed at system initialization stage. There is no requirement to deliver this public key to the Netrust CA.

6.1.3.2 Netrust PCS supports the requirements where the public key is delivered to Netrust CA in a secure on-line transaction. Alternatively, the public key can be delivered to the Netrust CA via PKCS#10 Certificate requests standards.

6.1.4 CA Public Key Delivery to Subscribers

6.1.4.1 Netrust PCS supports the requirements where the CA public key is delivered in a secure online transaction or downloaded from the Netrust website.

6.1.5 Key Sizes

6.1.5.1 The asymmetric key pairs in Netrust PCS will be at least 2048 bits RSA.

6.1.6 Public key parameters generation

6.1.6.1 The public key parameters will be generated via Netrust authorized software.

6.1.7 Parameter Quality Checking (Not Applicable)

6.1.8 Hardware/Software Key Generation

6.1.8.1 Netrust CA signature and encryption key pairs must be generated in a hardware cryptographic module.

6.1.8.2 Key pairs for all Subscribers may be generated in a software or hardware cryptographic module.

6.1.9 Key Usage Purposes (as per X.509 v3 key usage field)

6.1.9.1 The usage of key within the Netrust PCS is differentiated by the classes of Certificate.

6.1.9.2 Netrust PCS ensures that CA signing key is the only key permitted to be used for signing Certificate and CRLs.

6.1.9.3 The signing key may be used to provide services such as authentication, non-repudiation and message integrity.

6.1.9.4 The encryption key pair may be used to establish session key to perform message encryption.

6.2 Private Key Protection

6.2.1 Standards for cryptographic module

6.2.1.1 Refer to Clause 6.8

6.2.2 CA Private key (n out of m) Multi-person Control

6.2.2.1 The Netrust CA private key requires the presence of three or more persons to complete the generation successfully. No single Netrust trusted personnel is allowed to generate the CA private key.

6.2.2.2 The respective individual generates the Netrust Administrator and Subscriber private keys using Netrust authorized software.

6.2.2.3 The Netrust trusted personnel will be required to ensure that the Netrust CA private key will be erased from the temporary memory of the requisite equipment or Netrust authorized software upon the completion of the generation.

6.2.3 Private Key Escrow (Not applicable)

6.2.4 Private Key Backup

6.2.4.1 In Netrust PCS, Netrust shall not backup the private signing keys of the Subscriber. The Subscriber should backup their private signing keys and to ensure those keys are securely protected.

6.2.4.2 In Netrust PCS, Netrust may backup the private encryption keys of the Subscriber and ensure the keys are securely protected.

6.2.4.3 In Netrust PCS, Netrust may backup the Netrust CA private key and shall ensure that the backup is as securely protected as the storage of the Netrust CA private key.

6.2.5 Private Key Archival

6.2.5.1 The Netrust PCS supports encryption private key archival.

6.2.6 Private Key Entry into Cryptographic Module

6.2.6.1 In Netrust PCS, only Netrust Certificate Manager may submit the encrypted Netrust CA private signature key to the cryptographic module.

6.2.7 Method of Activating Private Key

6.2.7.1 The activation of private key in the Netrust PCS is via password authentication.

6.2.8 Method of Deactivating Private Key

6.2.8.1 The de-activation of private key in Netrust PCS is program termination initiated. Once terminated, the keys must be cleared from memory before the memory is de-allocated.

6.2.8.2 The cryptographic module in Netrust PCS also supports automated de-activation of private key after a pre-set period of inactivity.

6.2.9 Method of Destroying Private Key

6.2.9.1 The destruction of private key in Netrust PCS takes the following forms:

- The storage media for the private is damaged or lost.
- The surrender of keys to Netrust or its ORA.
- The keys are superseded by a new set of keys.
- Netrust carries out the waste disposal procedures as stated in Clause 5.1.6.

6.3 Other Aspects of Key Pair Management

6.3.1 Public Key Archival

6.3.1.1 The Netrust PCS performs public key archival in accordance with the archival procedures.

6.3.2 Usage Periods for Public and Private keys

6.3.2.1 The usage period of public and private keys in Netrust PCS is in accordance with the applicable Netrust CP. Netrust PCS supports validity period of keys up to six months, one year, three years and even up to twenty-five years.

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

6.4.1.1 The Netrust PCS supports unique and unpredictable activation data such as the set of reference and authorization codes and private key password.

6.4.2 Activation Data Protection

6.4.2.1 Netrust provides recommendation to ensure the activation data is protected from unauthorized use, this included physical access control and cryptographic mechanism where locking is activated after a predetermined number of unauthorized attempts is made.

6.4.3 Other Aspects of Activation Data (Not Applicable)

6.5 Computer Security Controls

6.5.1 Specific Computer Security Technical Requirements

6.5.1.1 Netrust ensures the security controls in Netrust PCS are addressed via:

- Physical and logical access control to the CA Systems.
- Segregation of Netrust trusted roles.
- Use of cryptography for communication with the Netrust CA Systems.
- Audit of all security related events

6.5.2 Computer Security Rating

6.5.2.1 Netrust is working with various vendors and standard bodies to achieve international security standards in Netrust PCS.

6.6 Life Cycle Technical Controls

6.6.1 System development controls

6.6.1.1 The design and development process for Netrust PCS software will be supported by:

- Third party verification/review.
- Ongoing risk assessment to influence security safeguard design.

6.6.2 Security management controls

6.6.2.1 The configuration of the Netrust PCS, as well as any modifications and upgrades will be documented and controlled.

6.6.2.2 Netrust will establish a change management system to control and monitor the configurations of the systems and prevent unauthorized modification.

6.6.3 Life Cycle Security Ratings

6.6.3.1 Netrust is working with various vendors and standard bodies to achieve international security standards for the development life cycle in Netrust PCS.

6.7 Network Security Controls

6.7.1 At least a firewall must be used to protect Netrust CA Operations environment against attacks from the Internet community.

6.7.2 Access to Netrust Certificate Manager, Netrust Certificate Directory, HSM and any device in Netrust operating center will only be granted to Netrust authorized personnel via access control mechanism such as ID and password authentication.

6.8 Cryptographic Module Engineering Controls

6.8.1 The cryptographic operations controls in Netrust PCS may be validated to at least FIPS 140-1 Level 2 or equivalent level of functionality and assurance.

7 CERTIFICATE AND CRL PROFILES

7.1 Certificate Profile

7.1.1 Version Number(s)

7.1.1.1 The Netrust Certificate is x.509 version 3 in accordance with the latest ITU-T Rec. X.509 and common standard ISO/IEC 9594-8.

7.1.2 Algorithm Object Identifiers

7.1.2.1 The Netrust PCS supports, but not limited to, the following algorithms:

- RSA 2048/4096/ 6144 digital signature
- Elliptic Curve -192 digital signature
- RSA 2048/4096/6144 key transfer
- SHA-1, SHA-256, SHA-384 and SHA-512
- Triple-DES and AES
- Message Authentication Code (MAC)
- MD5 Message-Digest Algorithm

7.1.3 Name Forms

7.1.3.1 The Netrust PCS supports unique person name form for the following categories of Subscriber:

- Individual
- Corporate/corporate representative
- Application server
- The specification of this name form consists of attributes common Name and/or serial Number

7.1.4 Name Constraints (Not applicable)

7.1.5 Certificate Policy Object Identifier (OID)

Type	OID
Netrust Net Server Certificate	1.2.702.0.1002.6.1
Netrust Personal NetID Certificate	1.2.702.0.1002.6.2
Netrust Corporate NetID Certificate	1.2.702.0.1002.6.4
Netrust Professional ID Certificate	1.2.702.0.1002.6.5
Netrust Corporate Org ID Certificate	1.2.702.0.1002.6.6
Netrust Enterprise Email Certificate	1.2.702.0.1002.6.9
Netrust Adobe Certificate	1.2.702.0.1002.7.1
Netrust SSL Certificate	1.2.702.0.1002.7.2
Test Server Certificate	1.2.702.0.1002.11.1
Test Individual Certificate	1.2.702.0.1002.11.2
Test Corporate Certificate	1.2.702.0.1002.11.4
Test Professional Certificate	1.2.702.0.1002.11.5
Test Organization Certificate	1.2.702.0.1002.11.6
Netrust Test Certificate (Others)	1.2.702.0.1002.15.1

7.1.6 Usage of Policy Constraints Extension (Not applicable)

7.1.7 Policy Qualifiers Syntax and Semantics (Not applicable)

7.1.8 Processing Semantics for the Critical Certificate Policy Extension (Not applicable)

7.2 CRL Profile

7.2.1 Version number(s)

7.2.1.1 The Netrust CRL is x.509 version 3 in accordance with ITU-T Rec. X.509 and common standard ISO/IEC 9594-8.

8 Personal Data Protection

8.1 Netrust Data Protection policy

8.1.1 This Data Protection Notice sets out the basis which Netrust may collect, use, disclose or otherwise process personal data of our customers in accordance with the Personal Data Protection Act (PDPA). This Notice applies to personal data in our possession or under our control, including personal data in the possession of organisations which we have engaged to collect, use, disclose or process personal data for our purposes.

8.1.2 In accordance to our CPS 4.1.2, Netrust requires the NRIC to validate the identity of the individuals applying for the issuance of Netrust Digital Certificates the information in the Netrust Digital Certificate shall be unique to the identity of the as user reflected in our Certificate Policy.

E.g. of Corporate Net-ID Certificate ("NCNC") certificate policy requirement

3.1. Serial Number (2.5.4.5)	(ISO Alpha-2 country code + '-' + Masked NRIC or Passport No. or FIN No.) or (Employee No.) + ':' YYMMDDHHMMN* + ':' E or W + ':' + 0 E.g. SG-XXXXX567A:1908010900N1:E:0
5.1. Policy Identifier	1.2.702.0.1002.6.4

8.1.3 Netrust being a Certificate Authority has always safeguarded applicants' personal data from unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks with appropriate administrative, physical and technical measures such as up-to-date antivirus protection, encryption and the use of privacy filters to secure all storage and transmission of personal data and shall disclose personal data internally only on a need-to-know basis.

9 SPECIFICATION ADMINISTRATION

9.1 Specification Change Procedure

9.1.1 Prior to making any changes in Netrust CP and this CPS, Netrust will document the list of proposed changes. The list will be circulated to ORA, CA whom Netrust has directly cross-certified with, and the Controller of Certificate Authority of Singapore, for comments. The comment period will be thirty days unless otherwise specified.

9.1.2 All comments will be consolidated and reviewed by Netrust management. The decision to implement the proposed changes is at the sole discretion of Netrust, or subject to regulatory government body approval, where appropriate. A decision for the final change will be announced within two weeks.

9.1.3 Netrust will adhere to its change management control procedures such that all changes made to the CP and CPS are tracked and version controls are in place.

9.2 Publication and Notification Policies

9.2.1 All items in Netrust CP and this CPS are subject to the publication and notification requirement.

9.2.2 All publication and notification will be done via the Netrust web site at http://www.netrust.net unless the notification has great impact to Netrust, Sponsor, ORA, Subscriber and Relying Party, e.g. termination of CA services.

9.2.3 Netrust may digitally sign each publication and notification before they are posted at the Netrust web site.

9.2.4 Netrust will, from time to time, suggest and make available to, publish or will notify the Subscriber of what may be constituted as adequate private key protection measures.

9.2.5 Netrust will make available to, publish or will notify the Subscriber of risks associated with the use of any Certificate, issued by Netrust to the Subscriber, based on any technologies used by Netrust which have been discontinued or superseded.

9.3 CPS Approval Procedures

9.3.1 Once a revised CPS is ready for publication, Netrust management will approve it with legal advice from the Company lawyers.

GLOSSARY

Abstract Syntax Notation.1 (ASN.1) - ASN.1 is an abstract language representation used to describe data types in a machine-independent fashion.

CA System Administrator - A trusted Netrust personnel responsible for day-to-day activities involving administering an X.509 Directory.

CA Security Officer - A highly trusted Netrust personnel in a position to set Netrust's security policies for the Netrust CA operation.

CA Administrator - A trusted Netrust personnel responsible for day-to-day activities involving administering a Netrust CA system

CA Operator - A trusted Netrust personnel responsible for day-to-day batch activities such as backup, restore and etc.

Certification Authority ("CA") - A CA is a trusted third party ("TTP") that issues and signs a Certificate.

Certificate Policy ("CP") - A CP is the named set of rules that sets out, determines and indicates the applicability of a Certificate to a particular community and/or classes of applications with common security requirements.

Certification Practice Statement ("CPS") - Please see Netrust CPS.

Certificate Revocation List (CRL) - A CRL is a signed list of entries corresponding to revoked public keys, with each entry indicating the serial number of the associated Certificate, the time the revocation was first made, and possibly other information such as the revocation reason.

Governing Law - The laws of the Republic of Singapore.

Grace Period - The time period under which Netrust will take to respond to an action.

Netrust Pte Ltd - Netrust Pte Ltd ("Netrust") is a private limited company incorporated in the Republic of Singapore and having its principal place of business at 70 Bendemeer Road, #05-03 Luzerne Building, Singapore 339940.

Netrust CP - Netrust CP is the named set of rules that sets out, determines and indicates the applicability of a Netrust Certificate to a particular community and/or classes of applications with common security requirements.

Netrust CA - Netrust CA is the trusted third party ("TTP") that issues and signs a Netrust Certificate.

Netrust Certificate Manager - A software system that manages cryptographic keys for Netrust users.

Netrust CPS - Netrust CPS is a detailed statement of the practices and operational procedures that supports multiple CP, of Netrust.

Netrust Directory

Netrust Disaster Recovery Plan - The Netrust Disaster Recovery Plan means the current plans and procedures implemented by Netrust which may be verified by Netrust's independent auditors or controller.

Netrust Public Certification Services Framework ("PCS") - Netrust PCS is the Certificate-based public key infrastructure (PKI) that issues, manages, revokes and renews Netrust Certificate in accordance with the practices set out in the Netrust CPS. Please see Netrust CPS.

Non-Sponsor ORA - A non-Sponsor ORA is an ORA performing the functions of an ORA without any payment obligations as required of a Sponsor.

Organization Registration Authority ("ORA") - An ORA is an agent authorized by Netrust to issue Netrust Certificate.

Object Identifier ("OID") - An OID is a value, comprising a sequence of integer components, which can be conveniently assigned for some specific purpose, and which has the property of being unique within the space of all OIDs.

On-line Revocation Checking Requirements

ORA Agreement - An ORA agreement is a contract which provides detailed outline of procedures, obligation and liabilities for each Netrust appointed ORA.

Relying Party - A Relying Party is a recipient of a Subscriber's Certificate in the Netrust PCS who acts in reliance on that Netrust Certificate.

Sponsor - A Sponsor is the party who will be responsible for all payment obligations in relation to each Subscriber's Certificate and shall be entitled to such Netrust Certificate management rights as set out in the CP.

Sponsor ORA - A Sponsor ORA is an ORA performing the functions of an ORA with payment obligations in relation to each Subscriber's Certificate (s).

Subscriber - An individual, partnership, corporation, application server or such other categories of person who is a holder of any Netrust Certificate.

In the CPS and the CP, except to the extent that the subject matter or context may otherwise require, (i) expressions including the singular may indicate the plural and vice versa, (ii) expressions indicating any particular gender may indicate all other genders and (iii) expressions indicating bodies corporate may also indicate natural persons and vice versa.